# \*\*\*\*Resilience Affirmative: GDI22 Packet\*\*\*\*

# Resilience Aff: FYI

### FYI: Resilience Strategies

#### Resilience explained in context of NATO

Hall & Sandeman, London School of Economics researchers, ‘22

[Jonny Hall, PhD Candidate, International Relations, London School of Economics and Political Science and Hugh Sandeman, Visiting Senior Fellow, LSE Ideas and Project Head of Global Strategies, “NATO’s Resilience: The First and Last Line of Defence,” Strategic Update, LSE IDEAS, 5—22, London School of Economics p. 7-8]

What Is Resilience?

NATO defines resilience as “a society’s ability to resist and recover from such shocks” as natural disaster, failure of critical infrastructure, or a hybrid or armed attack.5

This definition touches on two features of resilience: First, resilience concerns the ability to absorb and recover from a state of crisis.6 Second, resilient actors must be able to respond to a range of potential shocks, both expected and unexpected. This relates to the ability to survive; as one widely adopted definition of resilience puts it, an actor must be able “to maintain its core purpose … in the face of dramatically changed circumstances”.7 This can be seen in NATO’s seven baseline requirements for national resilience, which represent an effort to delineate the core components of a functioning state by focusing on the continuity of government and hospital services, energy supplies, food and water resources, communication networks, and transport systems.8 Conceived as the power to survive in crises, resilience can be seen as a defensive and reactive concept.

Resilience is as much about coping with all possible eventualities as trying to anticipate specific events. While national preparedness for systemic shocks is now motivated by at least some clearly identifiable defence and national security priorities, it is still helpful to take a generic approach to preparing for unexpected shocks. Such generic measures include allocation of responsibilities at the national, regional and local level; the requirement for a single lead agency at the centre of government in any emergency; disciplines for exercising pre-agreed procedures with senior people involved; and rolling audit programmes to test that these disciplines remain effective.9

Resilience, therefore, has political and psychological as well as physical dimensions.10 It can be viewed in exclusively material terms as shown above, but also as a psychological mindset held by groups or individuals which allows them to function in the face of adversity. Structures and procedures for coping with shocks cannot ensure national resilience in a crisis if the mindset for responding effectively is not there. It was this mindset for recognising and rising to an emergency that was missing in the UK’s initial response to the COVID-19 emergency in early 2020. The same applies to Europe’s response to the Russian invasion of Crimea and eastern Ukraine in 2014, when the governments of larger European powers did not fully register the alarm felt on the continent’s northern and south-eastern borders.

Conceived as a mindset to respond to adversity, resilience thus entails a “social dimension, located not only in the state but also among the actors of civil society”.11 It is this societal cohesion that Russian information warfare has explicitly targeted in its attempts to undermine the political stability of NATO states. In response, a wholeof-society approach has formed the basis of NATO’s increased cooperation with the European Union on encouraging societal resilience, such as the 2016 joint EUNATO declaration.12

Military, physical, political and societal resilience have the potential to deter as well as defend. As NATO’s Brussels Communiqué recognised, the capacity for resilience can influence the policies of opponents by deterring them from armed attack or other offensive measures.13 Effective and visible resilience is therefore strongly linked to deterrence by denial. Contrary to the idea of deterrence by punishment, which threatens actors with severe penalties if they launch an attack, deterrence by denial seeks to deter actions by making them appear unlikely to succeed.14

#### Description of resilience (and resilience-thinking

Pernik & Jermalavičius, International Centre for Defence & Security analysts, ‘16

[Piret Pernik and Tomas Jermalavičius, Research Fellows, International Centre for Defense and Security “Resilience as Part of NATO’s Strategy: Deterrence by Denial and Cyber Defense,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. 100]

In generic terms, resilience has been defined as a “process linking a set of adaptive capacities to a positive trajectory of functioning and adaptation after a disturbance.”3 This definition implies that resilience is a process, although it can also be seen as a strategy or as the “capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must.”4 It draws on certain resources of the system and on “dynamic attributes of those resources (robustness, redundancy, rapidity).”5 This perspective allows a proactive approach to building resilience by means of accumulating necessary resources in a system and ensuring that those resources possess the dynamic attributes required at a time when disruptions occur. System managers can thereby devise policies (e.g. principles, norms and standards, priorities of investments) which are conducive to resilience. This is particularly applicable to enhancing cybersecurity, which we cover later in this chapter.

### FYI: NATO Cyber Policy

#### Description of current NATO cyber policies and bodies

Ilves et al., Estonian Counselor at EU, ‘16

[Luukas K. Ilves, Counselor for Digital Affairs, Permanent Represnetation of Estonia to the EU, Timothy J. Evans, Senior Advisor, Cyber Strategy and Policy, Johns Hopkins University Applied Physics Laboratory, Frank J. Cilluffo, Director, Center for Cyber and Homeland Security, George Washington Univesity, and Alec A. Nadeau, Presidential Administrative Fellow, Center for Cyber and Homeland Security, George Washington University, “European Union and NATO Global Cybersecurity Challenges: A Way Forward,” PRISM v. 6 n. 2, 2016, p. 129-130]

How did NATO get to its current state in cybersecurity? NATO has always defended its military communication networks; however, during the 2002 Prague Summit, NATO stated that cyber defense was also part of its agenda and that it would strengthen its “capabilities to defend against cyber attacks.”10 The Prague Summit paved the way for NATO’s creation of the NATO Computer Incident Response Capability (NCIRC) in 2002. Following the cyber attacks against Estonia in April and May of 2007, NATO issued its first “Policy on Cyber Defence” in January 2008. It later issued its “Strategic Concept” in 2011, as well as a newly enhanced cyber defense policy in 201411 in which NATO clarified that Article 5 could be invoked for a major digital attack.12 It also pledged to improve cyber defense education, training, and exercise activities, in addition to its commitment to create a NATO cyber range capability.13

While NATO does not have a standing cyber defense force per se, its structures now cover the political, operational, and technical challenges of cyber defense. The North Atlantic Council (NAC), established under Article 9 of the North Atlantic Treaty, is the key entity within the Alliance that decides whether NATO responds to an attack of any nature. The Cyber Defence Committee (CDC), known as the Defence Policy and Planning Committee until 2014, is a senior advisory body that advises the NAC on cyber issues, as does the Cyber Defense Management Board (CDMB). Cyber is part of the NATO defense planning process that sets force goals for the Alliance as a whole.14

In 2012, NATO officials created the NATO Communication and Information Agency (NCIA) through a merger of a number of existing agencies.15 The NCIA acts as NATO’s principal deliverer of communications, command, and control (C3), which includes IT support to NATO Headquarters, the NATO Command Structure, and NATO Agencies. NCIA is responsible for defense capability planning; command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) architecture, exercises, and training; and acquisition and procurement of advanced technology. NCIA also functions as NATO’s first line of cyber defense and houses both the NCIRC team and NATO’s Information Security Operations Centre.16

Though formally outside of the NATO command structure, the Alliance also relies on work done by the NATO Cyber Defence Center of Excellence (CCD COE) in Tallinn, Estonia. The CCD COE develops doctrinal and legal concepts, conducts training and exercise programs, carries out technical research and experimentation, and contributes to national and NATO capabilities.17 The CCD COE launched the Tallinn Manual process, which has become the main authority on the applicability of the law of armed conflict to cyberspace. The Tallinn Manual 2.0 will be published in 2016 and will examine international law for cyber operations below the threshold of armed conflict.

NATO, much like the U.S. Government, is intensifying its relationships with private-sector cyber security companies. The NATO Industry Cyber Partnership (NICP) initiative is designed to encourage relationships with industry.18 NATO is also developing a Cyber Rapid Reaction Team (RRT)19 to protect its critical infrastructure, much like U.S. Cyber Command’s Cyber Protection Teams (CPTs).20 The protection of critical infrastructure under some circumstances may require offensive cyber capabilities to stop an attack. Unlike U.S. Cyber Command, NATO does not have an inherent offensive capability.

Finally, NATO is actively exercising its cyber forces. Cyber Coalition, a primarily table-top exercise, now includes more than 35 participating countries and has been integrated into NATO’s crisis management exercises.21

In addition, the NATO CCD COE organizes the world’s largest international live-fire cyber defense exercise in Tallinn,which in its 6th iteration in 2016 saw more than 550 people and over 26 nations participate.22 Using a fictional scenario and virtualized networks, the exercise involved defenders, attackers, and bystanders. Twenty blue (“friendly”) teams, represented by 19 nations and the NCIRC, were tasked with maintaining networks and services in a fictional country that was under attack.23

NATO’s trend toward increased cooperation and joint operational exercises in the cyber realm tends to reflect a broader shift toward more robust coordination in the majority of its mission areas. NATO currently does not have any operational cyber capabilities as an organization, relying instead on Allied capabilities. The technical capabilities of NCIRC are used solely to protect the limited footprint of NATO’s own command structure. As cyber defense becomes an operational domain in its own right, NATO should consider creating a tactical command similar to those for land, air, and maritime.24 Given that cyber lends itself to economies of scale, NATO could also consider developing certain shared capabilities, similar to its strategic airlift and airborne warning and control systems capabilities.

#### Decription of NATO policies post-2018 creation of Cyberspace Operations Centre

Lewis, USAF Colonel, ‘19

[Don Lewis, Colonel, U.S. Air Force and Deputy Director, Cyber Operations Centre, Suprme Headquarters, Allied Powers Europe, “What Is NATO Really Doing in Cyberspace?” WAR ON THE ROCKS, 2—4—19, <https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/>, accessed 6-3-22]

Who Are NATO’s Cyberspace Defenders?

The North Atlantic Council is the principal political decision-making body in NATO, representing the heads of state of all 29 nations in the alliance. As explained earlier, NATO heads of state and government made the declaration recognizing cyberspace as a domain of operations. They also, at the July 2018 Brussels Summit, declared that NATO would establish the Cyberspace Operations Centre in Belgium. The center launched in August 2018 and, still in its early stages of development, is the central hub of cyberspace operations in the alliance, but its primary role is to orchestrate the efforts of numerous, existing, and well-established elements, inside and beyond the command structure, to execute cyberspace operations.

NATO headquarters in Brussels conducts several committees and boards that provide governance, doctrine, and policy for numerous efforts, including cyberspace operations. Among them is the Military Committee, the Cyber Defense Committee, and the Cyber Defense Management Board. These entities set the parameters and identify roles and responsibilities for cyberspace activities.

Responsibility to defend NATO in cyberspace “as effectively as in Air, Land, and Maritime” environments belongs to the head of Allied Command Operations, the Supreme Allied Commander Europe, who has domain advisors for each operational domain: the commanders of Air Command, Land Command, and Maritime Command. In a prudent measure, the center stood up within Allied Command Operations headquarters in Mons, Belgium — the Supreme Headquarters Allied Powers Europe. In this manner, the Cyberspace Operations Centre can leverage the strategic staff capabilities of the existing headquarters without having to provide them for itself, which also serves to hasten its development. The center functions as the theater component for cyberspace, just as the geographic commands do for their respective operational domains. The deputy chief of staff for cyberspace is supreme allied commander Europe’s domain advisor for cyberspace. The director of the Cyberspace Operations Centre reports to deputy chief of staff for cyberspace.

How Will the Cyberspace Operations Centre Defend NATO in Cyberspace?

The Cyberspace Operations Centre cannot defend NATO in cyberspace all by itself. That will require a NATO-wide approach — and beyond.

The center’s mission is three-fold: providing situational awareness of the domain, planning for the cyberspace aspects of allied operations, and managing the execution of operational direction to ensure freedom of maneuver in in all domains affected by cyberspace activities.

The center executes its mission at both the strategic and operational levels. It supports commanders with strategic domain advice, planning support, and integration of effects via Cyberspace Operations Centre liaison elements who are tasked to directly support the regional joint force commands and, when necessary, joint task force commanders.

The Cyberspace Operations Centre provides the central role of cyberspace defense, and it collaborates with several entities to do so. In order to achieve situational awareness, it needs intelligence from NATO’s member nations. There are intelligence analysts embedded within the center to request intelligence from the nations and assess it, and there are other intelligence organizational elements which support that function, including the NATO Intelligence Fusion Centre and Allied Command Counter-Intelligence. The Cyber Threat Assessment Cell at NATO headquarters provides additional information from a political assessment perspective.

Another key player is the NATO Communications and Information Agency. The agency is the primary communications and information service provider for NATO and, like every service provider, one of its main service lines is cyber security. Cyber security, a subset of cyber defense operations, is a set of practices and procedures necessary to protect networks and the information that resides in them. As such, the agency needs to persistently report the status of NATO networks to the Cyberspace Operations Centre, manage routine cyber security incidents from a technical perspective, and respond to operational direction from the Cyberspace Operations Centre when incidents have operational impact. The agency needs to continue its cyber security operations, and continuously enhance them, as NATO seeks to strengthen its cyberspace defense stance.

While the agency is largely responsible for the provision of static networks, the NATO Communications and Information Support Group extends them where they are needed operationally for deployed forces. Likewise, the group needs to respond to operational direction from the Cyberspace Operations Centre through its deployed coordination cell.

The Cyberspace Operations Centre will also need liaison with its counterparts in allied nations to share information contributing to situational awareness. Those mutually beneficial relationships are in development.

# Resilience Aff: 1AC

### Plan + Solvency: 1AC

#### The United States federal government should increase its security cooperation with the North Atlantic Treaty Organization by facilitating:

#### enactment of resilience as a core concept;

#### cyber coordination;

#### expansion of industry partnerships, including to appropriate non-members;

#### foresight analysis;

#### development of a cyber code of conduct.

#### A—Adopting a resilience strategy is necessary to respond to new cyberthreats, and should be a part of NATO’s partner initiative

1—update stategic concept

2—upgrade coordination

3—expand industry partnerships to non-members

4—foresight analysis

5—code of conduct

Blessing, American Enterprise Institute fellow, ‘22

[Jason Blessing, Visting Research Fellow, American Enterprise Institute and PhD, Political Science, Syracuse University, “Fail-Deadly, Fail-Safe, and Safe-to-Fail: The Strategic Necessity of Resilience in the Cyber Domain,” NATO 2030: TOWARDS A NEW STRATEGIC CONCEPT AND BEYOND, Ed. J.Blessing, K.KjellstromElgin, N.M.Ewers-Peters, School of Advanced International Studies, Johns Hopkins University, 2022, p. 273-280]

‘Safe-to-Fail’: Building Cyber Resilience into NATO

The political and technical dynamics discussed in the previous section highlight the necessity of a safe-to-fail strategy for NATO in the cyber domain. Cyber resilience offers a way for the Alliance to address a range of threats below the threshold of armed conflict to which fail-deadly and fail-safe strategies fail to apply—such as ransomware attacks, distributed denials of service, exploitation of digital supply chains, or operations conducted by non-state proxy actors. Moreover, even low-sophistication cyberattacks can produce disruptive and cascading effects across societies with consequences that are difficult to anticipate. Resilience thus offers a broader strategic umbrella for the Alliance to plan for, recover from, and adapt in the wake of unanticipated disruptions from cyberspace.

From a technical perspective, cyber resilience hinges on the ability of key information and communications systems to anticipate and withstand disruptions to service provision by allowing core services and functions to fail without compromising their ability to recover at or above original capacity.55 These same principles can be applied to the strategic level. As a safe-to-fail strategy, cyber resilience is premised on both the failure to deter and defend against all cyber threats and the failure to foresee all potential strategic disruptions. The goal of cyber resilience is thus to favorably shape the conditions of such failures by forecasting, preparing for, and learning from strategic shocks in or through the cyber domain that can have unanticipated, multiple-order, and spillover effects.

NATO already possesses the strategic foundation for pursuing greater cyber resilience and has recently reiterated its commitment to resilience writ large.56 At the 2016 Warsaw Summit, Allies agreed to seven baseline requirements for national resilience, one of which seeks to strengthen civil communications systems. This requirement was updated in November 2019 to reflect considerations for 5G.57 The Cyber Defense Pledge offers a more specific platform for linking national capability development to allied resilience. It emphasizes the need for greater resources, more domestic stakeholder interaction and information sharing, and better cyber hygiene and education.58 However, these initiatives have both been couched in the self-help principle of Article 3 of the North Atlantic Charter, whereby Allies work towards greater resilience “separately and jointly, by means of continuous and effective self-help and mutual aid.”59 As such, Allies pursue cyber resilience relatively independently. For example, the Cyber Section of NATO’s Emerging Security Challenges Division (ESCD) conducts a regular survey of all member states for the Cyber Defense Pledge, but national responses are voluntary and Allies must individually request information from previous surveys.

Yet, fully incorporating safe-to-fail principles into the Alliance necessitates viewing resilience outside of the Article 3 context as a necessarily shared effort among member states. The limitations of collective defense discussed in this chapter highlight the potential for cyber operations to produce unanticipated, cross-boundary effects. Allied resiliency is inextricably interdependent—the digital interconnectedness of allied economic and defense efforts means that the vulnerabilities of one ally become vulnerabilities for all. Entanglement with the private sector is also an important confounding factor for members’ self-help efforts. NATO and its members will continue to rely on the private sector and civilian infrastructure for mission-critical systems and new technologies. The speed and spillover of disruptive cyber incidents like the WannaCry ransomware and the NotPetya wiperware-disguised-as-ransomware speak to the insufficiency of relying only on self-help measures to build cyber resilience.60 Resilience through selfhelp is therefore only part of the puzzle; safe-to-fail policies require more formalized coordination across NATO. Such efforts can leverage consultation mechanisms and processes derived from Article 4 of the North Atlantic Treaty,61 and Article 2 provides a powerful basis for members to coordinate with the private sector and deconflict economic policies underlying cyber resilience.62

This shared resilience must also be projected forward outside the bounds of the Alliance to NATO’s partners. The same cyber threat dynamics that make resilience a shared endeavor among members also highlight the importance of developments in partner and other third-party states (on partnerships, see Elgin and Wieslander in this volume). Unlike in traditional domains, NATO’s resilience and collective defense in the cyber domain are directly affected by the resiliency of non-members. Ukraine serves as a key example, as the country has been a testbed for Russian cyber operations with international implications. For instance, the BlackEnergy Trojan malware deployed against the Ukrainian power grid in 2015 was later found on US power grid networks.63 In the case of the 2017 cyberattacks on Ukraine, the NotPetya malware self-replicated and spread rapidly and destructively to over 150 countries using the Windows-based exploits.64 These incidents show the tenuous nature of cyber resilience and the need for the Alliance to aid partners in modernizing and building resilient digital infrastructures. Article 10 of the Treaty already lays the foundation for projecting resilience forward to aspiring members65 and can be used to set cyber resilience requirements alongside more traditional standards. Forward cyber resilience is in NATO’s best interests: the Alliance will be more resilient if its neighbors and partners are more resilient.

Operationalizing shared and forward cyber resilience as a safe-to-fail strategy will require four main lines of effort.66 First, critical cyber assets, functions, personnel, and intersections and dependencies, must be identified and prioritized. Prioritization hinges on determining the relative exposure and significance of assets, how they may be targeted and attacked, and the areas where greater risks can be assumed. Second and related is risk minimization, particularly in terms of supply chains. One issue that has risen in prominence is the use of 5G infrastructures and networks. For instance, relying on non-allied suppliers of military or other vital communications infrastructures, such as Chinese companies Huawei and ZTE, can entail increased vulnerabilities for the Alliance.67 Other important aspects of risk minimization include continuous threat monitoring and the development of continuity-of-operations plans for cyber crises. Continuity plans are particularly crucial for ensuring that adversaries gain fewer and shorter-term payoffs from disruptions like ransomware attacks or sophisticated wiper worms that delete information. Third, foresight and long-term trend analysis are critical for cyber resilience, as strategic and technological change will further complicate an already complex operational environment. Threat actors will continue to develop new doctrines, institutions, and capabilities for the cyber domain. Emerging technologies, such as quantum computing, and the increased use of artificial intelligence will undoubtedly impact the scope, nature, and disruptive potential of cyber threats to the Alliance and its members.68 In this vein, NATO’s proposed establishment of a defense innovation accelerator is an important forward-looking development.69 Fourth, effective cyber resilience requires not only bouncing back to normal from disruptions, but also bounding forward via adaptation and the institutionalization of ‘lessons learned.’ Each of these lines of efforts will require institutionalized cooperation among member states and between NATO and its partner countries.

Shared and forward cyber resilience complements collective defense by addressing a range of grey zone threats to which fail-deadly and fail-safe logics do not apply. At the same time, the safe-to-fail logic of resilience can strengthen the Alliance’s ability to carry out its other core tasks. Resilience makes collective defense more credible, as the continuity of critical functions and services are crucial for reducing the benefits of disruption for adversaries. For instance, implementing a safe-to-fail strategy helps to reduce the impact of defensive capability gaps between allies in the cyber domain. Resilience efforts also support collective defense by overlapping with deterrence-by-denial measures.70 Moreover, and particularly in terms of crisis management, cyber resilience can support efforts in traditional domains by ensuring that NATO and Allied land, sea, and air components dependent upon cyberspace can continue to operate with minimal disruption. Projecting cyber resilience forward to NATO’s partner countries also provides an avenue from which to strengthen the Alliance’s cooperative security engagements. Finally, the future-oriented and adaptive nature of resilience provides an important foundation for collective defense, crisis management, and cooperative security in the cyber domain to evolve with the emergence of new technologies and threats as the Alliance heads into the next decade and beyond.

Recommendations

The Alliance can take several steps to better integrate cyber resilience into its activities as it looks to 2030 and beyond. This section provides five recommendations to help NATO operationalize the main aspects of cyber resilience set forth in the previous section. These are: the adoption of comprehensive resilience as a core task; the formalization of cyber resilience efforts among members; the expansion of the NATO Industry Cyber Partnership; the creation of a NATO Office of Net Assessment; and the longer-term development of a cyber ‘code of conduct.’

1. Update the Strategic Concept and adopt a fourth core task of comprehensive resilience.

Most pressingly, NATO should update its Strategic Concept to accurately reflect its commitment to collective defense in the cyber domain and to incorporate a fourth core task of comprehensive resilience, of which shared and forward cyber resilience is a component. Given the scant attention to cyber issues in the 2010 Strategic Concept, a new Strategic Concept is needed to tie together and bring further coherence to a decade’s worth of strategic developments for cyberspace. Moreover, a revised Strategic Concept is a necessary step for integrating fail-deadly, fail-safe, and safe-to-fail logics into the Alliance’s cyberspace initiatives. Given the limits of fail-deadly and fail-safe strategies, safe-to-fail policies that underlie resilience are needed to address a wider range of threats the Alliance faces in and through the cyber domain.

2. Formalize coordination, consultation, and mutual aid for cyber resilience among Allies.

Resilience as a core task across the Alliance will require moving past self-help notions of resilience towards a conception of shared resilience. This move should entail the development and use of common defensive metrics,71 defensive capability standards, and frameworks for reporting major cyber incidents. In this regard, formalizing the ‘infor- mation broker’ role of the ESCD’s Cyber Division vis-à-vis the Cyber Defense Pledge would be a significant initiative. NATO should formalize the ways in which the Cyber Division collects, processes, and disseminates data on Allied cyber resilience. The routine production of qualitative case studies represents an important mechanism for contextualizing trends from quantitative data and identifying policy and technical problems, common deficiencies, ‘lessons learned,’ and best practices for addressing respective problems. Just as it surveys Allies on cyber resilience, the Cyber Division should also develop survey methods for member states that help identify informational needs – both individually and multilaterally – across the Alliance. The Cyber Division could thus act as a data repository that facilitates issue-centric ‘minilaterals’ among Allies. Concomitantly, the Cyber Division should explore new avenues for the regular distribution of cyber resilience trends and findings, such as quarterly reports or published case studies for all Allies, which supplement yearly conferences and reporting.

Consultation mechanisms will be crucial transferring skills and expertise among allies, a key component to help build domestic cyber exercise staging capabilities in smaller Allies. One such avenue for greater coordination, consultation, and mutual aid is expanding the scope of NCIRC so that teams are available outside of crisis situations, much like the Resilience Advisory Support Teams. While the NCIA does offer advisory teams, these teams are not formalized like emergency response teams under NCIRC. Should NCIRC be expanded to include formal advisory teams, member states could request these teams as an observing or assessing party for bilateral and multilateral “hunt forward” missions. Such a role can serve to facilitate NATO’s broader goals of situational awareness, threat intelligence sharing, and vulnerability assessment.

3. Expand the NATO Industry Cyber Partnership on a case-by-case basis to include actors in like-minded non-NATO nations.

Building bridges with key private sector actors in non-NATO member states through the NATO Industry Cyber Partnership72 will be an important aspect of projecting resilience forward. Companies in Enhanced Opportunity Partner nations, like Ericsson in Sweden and Nokia in Finland, represent natural candidates for expansion. The Al- liance should also look to broader Interoperability Platform Partners with vibrant telecommunications sectors like South Korea and Japan, home to Samsung and Sony, respectively. Expanding the NATO Industry Cyber Partnership on a case-by-case basis can help build greater resilience into digital supply chains and spur the development of viable alternatives to digital infrastructures and products from companies in countries like China.

4. Improve cyber foresight and adaptation to future threats by establishing a NATO Office of Net Assessment.

Resilience requires systematic evaluation of present and future conditions; as such, NATO should establish an Office of Net Assessment to institutionalize the Alliance’s future-oriented analysis. A NATO Office of Net Assessment should be tasked with analyzing organizational strengths and weaknesses vis-à-vis adversaries in the cyber domain. Part of this effort should include developing metrics for assessing Allied operational success in cyberspace. Doing so will provide a clearer picture of the current and future threat environment and should help reconcile differential threat assessments by Allies. Additionally, an Office of Net Assessment should play a role in forecasting the impact of emerging cyberspace technologies across a variety of scenarios. This forecasting role should extend to the development of wargaming scenarios specific to the cyber domain as well as for broader cross-domain operational contexts where conventional forces operate in degraded communications environments. This effort can look to leverage the expertise and collaborate with the NATO Cooperative Cyber Defense Center of Excellence located in Estonia, which sponsors the annual Locked Shields and Crossed Swords exercises.73

5. Develop a cyber ‘code of conduct.’

In the longer term, NATO should work to develop a normative ‘code of conduct’ for states operating in the cyber domain that focuses on behavior and standardization and complements the work of the United Nations Group of Governmental Experts. Such a code of conduct could presage a formal policy and would be a critical first step in determining when and how to respond to the cumulative costs of below-threshold cyber incidents over time. A code of conduct could also be the basis for promoting best practices for cyber hygiene and for outlining responsible applications for artificial intelligence and emerging technologies like quantum computing in military contexts. Likewise, it can be the foundation for developing stances on more contentious issues like out-of-network operations on allied or partner networks and defining violations of sovereignty in cyberspace. This should ultimately be an intra-Alliance agreement, but it should be developed with input from key partner states who can subsequently voluntarily pledge to adhere to the code of conduct.

In addition to behavior, a code of conduct can be used to standardize risk minimization across the Alliance. In this vein, NATO’s Standardization Office should be used to develop guidelines for digital supply chain issues like 5G or software investments. It is impossible for NATO and its members to scrutinize every piece of new technology, and formal accreditation or standardization is a slow and financially costly political decision. For instance, software is one of the largest attack surfaces of digital supply chains and is an important component of mission-critical systems. Although it will be nearly impossible to fully obtain compliance throughout the entire supply chain, NATO can introduce transparency and visibility with guidelines addressing suppliers, code authors, product components, and versions. The Standardization Office can produce recommended standards for vetting domestic vendors for quality and for screening foreign investments into digital infrastructure, intellectual property, and technology companies.

While collective defense will continue to be a necessary part of NATO’s approach to the cyber domain, the Alliance must incorporate resilience into a new Strategic Concept. ‘Fail-deadly’ and ‘fail-safe’ logics alone cannot address the myriad of challenges emanating from cyberspace. These recommendations offer potential avenues for the Alliance to implement the ‘safe-to-fail’ logic underpinning cyber resilience in a way that is shared and extends forward beyond NATO’s borders to its partners.

#### B—NATO action is critical to fostering effective national-level resilience strategies

Marovic, Politikon Executive Director, ‘19

[Jovana Marovic, Exeuctive Director, Politikon Network, “Wars of Ideas: Hybrid Warfare, Political Interference, and Disinformation,” NEW PERSPECTIVES ON SHARED SECURITY: NATO’S NEXT 70 YEARS, 11—28—19, https://carnegieeurope.eu/2019/11/28/wars-of-ideas-hybrid-warfare-political-interference-and-disinformation-pub-80419, accessed 4-25-22]

SHARE BEST PRACTICES

NATO provides a platform from which allies can work when coping with individual problems and vulnerabilities. The alliance can also help identify particular challenges, sometimes before the governments concerned do, and can play a role in early warning. This matters because rapid decisionmaking is sometimes the key to success in hybrid warfare.

THINK AND SPEAK COHERENTLY

NATO is meeting the hybrid challenge with twenty-nine member states experiencing very different sociopolitical realities and often using different concepts. A unified vocabulary and strategy would limit the misunderstanding of threats, improve collaboration, and make the sharing of lessons learned more effective—so would an agreement on the prioritization of tasks and responsibilities and a shared understanding of NATO’s role.

This would greatly help individual countries to build compatible and comparable national strategies. Many of these strategies, including that of the youngest member Montenegro, are in early stages of preparation, but divergences are already becoming evident. Those that have been completed—such as Slovenia’s 2018 regulation on cyber and information security or Croatia’s 2017 National Security Strategy, which partly deals with hybrid challenges—have largely opted for different approaches.

NATO member states must send a unified message inside and out. As strategic communication is a mind-set, it has to be built together carefully and fundamentally.12 NATO’s communication strategy should be a result of joint efforts and hence a common instrument against all threats, not just hybrid ones, at all levels.

#### [Optional] C—Resilience strategies enhance deterrence

Prior, Center for Security Studies researcher ‘18

[Tim Prior, Head, Risk and Resilience Research Team, Center for Security Studies (CSS) and PhD, Social and Environmental Psychology, University of Tasmania, “Resilience: The ‘Fifth Wave’ in the Evolution of Deterrence,” STRATEGIC TRENDS 2018: KEY DEVELOPMENTS IN GLOBAL AFFAIRS, Ed. O.Thränert & M/ Zapfe, Center for Security Studies, 2018, p. 77-78]

Resilience thinking and being resilient can offer concrete advantages in security policy, and specifically in deterrence. Applied resilience is becoming the cornerstone of security policy, and represents the fifth wave of deterrence.

Modern threats are complex, multiactor, cross-scale problems, which must be met with agile, resilience thinking-style institutional decisionmaking that fits the nature of the problems. Proactively countering complex threats with equally networked and distributed policy responses, guided by resilience, will improve the effectiveness of those security policies. In this context, the increasing resilience of society, critical infrastructure, and organizations – the product of a decade of resilience promotion in security policies – and the concomitant reductions in vulnerability will deter asymmetric threats by denying threatening actors suitable targets for their attacks.

Where classical (nuclear) deterrence was hierarchical and deterministic, based on the known relationships between the actors, and on the simple and well-understood principle of assured destruction, which held the actors in check, modern deterrence is altogether different. Threats are uncertain, and unpredictable; actors are unknown, as are the vulnerabilities they target. As threats have become less state-centered, and more likely to originate from distributed networks, the means of addressing these threats must also change.

The fifth wave of deterrence development is rising at a point when established international security practices are fumbling to respond effectively to security challenges. Resilience thinking presents a potential breakthrough that can increase the ability of established security institutions to improve their links and address complex threats deliberatively. If institutions can accept the current shift toward resilience as an important and practical one, then the “complex adaptive system” of international security is more likely to meet future system changes or disruption in a more prepared state. The fifth wave of deterrence will be characterized by the network-driven, tailor-made solution.

Deterrence is an uncertain art, not a science, and if the decision-making processes that determine deterrence actions do not match the problems, it is unlikely that practical deterrence solutions commensurate to modern threats can be identified and deployed.

Modern approaches to national and international security are already built on networks, but control tends to remain hierarchical and linear. Dealing with complex threats highlights the necessity to move away from traditional reductionist and hierarchical approaches to problem governance, and to engage existing networks with distributed and deliberative approaches.

To a certain degree, policy failures must be accepted as inevitable in a complex, uncertain, and unpredictable security environment. But policy failures will be more likely if policymaking processes are not suited to this current security environment. If policy processes are deterministic, reductionist, and hierarchical, then they are not suited to governing systems that are characterized by nonlinearity, unpredictability of interactions, and uncertain feedbacks. By contrast, if policy processes are designed to match the complex systems and problems they are attempting to govern – i.e., if they are flexible, reactive, and distributed – then they are likely to be more successful.

#### [Optional ] D—We should seize the moment and push resilience strategies—existing consultative frameworks solve

Hall & Sandeman, London School of Economics researchers, ‘22

[Jonny Hall, PhD Candidate, International Relations, London School of Economics and Political Science and Hugh Sandeman, Visiting Senior Fellow, LSE Ideas and Project Head of Global Strategies, “NATO’s Resilience: The First and Last Line of Defence,” Strategic Update, LSE IDEAS, 5—22, London School of Economics p. 11-13]

Policy Recommendations

NATO could resolve the tension between its collective responsibility for resilience and the continuing national responsibility among member states for implementing resilience measures by addressing resilience in the framework of deterrence and defence.

This aligns with the concept of deterrence used in the 2019 NATO Military Strategy and the 2020 Concept for the Deterrence and Defence of the Euro-Atlantic Area, which focuses less on crisis response and more on how deterrence can be used in persistent competition.33 The growing use of hostile measures short of war—which prompted the search for more sustained and wider resilience after 2014—has increased the importance of deterrence by denial.

Considering resilience within the context of deterrence will establish the overarching logic of NATO’s engagement with resilience issues and encourage the practicalities of moving towards “collective resilience”. As a form of deterrence, resilience policies will need to meet the three key criteria of all forms of deterrence: commitment, capability and communication.34

Commitment to strengthening resilience, already significantly enhanced among member states after the Russian invasion of Crimea, will be greatly strengthened by the war in Ukraine. It will be important for NATO and its members to take advantage of the political capital created by these developments and the COVID-19 pandemic in enacting costly resilience measures. NATO should therefore focus on four aspects of resilience rather than the broader seven baseline requirements. These are: continuity in energy and essential supplies; the security of the digital realm to ensure key socioeconomic functions; maintaining the independence of critical technologies beyond the control of adversaries; and the ability to detect and dispel disinformation.

In terms of capability, NATO should adopt a practical approach to helping the process of strengthening alliancewide resilience. Rather than trying to “establish, assess, review and monitor broad resilience objectives to guide nationally-developed resilience goals”, NATO should start the other way round. A similar approach to the NDPP, which consults with allies about their military plans, could be taken to encourage the harmonisation of member state and NATO objectives concerning resilience.

The NDPP identifies shortfalls in NATO capabilities before setting, assisting and reviewing the efforts of individual members to achieve country-specific targets aimed at resolving weaknesses and strengthening NATO’s defensive posture.35 As a process tailored for each member, “capability targets” are produced for each member according to the “political principles of fair burden-sharing”.36 Though this expectedly produces political tensions surrounding the issue of what is “fair”, it represents a more nuanced and realistic approach than the adoption of organisation-wide requirements. As argued above, it would still be advisable for NATO to set relatively few, clearly understandable goals that allow for the positive effects of peer competition, much like the success of the Defence Investment Pledge of 2014 in which members committed to spend at least 2 percent of Gross Domestic Product on defence and 20 percent of defence spending on major new equipment within a decade.37 Resisting the temptation to set numerous goals also helps bring clarity and focus to avoid potential gaps between rhetorical commitments and policy fulfilment.

Lastly, communication with both internal and external audiences will be essential to fostering resilience within NATO. The ability to demonstrate resilience to external audiences can serve as an effective deterrent against aggressive action. As with NATO’s annual military deterrence exercise,38 comprehensive preparation and regular exercises can play an important role in resilience measures by enhancing deterrence by denial. Exercises can get messages across to allies and domestic audiences.39 Societal and psychological resilience is also an essential complement to developing physical resilience capabilities. This was exemplified in 2018 by NATO partner Sweden’s delivery of a brochure to every household titled “If War or Crisis Comes”, which offered advice on what to do in events of power shortages or loss of internet access.40 The leaflet stated that “everyone who lives in Sweden shares a collective responsibility for our country’s security and safety”.41

One avenue for building societal resilience that could be explored by NATO members is working with creative industries to put across the need—and help create a narrative—for preparation for crisis events. Following precedents from the Cold War, in 2019 the French military employed science fiction writers to assist in conceptualising potential threats to national security.42 The same logic could be applied to getting the public to think about unfamiliar scenarios that may emerge in the contemporary and future security environment.

### Advantage One: The Alliance

#### A--Current policy leaves NATO vulnerable to *cyber attacks*—its deterrence posture faces multiple challenges, and defense is too fragmented

1—deterrence target limits

2—Article 5

3—response challenges

Blessing, American Enterprise Institute fellow, ‘22

[Jason Blessing, Visting Research Fellow, American Enterprise Institute and PhD, Political Science, Syracuse University, “Fail-Deadly, Fail-Safe, and Safe-to-Fail: The Strategic Necessity of Resilience in the Cyber Domain,” NATO 2030: TOWARDS A NEW STRATEGIC CONCEPT AND BEYOND, Ed. J.Blessing, K.KjellstromElgin, N.M.Ewers-Peters, School of Advanced International Studies, Johns Hopkins University, 2022, p. 266-273]

NATO’s Major Cyberspace Efforts to Date

Cyber defense first appeared on NATO’s political agenda at the 2002 Prague Summit, and Allies reaffirmed their commitment to securing the Alliance’s information systems at the 2006 Riga Summit. After Estonia’s 2007 cyber incident, NATO members had a greater urgency to address cyberspace challenges and, in January 2008, approved an initial Policy on Cyber Defense. With the release of the 2010 Strategic Concept, the North Atlantic Council (NAC) was tasked with formulating an in-depth cyber defense policy and implementation plan. By June 2011, a second Policy on Cyber Defense had been approved by Allied defense ministers. Cyber defense was incorporated into the NATO Defense Planning Process in 2012, and, as part of the Chicago Summit, Allies centralized and enhanced network defense under the NATO Computer Incident Response Team (NCIRC). Subsequently, NATO established the Communications and Information Agency (NCIA) in July of 2012 to house NCIRC.24 Only in 2014 at the Wales Summit did Allies formally acknowledge cyber defense as part of the collective defense task.25

Allies have taken several steps within the last five years to bolster NATO’s cyber posture. At the 2016 Warsaw Summit, member nations agreed that the Alliance would recognize cyberspace as an official military operating domain. The agreement also confirmed that NATO’s defensive mandate extended to cyberspace. This recognition built on developments from the 2014 Wales Summit, where Allies affirmed the applicability of both international law and Article 5 of the North Atlan- tic Treaty to cyberspace. The Warsaw Summit thus solidified the ability of member nations to invoke the Alliance’s collective defense provision in response to cyber incidents. Signaling their commitment to the Enhanced NATO Policy on Cyber Defense adopted at the Wales Summit,26 the Warsaw Summit also saw Allies agree to the Cyber Defense Pledge, a set of seven implementation points for improving national cyber defense capabilities.27 Shortly after the 2016 Warsaw Summit, NATO also issued a joint declaration with the European Union (EU) aimed in part at developing broader “coordination on cyber security and defence including in the context of…missions and operations, exercises and on education and training.”28 This expanded upon a previous NATO-EU Technical Arrangement on Cyber Defense, signed earlier in the same year to facilitate information sharing and best practices between respective emergency response teams.29

The 2018 Brussels Summit provided another important milestone. The resultant communiqué offered several public affirmations of the Alliance’s Cyberspace Roadmap, a private agreement made among defense ministers in February 2017 to develop the ability to conduct cyberspace operations and achieve mission assurance vis-à-vis the cyber domain.30 These affirmations included: identifying cyber defense as part of NATO’s collective defense efforts; signaling that Allies could volunteer sovereign cyber effects (i.e., effects produced by offensive capabilities) in service of NATO missions; and announcing the establishment of a Cyberspace Operations Centre (CyOC) in Belgium to provide situational awareness and coordinate operational activity.31 Secretary General Jens Stoltenberg also signed a new Joint Declaration on EU-NATO Cooperation that reinforced a commitment to cooperation in cyberspace.32

More recently, in 2019, the Alliance agreed to a general framework for integrating sovereign cyber effects and has released a preliminary draft of its Joint Allied Doctrine for Cyberspace Operations (as of January 2020). The latter provides the most comprehensive overview of NATO’s operation in cyberspace to date.33 Lastly, at the 2021 Brussels Summit, Allies endorsed the development of the Comprehensive Cyber Defense Policy to support the Alliance’s three core tasks and increase overall resilience.34

The Focus on Operationalizing Collective Defense

Much of NATO’s approach to the cyber domain has focused on developing collective defense frameworks. Although the Alliance has outlined a crisis management role for the NCIRC and advanced preliminary cooperative frameworks for malware disclosures and cyber intelligence sharing,35 operationalizing collective defense has taken priority. Article 5 considerations have been the foundation for NATO’s strategic approach to cyberspace, and there are three ‘fail-deadly’ scenarios in which Article 5 can be applied. First, an ally can invoke Article 5 in response to a cyberattack and the Alliance can respond using in-kind cyber operations as a within-domain retaliatory measure. Second, NATO can utilize cyber operations as a cross-domain retaliatory measure in response to a conventional attack that has triggered Article 5. Finally, the Alliance can utilize conventional military measures in response to a cyberattack on a member state that has subsequently invoked Article 5.

Operationalizing and implementing NATO’s ability to address such collective defense scenarios related to the cyber domain has required several organizational changes, the primary being the creation of the Cyber Operations Centre (CyOC) within ACO at the Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium. CyOC is the primary point for planning, coordinating, and executing NATO’s cyber operations. For each of these functions, CyOC must rely on Allies to volunteer operational intelligence. CyOC also provides situational awareness and interacts closely with the NCIA through the NCIRC for the ‘fail-safe’ protection of static networks and extended networks for operationally deployed forces. As with NATO’s geographic theater commands, the Director of CyOC reports to the Deputy Chief of Staff for Cyberspace, who provides strategic guidance to the Supreme Allied Commander Europe. Posts within CyOC are rotational and hinge on a bidding process to see which Allies will support which posts.36

NATO only conducts defensive cyber operations to secure its own networks and to support Allies and their networks when requested. The Alliance takes a restrictive view of defensive operations, excluding any active defense measures that might seek to disrupt an attack at its source outside of NATO’s own networks. Offensive cyber op- erations must necessarily be conducted by individual member states, though national-level offensive cyber operations can be integrated into NATO operations in two ways. First, member states may independently conduct an offensive cyber operation in support of NATO operations; this is less integrated and more loosely coordinated. Second, under the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) framework, an operational-level NATO commander may request an offensive cyber effect from allied nations. Unlike with conventional capabilities, authority over cyber capabilities is not directly handed over to NATO commanders. Instead, member states retain the capability, providing only the intended effect. In this way, individual member states maintain secrecy over the sources and methods of creating cyber effects. In these circumstances, CyOC is responsible for coordinating NATO commander requests and the individual member states providing effects. Only five member states have announced that they will make sovereign cyber effects available to the Alliance. These are: Denmark, Estonia, the Netherlands, the United Kingdom, and the United States.37

The Limits of Collective Defense in Cyberspace

There are, however, several dynamics that reveal the limits of the fail-deadly and fail-safe logics underlying NATO’s collective defense initiatives. In short, these strategic logics only apply to a narrow set of threats; they will not apply to the full spectrum of threats presented by the cyber domain. Fail-deadly deterrence is only likely to succeed in preventing state-level adversaries from undertaking resource-intensive cyber operations that reach the threshold of armed conflict with physical, destructive effects and that are quickly attributable.38 Fail-safe defensive measures also face several political and technical challenges, all of which point to a role for cyber resilience.

Three main complications limit the applicability of the fail-deadly logics underpinning collective defense efforts in cyberspace. The first is deciding which actors are to be deterred. Compared to traditional warfighting domains, there are relatively low entry costs for conducting operations in the cyber domain.39 As such, both state and non-state actors can target the Alliance. There are also asymmetric operational costs—actors are faced with multiple avenues for potential gains and few risks. This means that it will be near-impossible to change the decision calculus of a malicious actor deploying low-cost, low-risk techniques such as distributed denials of service. Conversely, sophisticated cyber operations that can produce strategic effects equivalent to those of conventional military attacks will have both significant and costly intelligence requirements that can only be borne by state actors. These higher ‘start-up’ costs mean it may be possible to change the decision calculus of actors seeking to conduct highly sophisticated cyber operations. Due to this asymmetry, only state actors undertaking costly cyber operations are likely to be deterred. In all other circumstances, deterrence will be more prone to failure.40

Attribution difficulties present further challenges to the ‘who’ of deterrence. Adversaries with rapidly changing tactics, techniques, and procedures—along with the ability to easily conceal an operation’s origin and perpetrator—can pose hurdles to technical attribution.41 Technical difficulties can weaken deterrent postures by delaying the timeliness of retaliatory punishment. Moreover, the effects of an operation that a defender notices may actually be second- or third-order effects. This can add additional time between attribution and punishment.42 The larger attribution issues, however, are political. NATO lacks common standards or guidance for attributing cyber operations in either a technical or political sense. Indeed, attribution remains a member state prerogative. Not only are the targeted member states responsible for attribution, but those members looking to contribute to collective defense must perform independent attribution assessments, and the political decision for a collective defense response must come from the NAC.43 Reaching a consensus decision to trigger collective defense in response to cyberspace operations is likely to be politically contentious, and member states will have few incentives to risk revealing the intelligence sources and methods that underlie attribution decisions. These dynamics are likely to intensify when additional links in the attribution chain are required, such as when a perpetrator is encouraged or sponsored by an adversarial state but lacks direct ties. Attribution is less likely to be politically controversial across the Alliance once a conventional conflict is underway as contextual clues from kinetic attacks can reduce uncertainty. This discussion points to a greater role for deterrence-by-denial. Deterring an adversary by taking measures to deny potential gains does not hinge on attribution and thus possesses a potentially wider scope of application.44

A second and related hurdle for cyber deterrence is determining which actions the Alliance seeks to deter. Much of the activity in cyberspace falls below the physical effects thresholds associated with the disruption, degradation, or destruction of computers and networks. Such considerations complicate decisions to invoke Article 5—specifically, the types of cyberattacks to which Article 5 should apply. Indeed, cyber operations targeting military assets or critical civilian infrastructure can be incredibly costly but may not reach damage levels associated with conventional attacks.45 Moreover, espionage via network exploitation is widespread, varied, and falls well below the threshold of armed conflict.46 Problematically, such exploitation can be nearly indistinguishable from operations that eventually seek to attack computers or networks and produce effects. Network exploitation can even be precursor to conventional military operations.47

Determining how to deter presents a third obstacle to NATO’s cyber deterrence efforts. Threatening conventional military means in response to cyber operations poses dilemmas of proportionality and can risk unintended escalation.48 Retaliation with cyber tools carry their own problems. First, the Alliance faces issues of political reliability, particularly in the context of the SCEPVA framework. Legally, Allies retain different constitutional restraints on offensive cyber operations that can hamper the ability to volunteer sovereign effects. Strategically, states may be hesitant to volunteer their ‘best’ cyber effects for fear of burning an exploit that could have had a greater payoff when used in a national context. Volunteering sovereign effects can also inadvertently give unwanted insight to an adversary regarding an Ally’s techniques, tactics, and procedures. Second, the temporary and transient nature of cyber capabilities makes it incredibly difficult to establish repeatable and predictable effects required of deterrent threats.49 Finally, signaling in cyberspace is generally ambiguous and rarely straightforward.50 For instance, an adversary may not even recognize a signal, believing it instead to be a technical glitch. Even if a costly signal is received, there is no way to ensure that it has interpreted as intended.

In addition to deterrence, NATO’s fail-safe cyber defense efforts face political and technical challenges. Because NATO will not undertake any active defense measures, actions to mitigate the effects of a cyberattack are limited to NATO networks or to individual member state networks when requested. This forecloses the possibility of developing an institutional strategy to mitigate the costs of a cyberattack upstream by disrupting the source of an attack, much like US Cyber Command does with its “defend forward” posture.51 More problematically, Allies have and will continue to have different legal, strategic, doctrinal, and threat frameworks for cyberspace that complicate defensive measures for the Alliance.

Most immediately this means that Allies will locate resources to different aspects of cyber defense based on individual country circumstances. Different strategic focuses have the potential to intensify disparate threat perceptions, capabilities, and skillsets. This can also exacerbate interoperability problems; for example, during an operation or crisis, some systems will be controlled by NATO while others will be controlled by an ally or a group of allies with different skill and knowledge levels. In the longer term, disparate legal understandings, particularly regarding sovereignty in cyberspace, will become more impactful as a greater number of allied nations develop forward defense strategies and the requisite capabilities for out-of-network operations. An out-of-network operation can in and of itself cause operational friction. However, differing definitions of sovereignty in cyberspace—and what violates it—inevitably create political friction between Allies as some look to operate and produce effects on other Allies’ networks.52 This political friction will contribute to even greater hesitancy over cyber-intelligence sharing and complicate the coordination of defensive mitigation measures across the Alliance.

Even if political barriers were removed, there are technical challenges to Allied implementation of fail-safe measures. Although there are conditions that can favor defense, such as the ability to manipulate the environment,53 offensive cyber operations can be both unpredictable and undetectable. Moreover, cyberspace presents a large and complex attack surface, where attacks can have unintended, cross-border effects. Given the sheer quantity of daily network probes experienced by NATO and individual member states, it is unlikely that every intrusion can be successfully countered or even identified. Highly sophisticated cyber operations are also likely to evade most defensive measures. Finally, fail-safe measures cannot effectively mitigate supply chain risks, as computers and systems increasingly rely on commercially available products and internationally based manufacturers. Defensive strategies will have limited utility if hardware or software components have been preloaded with malware.54 Each of these technical hurdles can contribute to slow-downs in decision-making, coordination, and response times for the Alliance while highlighting the need for greater resilience.

#### [Optional] B—The threat is large and growing—Ukraine proves the brink

Maigre, 2022

[Merle, senior cybersecurity expert at e-Governance Academy in Estonia. In 2017–2018, she served as director of the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE), “NATO IN A NEW ERA: GLOBAL SHIFTS, GLOBAL CHALLENGES NATO’s Role in Global Cyber Security” German Marshal Fund APRIL 06, 2022 <https://www.gmfus.org/news/natos-role-global-cyber-security> accessed jcp-TM 6/8]

Introduction

What the war in Ukraine says about cyber power is yet not entirely cleared from the fog of war. Many aspects remain uncertain, but given the unpredictability of the Putin regime, the risk of an escalation in hostile cyber exchanges between Russia and NATO states remains high. What is clear is that, as of February 24, 2022, we live in a different world in which the European and global security orders have been shattered.

This brief first explores the challenge that cyber threats pose to NATO allies and how the rapidly evolving cyber-threat landscape can alter the inter- national security environment. Secondly, it looks at developments in cyber defense policy within NATO. Finally, the brief analyzes how NATO needs to adapt to address cyber challenges, studying how allies align their sovereign interests, capabilities, and cyber doctrines with NATO operational requirements and strategic ambitions. NATO is set to issue strategic documents in 2022 that will guide the next decade of its military planning. This will certainly require more transatlantic consultation on political-military matters with an emphasis on cyber security and cyber defense.

The Cyber Challenge to the World and NATO Allies

Malicious cyber activity has increased substantially over the past years while the world has kept turning amid the omnipresent pandemic and now war in Ukraine. States, non-state actors, and criminal groups compete and are increasingly weaponizing sensitive information and infiltrating other countries’ networks to steal data, seed misinformation, or disrupt critical infrastructure.

The coronavirus pandemic further complicated the cyber-threat landscape. In March 2020, attempts to mitigate the spread of the coronavirus led to social distancing measures, travel restrictions, and remote work. In a short span of time, IT security profes- sionals had to respond to the challenges of working from home, such as enterprise data movements when employees accessed cloud-based apps via their home internet, corporate software, videoconferencing, and file sharing.1 Even if hardware and software solutions were in place to secure the organization’s data, there were often no established policies to help employees wade through the jungle of threats and vulnerabilities they faced when moving their workplace out of the traditional office environment.2

According to the FireEye Mandiant Special Report: M-Trends 2021, the top five most targeted indus- tries in 2020 were business and professional services, retail and hospitality, finance, healthcare, and high technology. The main methods used were extortion, ransom demands, payment card theft, and illicit trans- fers. Direct financial gain was the likely motive for 36% of intrusions, and an additional 2% of intrusions were likely perpetrated to resell access. In 2021, data theft remained an important mission objective for threat actors; in 32% of intrusions, adversaries stole data.3

Currently, highly organized, technically proficient criminal syndicates comprise the most significant cyber threat to allies. These groups try to steal data or extort money through ransomware. In 2021, promi- nent ransomware attacks struck Colonial Pipeline, the operator of the largest fuel pipeline on the East Coast of the United States; JBS, the largest meat processing company in North America; and Coop, a major supermarket chain in Sweden. Healthcare was also targeted—in May of the same year, the entire health service system of Ireland was disrupted for weeks, and over the spring and summer, dozens of hospitals in Europe and the United States were locked out of life-critical systems by ransomware attacks.4

Another set of threats comes in the form of bellig- erent state actors that seek to steal sensitive data for espionage. In December 2020, Russian intelligence services infiltrated the digital systems run by US tech firm SolarWinds and inserted malware into its code. During the company’s next software update, the virus was inadvertently spread to about 18,000 clients, including large corporations, the Pentagon, the State Department, Homeland Security, the Treasury, and other US government agencies. The hack went unde- tected for months before the victims discovered vast amounts of their data had been stolen.5

There are also politically motivated cyberattacks mandated by states that interfere in democratic processes and political discourse. In September 2020, the internal email system of Norway’s parliament was hacked.6 Ine Eriksen Søreide, the Minister of Foreign Affairs of Norway, underlined the significance of the attack by calling it an important cyber incident that affected the “most important democratic institution” of the country.7 Norwegian authorities later identified Russia as the actor responsible for the attack, marking the first time that Norwegian authorities had made a political attribution to such an attack.

Since the beginning of this year, Ukraine’s govern- ment has been hit by a series of cyberattacks that defaced government websites and wiped out the data on some government computers. In mid-Jan- uary, hackers defaced about 70 Ukrainian websites, including the Ministries of Foreign Affairs, Defense, Energy, Education, and Science, as well as the State Emergency Service and the Ministry of Digital Trans- formation, whose e-governance portal gives the Ukrainian public digital access to dozens of govern- ment services. The hackers replaced the home pages of about a dozen sites with a threatening message: “be afraid and expect worse.” After a couple of days,however, most of the sites were restored.8 The inter- national hacktivist collective Anonymous has declared “cyberwar” against Russia’s government, claiming credit for several cyber incidents including distrib- uted denial of service attacks that took down Russian government websites and Russia Today, the state- backed news service.9

Around the globe, aging critical infrastructure has long been vulnerable to attack.

The most worrying type of cyberattack is sophis- ticated malware designed by states or state-backed actors that act as “time bombs” in the critical cyber networks of target countries, such as the energy, telecom, and transportation sectors. Around the globe, aging critical infrastructure has long been vulnerable to attack. In 2020, the UK’s National Cyber Security Centre issued a warning of Russian attacks on millions of routers, firewalls, and devices used by infrastruc- ture operators and government agencies.10

On the day of the Russian invasion, ViaSat, a provider of high-speed satellite broadband services, was hacked along with one of its satellites Ka-Sat, whose users included Ukraine’s armed forces, police, and intelligence service. Destructive wiper malware attacks by Russia against Ukraine included Whisper- Gate, discovered in January by Microsoft, in Ukraine’s networks that “provide critical executive branch or emergency response functions”;11 HermeticWizard and IsaacWiper,12 targeting multiple Ukrainian orga- nizations just hours before the Russian invasion began; and CaddyWiper, spotted by researchers at the Slovak internet security company ESET in mid-March.13 All of them were designed to wipe or overwrite critical files on infected systems and leave computer hard drives corrupted and unrecoverable. These incidents demonstrate that, in the words of cyber expert and Silverado Policy Accelerator think tank chairman Dmitri Alperovich, “Cyberattacks have become a theater for great-power conflict in which governments and militaries fight in the hybrid ‘gray zone,’ where the boundaries between peace and war are blurred.”14 The actors navigate a complex web of ambiguous and deeply interconnected challenges, where cyberattacks are not a separate front, but rather an extension of the conflict.

#### C—This undermines alliance effectiveness for two reasons

#### 1—Unchecked attacks threaten alliance cohesion

Kramer et al., Scowcroft Center Distinguished Fellow, ‘20

[Franklin D. Kramer, Distinguished Fellow, Scowcroft Center for Strategy and Security and Board Director, the Atlantic Council, Lauren Speranza, Director, Transatlantic Defense and Security, Center for European Policy Analysis, and Conor Rodihan, Assistant Director, Transatlantic Security Initiative, Scowcroft Center for Strategy and Security, “NATO Needs Continuous Responses in Cyberspace,” NEW ATLANTICIST, The Atlantic Council, 12—9—20, <https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/>, accessed 5-23-22]

Russia and China challenge NATO and its members in cyberspace on a daily basis, as part of ongoing hybrid campaigns to undermine the transatlantic community. The Kremlin’s actions have involved intrusions into Allies’ critical infrastructures, manipulating Allies’ elections through hacks and disinformation, and even blocking GPS information critical to NATO activities. The Chinese government has engaged in cyber espionage against Allies’ military capabilities; intellectual property theft related to sensitive technologies, industries, and infrastructure; and disinformation against transatlantic countries, including around the coronavirus. These efforts to weaken NATO countries and Alliance cohesion represent a persistent threat to Allied security.

NATO has recognized the collective dangers of these hybrid attacks in cyberspace. Up to this point, however, the Alliance has taken a reactive approach, responding as if Russian and Chinese cyber attacks are each isolated incidents. But because Russian and Chinese cyber efforts are part of continuous campaigns directed at the overall capability of the Alliance, NATO’s response has been insufficient, failing to reduce or dissuade further attacks. To assure the security of its members going forward, NATO needs its own continuous response campaign to these threats.

#### 2—They also threaten NATO operations—facilitated by emerging vulnerabilities and the democratization of technology

Bellasio & Silfversten, RAND analysts, ‘20

[Jacopo Bellasio, Senior Analyst, Defence, Security and Infrastructure, RAND Europe and Erik Silfversten, Co-Director, Centre for Futures and Foresight Studies, RAND Europe, “The Impact of New and Emerging Technologies on the Cyber Threat Landscape and Their Implications for NATO,” CYBER THREATS AND NATO 2030: HORIZON SCANNING AND ANALYSIS, ed. A.Ertan, K.Floyd, P.Pernik & T.Stevens, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), King’s College London, and William & Mary University, 2020, p. 99]

The technologies highlighted in this paper may contribute to the exacerbation of current trends in the cyber threat landscape and herald so-called grey swan scenarios.5 The increasing availability of powerful, easy-to-use and inexpensive technologies is likely to further stimulate the conduct of malicious activities by a wide array of state and non-state actors. The democratisation and ‘servitisation’6 of technology have enabled consumer access to a wide range of technologies that were previously accessible only by governments. This includes enabling technologies like additive manufacturing and largescale distributed computing, to more niche technological services such as ondemand development of bespoke software-defined radio applications that could be used for disrupting the electromagnetic environment. While most of these activities are likely to entail low-tech tactics, this trend could result in an even greater volume of malicious activities than currently witnessed.

The development of new, complex technological solutions and capabilities may also enable state-sponsored actors to conduct advanced, covert or persistent attacks and activities which could undermine or jeopardise NATO’s missions and day-to-day operations by, for example, exploiting unknown vulnerabilities in the NATO supply chain to gain access to sensitive information. Sophisticated and persistent attacks are likely to be less frequent, making these threats more challenging for NATO to identify, detect, prepare for and manage due to limited exposure to and knowledge of the tactics, techniques and procedures (TTP) employed. The proliferation of connected and embedded systems, particularly through a drive towards the Internet of Things (IoT) and the digitalisation of legacy infrastructure may also increase NATO’s attack surface and the likelihood of vulnerabilities that could be exploited by malicious actors.

#### D— A strong NATO is the cornerstone of global stability

Burns, Harvard professor, ‘18

[Nicholas Burns, Barbara Goodman Family Professor of the Practice of Diplomacy and International Relations, Harvard Kennedy School, “Assessing the Value of the NATO Alliance,” Testimony before the Senate Foreign Relations Committee, 9—5—18, <https://www.belfercenter.org/publication/assessing-value-nato-alliance>, accessed 6-11-22]

Mr. Chairman and Mr. Menendez, you have asked for an assessment of NATO’s value to the United States. In my judgment, NATO continues to be of vital importance to American security interests in five principal ways. First, NATO is at the core of one of the most significant foreign policy accomplishments in American history—the creation of a long-term peace in Europe following the close of the Second World War. Because of NATO and the emergence of the European Union, Europe is united after centuries of division and war. NATO’s military strength has been a major reason for the absence of war with the Soviet Union and Russia since 1949. A recent Atlantic Council study reminds that America spent 14.1 percent of its GDP on defense during the First World War, 37.5 percent during the Second World War and 13.2 percent during the Korean Conflict. We spend nothing close to those levels now in large part due to the great power peace we have enjoyed for over seventy years. NATO has been a major factor in that peace. And due to the expansion of NATO and the European Union eastward after the fall of the Soviet Union, millions of East Europeans now live in free, democratic societies—a significant success for U.S. diplomacy. Second, NATO delivers additional benefits to U.S. military objectives and operations beyond our shores. NATO is at the heart of our defense of North America and Europe from nuclear and conventional threats. British and French nuclear weapons join ours in deterring aggression in the North Atlantic area. Since the late 1940s, every Administration has believed that the best way to defend our country is through American forces forward deployed in Europe with the NATO allies. This strategy remains right for today given Russia’s invasion of Georgia in 2008, of Crimea and Eastern Ukraine in 2014 and its current pressure on Estonia, Latvia, Lithuania and Poland. NATO remains our primary vehicle for deterring Putin in Eastern Europe. The NATO allies host a great number of critical bases for U.S. forces—Ramstein in Germany, Aviano in Italy, Rota in Spain, Souda Bay in Greece and Incirlik in Turkey—that serve as a platform for our presence in Europe, as well as for U.S. force projection against terrorist groups in North Africa and the Middle East and for our continued military operations in Afghanistan. Europe is a critical link in the development of our Ballistic Missile Defense network focused on the Middle East with Turkey, Romania, Poland, Germany, Spain, the Netherlands, Denmark, the UK and other allies all hosting elements of this system. NATO allies continue to participate in the U.S.-led coalition against the Islamic State in the Middle East. Many of the allies play lead roles in other counter terror operations such as French forces in Mali supported by the U.S. In Afghanistan, the NATO allies remain with us in combat operations and in training the Afghan military. Over 1000 soldiers from European and other partner nations have died there during the last seventeen years. NATO continues to maintain the hard-earned peace in Kosovo with European troops bearing the large share of the burden. An EU-led force has taken on all of the peacekeeping responsibility in Bosnia, freeing up the U.S. for other activities. Third, the NATO allies are among our closest and most supportive global partners as we confront the great transnational challenges that define this century—the fight against terrorism, the entire complex of cyber threats, climate change, the risk of pandemics, mass migration and others. The NATO allies and our partners in the European Union act together with us on these and other issues. This is of incalculable benefit to the U.S. Neither Russia nor China have treaty allies. NATO is a significant advantage for the United States when it acts as a force multiplier for American interests.

#### [Optional] E—Independently, cyberattacks risk nuclear escalation—C3I entanglement

Afina et al., Chatham House analyst, ‘20

[Yasmin Afina, Research Assistant, ISP, Calum Inverarity, Research Analyst, ISP, and Beyza Unal, Research Fellow, International Security Program, Chatham House, “Ensuring Cyber Resilience in NATO’s Command, Control and Communication Systems,” Chatham House, Royal Institute of International Affairs, 7—20, p. 2]

Note: C3I = command, control, communications, and intelligence

Summary

 NATO’s nuclear capability is provided by the US and the UK. The modernization of systems and arsenals held by both states is proceeding apace. This has involved – and continues to involve – the integration and use of increasingly sophisticated new technologies within their nuclear programmes, including in their respective command, control and communication (C3) systems.

 Cyber operations targeting NATO members’ C3 systems and their assets, including nuclear assets, are also increasingly sophisticated in nature. While cybersecurity is a serious concern, and there is acknowledgment of the potential magnitude of cyberattacks, documentation available in the public domain indicates the need for NATO and its members to put in place further measures to ensure the cybersecurity of C3 systems, including those of nuclear systems (NC3). This is all the more pertinent given that some Allies’ military capabilities still include legacy systems from the Soviet era.

 The protection of C3 systems requires the adoption of adequate, adaptable and robust cybersecurity measures, in order to ensure the integrity of these systems and to shield them from both internal and external disruption. The following five considerations are of relevance for the protection of NATO’s own C3 systems, and those of its member states: software and network protection; data (integrity) protection; hardware protection; access/security controls; and cybersecurity awareness/security by design. These attest to the need for robust measures beyond the non-kinetic, digital realm to ensure the cybersecurity of NATO’s C3 ecosystem.

 The increasing reliance on C3 assets that may be used for both conventional and nuclear operations raises the prospect of entanglement, and the associated risk of rapid escalation. The potential for unintended escalation is further exacerbated by the threat of cyberattacks and possible new threats emanating from other emerging technologies, including quantum computing. Unknown and unanticipated effects from cyber operations targeted at C3 assets may compromise the legality of these attacks when such assets may be of both military and civilian use simultaneously.

 Measures to prevent misinterpretation and rapid escalation are critical to the security of C3 systems. Such measures could include a clearer understanding of: how adversaries think about command and control; what would constitute a cyberattack in the context of C3 systems; and what would constitute adequate responses to such attacks within the frameworks of international law – particularly international humanitarian law.

 False confidence and false stress are equally problematic. In addition to ensuring the cybersecurity of their existing nuclear planning and NC3 architecture, NATO and Allies must reflect on how these dynamics will affect current understanding, arrangements and strategies surrounding the concept of nuclear sharing. Concerns over legacy infrastructure, in the context of an evolving threat landscape and the modernization of systems with digital means, raise questions with regard to the way forward for the hosting of US nuclear weapons in Europe, as well as for existing nuclear burden sharing agreements.

#### F—The plan solves—incorporating safe-to-fail principles decreases cyber risks and addresses current policy failures

Blessing, American Enterprise Institute fellow, ‘22

[Jason Blessing, Visting Research Fellow, American Enterprise Institute and PhD, Political Science, Syracuse University, “Fail-Deadly, Fail-Safe, and Safe-to-Fail: The Strategic Necessity of Resilience in the Cyber Domain,” NATO 2030: TOWARDS A NEW STRATEGIC CONCEPT AND BEYOND, Ed. J.Blessing, K.KjellstromElgin, N.M.Ewers-Peters, School of Advanced International Studies, Johns Hopkins University, 2022, p. 261-264]

The last several years have seen calls for NATO to embrace strategic resilience, and the COVID-19 pandemic has both amplified and accelerated debates surrounding resilience. One recommendation that has emerged is that NATO should adopt “comprehensive resilience” as a fourth core task alongside the three existing tasks of collective defense, crisis management, and cooperative security laid out in the 2010 Strategic Concept. Resilience has generally referred to the ability to “anticipate, prevent, and…protect against and bounce forward from disruptions to restore critical functions.”1 Comprehensive resilience is thus meant to address a range of challenges facing the Alliance and is necessarily a shared endeavor that can be projected forward outside the membership bounds of NATO.2 This chapter addresses one dimension of comprehensive resilience by highlighting the Alliance’s cybersecurity challenges and the strategic necessity of resilience in the cyber domain.

The COVID-19 pandemic has highlighted that cybersecurity encompasses more than “cyber war”3 by underscoring the reliance of nations and their economies on cyberspace and digital infrastructures. Massive migrations to online services have occurred with the transition to remote telework and education, among other vital societal activities. NATO itself has been no exception, as the Alliance worked to facilitate remote work by shipping critical communication and information systems items to NATO Communications and Information Agency (NCIA) support teams across various countries. This effort included simultaneously shipping laptops from its Headquarters in Belgium to Allied Command Transformation (ACT) in Virginia, United States and shuttling devices across European borders to Mons, Belgium to ensure business continuity for Allied Command Operations (ACO).4 Pandemic-induced shifts into business and operational continuity plans have thus brought to the forefront security issues like threats to digital supply chains, which have become even more salient in the wake of the SolarWinds hack.5 Recent high-profile ransomware attacks against US companies Colonial Pipeline and JBS Foods have only intensified the need to secure supply chains from digital threats.6

Concomitantly, broader questions have arisen about NATO’s strategic approach to cyberspace. The most recent Strategic Concept, released in the wake of the 2010 Lisbon Summit, provides few clues as to how collective defense, crisis management, and cooperative security relate to cyberspace. In fact, the document only mentions the word “cyber” five times.7 An urgency to reconsider NATO’s efforts in the cyber domain has been evidenced by recommendations from the NATO 2030 Reflection Group, which devoted an entire sub-section of its report to hybrid and cyber threats. In particular, the Reflection Group highlighted the need to develop both greater collective defense capacity in cyberspace and a more robust consultation framework to facilitate collective defense, crisis management, and cooperative security in the domain.8 These concerns were largely echoed by Allies in the recent 2021 Brussels Summit Communiqué.9

This chapter argues that for NATO to effectively address the broad range of security challenges emanating from the cyber domain, the Alliance must complement its current collective defense efforts by incorporating resilience and “safe-to-fail” principles into a new Strategic Concept. The unique dynamics of cyberspace mean that resilience must be a shared effort among members, and it must be projected outside the Alliance’s borders. This chapter therefore recommends that NATO adopt a fourth core task of comprehensive resilience that includes shared and forward cyber resilience as a major component. While NATO has thus far prioritized the operationalization of collective defense in cyberspace, the strategic logics that underpin collective defense will not apply to the full spectrum of threats presented by the domain. Part of the challenge, then, is to reframe the Alliance’s cyber security conversations to acknowledge the limits of collective defense.

NATO’s ongoing efforts to operationalize collective defense have relied primarily on ‘fail-deadly’ and ‘fail-safe’ logics. On the one hand, the Alliance has drawn on deterrence principles in attempts to discourage and prevent adversarial actions in and through cyberspace through the imposition of costs that would outweigh potential gains.10 While denial strategies are vital to cost imposition, deterrence-by-punishment has been the strategic bedrock of NATO’s recent initiatives. The threat of retaliatory punishment is traditionally a ‘fail-deadly’ strategy: should an adversary undertake an undesired action, i.e., deterrence fails, the Alliance responds with the use of deadly force. On the other hand, NATO has also focused on implementing defensive measures to minimize the damage and fallout from an attack in or through cyberspace. Such a ‘fail-safe’ strategy seeks to ensure that, should deterrence fail, the Alliance and its members retain the ability (albeit degraded) to operate safely and securely in the cyber domain.

Combined, fail-deadly and fail-safe strategies look to prevent and mitigate of the costs of adversarial actions in the cyber domain. In contrast, resilience in cyberspace—the ability to anticipate, withstand, recover from, and adapt to strategic shocks or surprises occurring in or through the cyber domain11—emphasizes passive protection, risk-minimization, and forward-looking continuity-of-operations efforts.12 Unlike NATO’s current approach to collective defense, resilience rests on ‘safe-to-fail’ principles. As a ‘safe-to-fail strategy,’ resilience is built on the assumption that, despite deterrent and defensive measures, the Alliance may fail to foresee adverse strategic disruptions that remove the ability to operate and coordinate in the cyber domacain. To withstand and bounce forward from such disruptions, NATO must ensure that military cyber functions and capabilities fail safely—that is, to fail in ways that do not remove the ability to recover at or above original operating capacity. Resilience thus offers a way for the Alliance to account for a variety of threats and scenarios to which fail-deadly and fail-safe strategies prove ineffective. At the same time, resilience serves to enhance collective defense in the cyber domain: collective defense is more credible if the Alliance is more resilient.

This chapter proceeds in the following sections. The first describes the cyber threats facing the Alliance. The second section outlines NATO’s policy and organizational developments related to cyberspace. The third section discusses the limitations of collective defense; in short, collective defense efforts are best suited for countering the small subset of cyber incidents that reach damage levels analogous to conventional uses of force. The fifth section explores what cyber resilience looks like for NATO and why it must be a shared phenomenon that is projected forward outside the Alliance. The chapter concludes with several recommendations for the Alliance as it looks ahead to 2030 and beyond.

### Advantage Two: Russia

#### A—Russia is pursuing a hybrid warfare strategy to weaken the alliance and undermine the U.S.-led international order

Speranza, Center for European Policy Analysis director, ‘20

[Lauren Speranza, Director, Trans-Atlantic Defense and Security, Center for European Policy Analysis, “A Strategic Concept for Countering Russian and Chinese Hybrid Threats,” Scowcroft Center for Strategy and Security, Atlantic Council, 7—20, p. 13-15]

For Russia, hybrid warfare is a set of means for it to roll back the post-Cold War settlement and undermine the predominantly US-led, rules-based international order to regain clout as a major player on the global stage. The Kremlin’s key objectives to that end include: dividing and weakening NATO and the EU, both of which the Kremlin sees as a threat; subverting pro-Western governments and institutions; promoting pro-Russia policies; expanding Russia’s sphere of influence (geographically, economically, politically, etc.); and establishing a “moral equivalence” between Russia and the West.3 Moreover, hybrid activities help the Kremlin pursue these goals in a more effective and realistic way. Its leaders recognize Russia cannot necessarily counter or outright compete with the West militarily, technologically, or economically. By employing hybrid methods as part of an overarching strategy of intimidation, however, the Kremlin can have significant influence over international affairs.4

Russia’s hybrid toolkit is multi-level and often country specific, which has made it highly effective and difficult to combat. In its most widely known example, Russia used below-threshold force to illegally invade eastern Ukraine and annex Crimea. The Kremlin has also used proxies and privately contracted forces to influence the outcome of conflicts abroad, from Syria to Libya. Other examples of Russia’s low-level uses of force include attempted assassinations of pro-Western leaders and the use of deadly chemical attacks to target political enemies on foreign soil. In terms of cyber and operational activities, Russia has conducted reckless and dangerous cyberattacks, infiltrated critical infrastructure in the United States, and manipulated gas pipelines, electric grids, and financial systems in Eastern Europe and beyond to increase its leverage abroad.

With respect to political subversion and economic coercion, Russia has interfered in elections in the United States and across Europe in attempts to divide transatlantic populations and influence the outcomes toward candidates the Kremlin views as favorable to Russia. Other tools and tactics include: bribing officials in foreign countries; financing anti-European parties in Central and Eastern Europe to promote pro-Russian narratives; and investing in strategic sectors in foreign countries to maximize dependency on Russia. On the information-warfare front, the Kremlin has orchestrated widespread disinformation campaigns and strategic hack-and-release efforts designed to sow doubt, create chaos, and sway public opinion in its favor on key policy issues.

While Russian hybrid activities can be traced much further back than these examples—including to the major cyberattacks in Estonia in 2007 and the Russo-Georgia conflict in 2008—they have been steadily increasing since the Kremlin’s illegal annexation of Crimea in 2014. Looking ahead, several elements could impact the future course of Russia’s hybrid actions. First are the constitutional changes that Russian President Vladimir Putin has pushed through national courts to reset presidential term limits.5 The reforms allow Putin to remain in power until 2036, or possibly for life, pending a final national referendum.6 With his grip on power soon to be cemented, Putin is likely to attempt more aggressive hybrid actions, knowing the domestic political risks for him are low.

Another factor is the 2020 coronavirus pandemic, which has triggered a global recession and a drastic decline in demand for oil so critical to Russia’s energy-reliant economy. In early 2020, Russia and Saudi Arabia, the world’s biggest crude producers, failed to agree to mutual production cuts in response to the crisis, fueling a price war that further hurt Russia’s economy.7 Economic, public health, and social pressures inside Russia could push the Kremlin to temporarily scale back its ambitions in the short term. However, at the same time, uncertainty and anxiety around the pandemic could create more fertile conditions for Russia’s hybrid activities beyond its borders, especially as Euro-Atlantic governments take extraordinary domestic measures to respond.8 In the long term—even as the pandemic subsides, oil prices rebound, and the global economy begins to recover—conditions will remain difficult for Russia, whose economy has suffered from stagnation and sanctions from the West. These dynamics may lead Putin to be more assertive with hybrid strategies abroad with the aim of appealing to nationalist sentiments at home in order to quell domestic political tensions.

Further emboldening Putin is the lack of traditional US leadership and pushback that has helped to keep Russia in check. US President Donald Trump has instead tried to appeal to Putin, describing his own policy as “getting along with Russia” and reducing perceived or actual consequences of hybrid actions against the United States. Political allegations of the Trump campaign “colluding” with Russia to affect US elections9 have further divided the American public toward Russian aims, creating more fertile ground for the Kremlin’s malign influence.10 Compounding this is fraying transatlantic solidarity, whether the USGermany feud over defense spending or French President Macron’s comments that NATO is “braindead.”11 These divisions not only constrain the West’s response to Russia’s hybrid actions, but also expose cracks in the Alliance that Putin is all too eager to exploit.

Together, these factors indicate that as long as Putin remains in power, the Kremlin will likely continue escalating hybrid activities, short of an all-out war with NATO, to push boundaries and test what is acceptable going forward. In the relative near term, the transatlantic community must plan according to Russia’s current trajectory on hybrid issues, which demands a more proactive and widespread approach.

#### B—This risks nuclear escalation—strong incentives for Russia and NATO

Kulesa, European Leadership Network Research Director, ‘18

[Lukasz Kulesa, Research Director, European Leadership Network, “Envisioning a Russia-NATO Conflict: Implications for Deterrence Stability,” EURO-ATLANTIC SECURITY REPORT, 2—18, p. 5-8]

“Hybrid” scenarios: trigger for conflict?

One can envisage a number of “hybrid” scenarios of Russia-NATO conflict where operations which started in the cyber, economic, criminal, or “active measure” domains, below the threshold of conflict, trigger a military response or are followed by the physical use of force. As noted in the discussion on the definitions of a conflict, the threshold between crisis and military conflict may not be explicitly stated or otherwise clear to all sides; and it may also be ignored during a crisis. This aspect is especially relevant in the current period of increased interference in the internal affairs of NATO countries attributed to Russia and of the high volume of information ‘warfare’ between Russia and NATO countries.

Russia remains vigilant about foreign interference in its internal affairs and the threat of subversion leading to a severe destabilization of the regime. In the past, Moscow has made accusations about foreign sponsorship of Chechen and radical Islamic terrorists targeting Russia, and has alleged the existence of training camps on the territories of NATO states for activists planning colour revolutions in Ukraine and Belarus. In the extreme circumstances of a crisis, if the Russian leadership became convinced that a non-military campaign against it (which might also involve cyber activities and what Russia calls attempts to instigate colour revolutions) had intensified, this could lead to a military response.

With regards to NATO, some of its members’ views mirror the Russian assessment that we are already in a state of conflict, in which the boundary between peace and war is blurred, and that their defences are being actively attacked through nonmilitary means. They are thus concerned about a scenario in which Russia initiates an attack that moves swiftly from non-military to military means. This scenario should be not dismissed. At the same time, one needs to be wary of interpreting all disturbing developments as part of a grand Russian plan culminating in a provocation or use of force. So there should be prudence before any country presses the “panic button” at the national or NATO / European Union level. There should also be close analysis of early warning indicators related to the gravity, intensity and diversity of incidents and to connections between them. The overall political context and state of the RussiaNATO relationship would also be important: what would be the political and strategic reasons for Russia to move from sub-threshold to abovethreshold activities?

Individual NATO countries would have a decisive role in how some of the “hybrid” scenarios would play out. An Ally can choose to play down or up the importance of certain developments and incidents; it can seek NATO and/or EU support, decide to respond individually (including through actions that are escalatory), or use a mix of both approaches. The Ally’s overall reputation and patterns of international behaviour can matter for determining whether its “frontline” intelligence and assessments are to be trusted. But given the danger of alliance entrapment, NATO also needs to have multiple channels for corroborating the evidence and assessing developments.

Escalation: Can a NATO – Russia conflict be managed?

Once a conflict was under way, the “fog of war” and rising unpredictability would inevitably set in, complicating the implementation of any predetermined theories of escalation, deescalation and inter-conflict management. The actual dynamics of a conflict and the perceptions of the stakes involved are extremely difficult to predict. Simulations and table-top exercises can give only limited insights into the actual decisionmaking processes and interactions.

Still, Russian military theorists and practitioners seem to assume that a conflict with NATO can be managed and controlled in a way that would bring it to a swift end consistent with Russian aims. The Russian theory of victory would seek to exploit weak points in an Alliance war effort. Based on the conviction that democracies are weak and their leaders and populations are risk-averse, Russia may assume that its threats of horizontal or vertical escalation could be particularly effective. It would also try to bring home the notion that it has much higher stakes in the conflict (regime survival) than a majority of the NATO members involved, and thus will be ready to push the boundaries of the conflict further. It would most likely try to test and exploit potential divisions within the Alliance, combining selective diplomacy and activation of its intelligence assets in some NATO states with a degree of selectivity in terms of targets of particular attacks.

Any NATO-Russia conflict would inevitably have a nuclear dimension. The role of nuclear weapons as a tool for escalation control for Russia has been thoroughly debated by experts, but when and how Russia might use (and not merely showcase or activate) nuclear weapons in a conflict remains an open question. Beyond catch phrases such as “escalate to de-escalate” or “escalate to win” there are a wider range of options for Russian nuclear weapon use. For example, a single nuclear warning shot could be lethal or non-lethal. It could be directed against a purely military target or a military-civilian one. Detonation could be configured for an EMP effect. A “false flag” attack is also conceivable. These options might be used to signal escalation and could significantly complicate NATO’s responses.

Neither NATO nor its member states have developed a similar theory of victory. Public NATO documents stipulate the general goals for the Alliance: defend against any armed attack and, as needed, restore the full sovereignty and territorial integrity of member states. It is less clear how far the Alliance would be willing to escalate the conflict to achieve these goals, and what mechanisms and means it would use while trying to maintain some degree of control over the conflict.

The goals and methods of waging a conflict with Russia would probably have to be limited in order to avoid a massive nuclear exchange. Such limitations would also involve restrictions on striking back against targets on Russian territory. But too narrow an approach could put too much restraint on NATO’s operations: the Russian regime’s stability may ultimately need to be threatened in order to force the leadership into terminating the conflict. NATO would thus need to establish what a proportional self-defence response to Russian actions would involve, and to what extent cyber operations or attacks against military targets in quite different parts of Russia would be useful as tools of escalation to signal NATO’s resolve. Moreover, individual NATO Allies, especially those directly affected by Russia’s actions, might pursue their individual strategies of escalation.

With regards to the nuclear dimension in NATO escalation plans, given the stakes involved, this element would most likely be handled by the three nuclear-weapon members of the Alliance, with the US taking the lead. The existence of three independent centres of nuclear decision-making could be exploited to complicate Russian planning and introduce uncertainty into the Russian strategic calculus, but some degree of “P3” dialogue and coordination would be beneficial. This coordination would not necessarily focus on nuclear targeting, but rather on designing coordinated operations to demonstrate resolve in order to keep the conflict below the nuclear threshold, or bring it back under the threshold after first use.

Relying on concepts of escalation control and on lessons from the Cold War confrontation might be misleading. The circumstances in which a Russia -NATO conflict would play out would be radically different from the 20th century screenplay. Moreover, instead of gradual (linear) escalation or salami tactics escalation, it is possible to imagine surprizing “leap frog” escalation, possibly connected with actions in different domains (e.g. a cyberattack against critical infrastructure). Flexibility, good intelligence and inventiveness in responding to such developments would be crucial.

Conflict termination

Russian and NATO assumptions regarding conflict termination would most likely not survive the first hours of an actual conflict. Both sides are capable of underestimating the resolve of the other side to prevail in a conflict and the other side’s willingness to commit the necessary resources and endure the costs, especially once both sides start committing their political capital and resources and the casualties accumulate.

With regards to Russia, Moscow would most likely be approaching the conflict with a clearer concept of its war aims and thus develop better-formed views on conflict termination. It would seek to establish escalation dominance and confront NATO with a binary choice of either accepting defeat or further intensification of fighting. Such intensification might involve a move to the nuclear level, but Russia would also have conventional escalation options, such as conventional deep strikes.

At the same time, it should be highlighted that Russia is unlikely to start a conflict which involves a high degree of uncertainty about its final outcome and carries a risk of military defeat. Russia cannot safely assume that US-led NATO would act with restraint, nor could it be sure that the Alliance would be ready to surrender and terminate a conflict early. For internal reasons Russia cannot afford to lose a “big war”, so the most prudent option would generally be not to initiate such a conflict in the first place. Such logic could, however, get lost in some of the hybrid scenarios and scenarios of an inadvertent outbreak of a conflict.

On the NATO side, conflict termination has not been the focus of close attention, as the Alliance has concentrated in recent years on strengthening deterrence and probing the issue of defence. As one of the workshop participants put it, “NATO is in the deterring Russia business not in the winning a war with Russia business”. This is not a new problem. War termination proved to be a difficult subject for the Alliance in the Cold War, as it involved delicate questions about maintaining NATO’s political cohesion and dealing with the consequences of major nuclear exchanges. Nevertheless, NATO’s ability to persevere in a conflict should not be underestimated. Opinions that NATO would collapse following a Russian first strike seem to be based more on stereotypes about the weakness of Western democracies than on any insight into how Alliances actually operate during wartime, especially when fighting a defensive war that is perceived as just. Still, it may be assumed that NATO would have major difficulty in setting and implementing any conflict termination strategy based on the intensification of military pressure on Russia, especially beyond the immediate theatre of operations. Individual Allies, first and foremost the US, might have to take a lead in that.

#### [Optional] C--The liberal order stops great power wars—collapse risks competing blocks and undermine collective action needed to address existential risks

Beckley, Tufts University professor, ‘20

[Michael Beckley, Associate Professor, Political Science, Tufts University, “Rogue Superpower: Why This Could Be an Illiberal American Century,” FOREIGN AFFAIRS v. 99 n. 6, November / December 2020, Ebsco]

What would happen to the world if the United States fully embraced this kind of “America first” vision? Some analysts paint catastrophic pictures. Robert Kagan foresees a return to the despotism, protectionism, and strife of the 1930s, with China and Russia reprising the roles of imperial Japan and Nazi Germany. Peter Zeihan predicts a violent scramble for security and resources, in which Russia invades its neighbors and East Asia descends into naval warfare. These forecasts may be extreme, but they reflect an essential truth: the postwar order, although flawed and incomplete in many ways, has fostered the most peaceful and prosperous period in human history, and its absence would make the world a more dangerous place.

Thanks to the U.S.-led order, for decades, most countries have not had to fight for market access, guard their supply chains, or even seriously defend their borders. The U.S. Navy has kept international waterways open, the U.S. market has provided reliable consumer demand and capital for dozens of countries, and U.S. security guarantees have covered nearly 70 nations. Such assurances have benefited everyone: not just Washington’s allies and partners but also its adversaries. U.S. security guarantees had the effect of neutering Germany and Japan, the main regional rivals of Russia and China, respectively. In turn, Moscow and Beijing could focus on forging ties with the rest of the world rather than fighting their historical enemies. Without U.S. patronage and protection, countries would have to get back in the business of securing themselves and their economic lifelines.

Such a world would see the return of great-power mercantilism and new forms of imperialism. Powerful countries would once again try to reduce their economic insecurity by establishing exclusive economic zones, where their firms could enjoy cheap and secure access to raw materials and large captive consumer markets. Today, China is already starting to do this with its Belt and Road Initiative, a network of infrastructure projects around the world; its “Made in China 2025” policy, to stimulate domestic production and consumption; and its attempts to create a closed-off, parallel Internet. If the United States follows suit, other countries will have to attach themselves to an American or a Chinese bloc—or forge blocs of their own. France might seek to restore its grip on its former African colonies. Russia might accelerate its efforts to corral former Soviet states into a regional trade union. Germany increasingly would have to look beyond Europe’s shrinking populations to find buyers for its exports—and it would have to develop the military capacity to secure those new far-flung markets and supply lines, too.

As great powers competed for economic spheres, global governance would erode. Geopolitical conflict would paralyze the UN, as was the case during the Cold War. NATO might dissolve as the United States cherry-picked partners. And the unraveling of the U.S. security blanket over Europe could mean the end of the European Union, too, which already suffers from deep divisions. The few arms control treaties that remain in force today might fall by the wayside as countries militarized to defend themselves. Efforts to combat transnational problems—such as climate change, financial crises, or pandemics—would mimic the world’s shambolic response to COVID-19, when countries hoarded supplies, the World Health Organization parroted Chinese misinformation, and the United States withdrew into itself.

The resulting disorder would jeopardize the very survival of some states. Since 1945, the number of countries in the world has tripled, from 46 to nearly 200. Most of these new states, however, are weak and lack energy, resources, food, domestic markets, advanced technology, military power, or defensible borders. According to research by the political scientist Arjun Chowdhury, two-thirds of all countries today cannot provide basic services to their people without international help. In short, most countries depend critically on the postwar order, which has offered historically unprecedented access to international aid, markets, shipping, and protection. Without such support, some countries would collapse or be conquered. Fragile, aid-dependent states such as Afghanistan, Haiti, and Liberia are only some of the most obvious high-risk cases. Less obvious ones are capable but trade-dependent countries such as Saudi Arabia, Singapore, and South Korea, whose economic systems would struggle to function in a world of closed markets and militarized sea-lanes.

#### [Optional] D-- Misinformation is an existential threat—makes it impossible to solve the many challenges facing us

Lin, CISC Senior Research Scholar, ’19

[Herbert Lin, Senior Research Scholar, Center for International Security and Cooperation and Fellow, Hoover Institution, Stanford University, “The Existential Threat from Cyber-Enabled Information Warfare,” BULLETIN OF THE ATOMIC SCIENTISTS v. 75 n. 4, 2019, p. 189-194]

Corruption of the information ecosystem has become an existential threat to civilization as we know it because prosperity and advancement depend on a secure information infrastructure and environment that provides human beings with contextualized, reliable, trustworthy information when and where it is needed. Information is as much a part of human ecology and the essence of being human as DNA (itself a form of information!) is a part of the evolutionary processes in biological systems.

Today, chaos reigns in much of the information ecosystem on which societies depend. In many forums for political and societal discourse, national leaders shout about fake news, by which they mean information they do not like. These same leaders lie shamelessly, calling their lies truth, or perhaps “truthful hyperbole.” Acting across national boundaries, these leaders and their surrogates exacerbate existing divisions, creating rage and diminishing confidence in elections and democratic institutions. Using unsupported anecdotes and sketchy rhetoric, denialists undermine well-established science about climate change and other urgent issues. Established institutions of the government, journalism, and education – institutions that have traditionally provided stability – are under attack precisely because they have provided stability.

The founding of the Bulletin predates by several decades the widespread availability of computers, the Internet, smart phones, search engines, and social media. Few could imagine in 1945 a technological environment that affords today’s high-speed and widespread connectivity, high degrees of anonymity, insensitivity to distance and national borders, easy and customized information searches, democratized access to publishing capabilities, inexpensive production and consumption of information content (including and increasingly importantly emotionally evocative video and audio content), disintermediation of established information sources, and ubiquitous, always-on, always-available access to information sources through mobile devices.

Such advances in information technology have heralded the arrival of the information age, a world in which taking near-immediate advantage of information opens up enormous opportunities in both the private and public sectors for improved delivery of existing products and services and, perhaps more important, the creation of entirely new products and services. Products and services can be customized to individual needs and preferences on a large scale and at more affordable costs. Transactional friction can be tremendously reduced. Through the Internet of Things, actuators and sensors can be connected to process control computers to optimize the behavior and function of physical systems. Everywhere that information can be used to create and improve new and existing functionality (that is, essentially everywhere), one can find or imagine new information technologies to do so.

At the same time, advances in information technology have a dark side. The same increases in the volume and velocity of information have created a louder and more chaotic information environment that stimulates fast, angry, reflexive, intuitive, and visceral thinking, reaction, and action in people and thus displaces more complex, reflective, and rational thought. In a chaotic environment of information overload, people are more likely to use mental shortcuts as a way to reduce the cognitive burden that such an environment places on their thinking.

In recent years, we have seen how the Internet, social media, and mobile devices (and other technologies) can be used by foreign adversaries to interfere in elections and to disrupt the democratic process. We have seen:

● Social media exploitation of cognitive biases to increase their impact and reach – short messages of 280 characters and emotionally evocative video/ audio clips are nearly ubiquitous and much more the norm than they ever were two decades ago.

● Disintermediation of established information sources that reduces the role and influence of those previously responsible for providing factual information and proliferates information sources. The US Supreme Court noted in Associated Press v. US (1945) that “the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public, that a free press is a condition of a free society.” Today, modern information technology has enabled the creation of a larger number of information sources than the 1945 US Supreme Court could possibly have imagined.

● Search engines that return highly visible results for queries based in large part on the popularity of those results and the inferred desires of the user for specific information rather than their actual importance to those queries. Such functionality also makes it easier than ever for people to find information online “by doing their own research,” thus indulging in their confirmation biases by selectively finding and attending only to information that confirms one’s beliefs. Search engine optimization techniques enable gaming of search algorithms to promote the visibility of false, misleading, or worthless information. ● Many-to-many connectivity that enables the formation of echo chambers and media bubbles that reinforce pre-existing beliefs.

● Large-scale data mining that allows adversaries to sift huge amounts of personal data on individuals to identify and target those most susceptible to customized, inflammatory, false, malign, or misleading messages – and also to keep such messages away from public view.

● Near-immediate data transfer, which enables propaganda and other malign information to spread far and wide quickly, while efforts to correct false information are more expensive, often fall short, and frequently fail altogether.

● Inauthentic voices that are largely indistinguishable from authentic ones. Macedonian entrepreneurs discovered ways to monetize an affinity of Trump voters for fake news (Subramanian 2017). Paid human employees of the Internet Research Agency created and spread false information on behalf of the Russian government prior to the 2016 U.S. election (MacFarquhar 2018). And automated “bots”–accounts purportedly associated with human users but in fact managed entirely or mostly by machines – add further chaos to the information environment.

Is this state of information affairs really new? Haven’t adversaries of all stripes always employed propaganda and lies – otherwise known as information warfare (or at least a big part of it) – to advance their interests?

Yes. Information warfare indeed has a long pedigree that reaches into the past for at least the three millennia since the Trojan Horse enabled Greek warriors to breach the walls around the city of Troy. Much more recently, the rise of the Nazi regime in Germany relied on propaganda. As Hitler (1925, 155–56) wrote:

[I]ts purpose must be . . . to attract the attention of the masses and not by any means to dispense individual instructions to those who already have an educated opinion on things or who wish to form such an opinion on grounds of objective study – because that is not the purpose of propaganda, it must appeal to the feelings of the public rather than to their reasoning powers. . . . The art of propaganda consists precisely in being able to awaken the imagination of the public through an appeal to their feelings, in finding the appropriate psychological form that will arrest the attention and appeal to the hearts of the national masses. . . . The receptive powers of the masses are very restricted, and their understanding is feeble.

But more so today than at any earlier point in human history, human beings are vulnerable to information warfare. At the same time that new information technologies have led to an increase in the volume and velocity of information available on Earth by many orders of magnitude in the past few decades, the cognitive architecture of the human mind is more or less unchanged on the time scale of centuries or even millennia.

On human cognition

Research in the fields of cognitive and social psychology has formalized what Hitler knew intuitively. We now understand that human cognitive processing capability is not unlimited; humans have finite cognitive resources that can be “used up” under mentally stressful circumstances. Findings from the same cognitive psychology that has transformed neoclassical economics into behavioral economics (and resulted in three Nobel Prizes in economics) have made clear the “bounded rationality” of human thought and the simultaneous existence in every individual of the capability to engage in two types of cognitive processing.

Specifically, heuristic dual-system cognitive theory posits that human beings have two systems for cognitive processing – an intuitive, reflexive, and emotionally driven mode of thought (often designated as System 1) and a slower, more deliberate, analytical mode of thought (often designated as System 2). Kahneman (2011) provides a primer on System 1 and System 2 thinking. (See Petty and Cacioppo 1986; Chaiken 1987 for other variants of dual-system cognitive theory; see Kruglanski and Thompson 1999 for a contrary view on dual-system cognitive theory.)

System 1 is designed to operate rapidly, but it can do so because it does not take account of all available information and is thus more prone to error (also called bias). System 2 operates more slowly but is more likely to take into account the available information and is less prone to error. People engaging in System 1 information processing respond more emotionally and less rationally or critically than in System 2 processing.

Most important, System 1 thinking is the default mode of thought for human beings – it uses smaller amounts of cognitive resources, relies on simple gutbased judgments, and is used more often when humans are under stress. For most situations encountered in everyday life, System 1 thinking is adequate and produces mostly valid and useful outcomes, but it often fails when a situation requires complex inferences for understanding. For such situations, System 2 thinking, which is effortful and consumptive of cognitive resources, is more often appropriate – and when individuals fail to use System 2 when it is appropriate to do so, they are easily misled.

Most individuals are capable of both System 1 and System 2 thinking; thus, the important operative question is the circumstances under which they select one or the other type of thinking. Psychology has accumulated considerable evidence relevant to this question.

For example, Taber and Lodge (2006) show that an individual tends to be less critical of information that is favorable to his or her position than of information that is not favorable – that is, he or she is more likely to engage in System 1 thinking for favorable information. People have a confirmation bias in their information seeking and processing behavior – they preferentially seek out information that is consistent with their beliefs and they are highly critical of (or ignore) information that contradicts their beliefs. In a meta-analysis of 91 studies, Hart et al. (2009) considered two motivations for how an individual might select information to consume – the desire to gain an accurate understanding of reality and the desire to feel validated in his or her beliefs. These two motivations conflict when an accurate understanding of reality does not validate one’s beliefs, and such a situation motivates the question of which of these motivations is more powerful. Hart et al. concluded that both motivations drive human informationseeking behavior, thus moderating each other to a certain extent, but that on balance, humans do exhibit a tendency towards the validation of their beliefs. People are also subject to belief perseverance (a.k.a. a continuing influence effect) – a cognitive bias through which individuals do not revise beliefs based on erroneous information even when they know for sure that such information is erroneous (Lewandowsky et al. 2012).

Maintenance of an individual’s social identity is an important influence on his or her invocation of System 1 or System 2 thinking. Evidence suggests that individuals tend to adopt the views of the peer groups that are most salient to them, even if the “objective” or “factual” information available to them contradicts those views. (Asch 1951 performed the classic “conformity experiments” that demonstrated this phenomenon in the early 1950s.) Uncritical System 1 thinking is active in processing information that is consonant with the beliefs and attitudes of those peer groups. Critical and skeptical System 2 thinking is active in processing information that is dissonant to those groups’ beliefs. These effects (that individuals tend to accept salient group norms) are even more pronounced in an anonymous environment, such as that which characterizes much online interaction (Postmes et al. 2001).

Lastly, there is evidence that emotion and motivation affect cognition. For example, people who are angry tend to rely more heavily on simple heuristic cues (suggestive of System 1 thinking) than those who are not angry (Bodenhausen, Sheppard, and Kramer 1994). Individuals are more likely to stereotype people (a form of System 1 thinking) when that stereotype is consistent with their desired impression of those people; conversely, when the stereotype is inconsistent with their desired impression, individuals tend to inhibit the use of this stereotype (Kunda and Sinclair 1999). Negative emotions (such as those induced by the receipt of information incongruent with a person’s prior beliefs) can improve the ability of a person to reason logically, thus enabling him or her to negate or discount that information (Goel and Vartanian 2011).

In the new information environment, exploitation of human cognitive architecture and capabilities – which are largely unchanged from what existed millennia ago – provides the 21st century information warrior with cyber-enabled capabilities that Hitler, Stalin, Goebbels, and McCarthy could have only imagined. By exploiting cognitive limitations, the perpetrators of cyber-enabled information warfare have learned to exacerbate prejudices, biases, and ideological differences; to add heat but no light to political discourse; and to spread widely believed “alternative facts” in advancing their political positions.

Russian interference in the 2016 US presidential election has dominated news headlines ever since. But interference by authoritarian countries in the elections of democratic states – as undesirable and threatening as it may be – is hardly the only negative consequence of cyber-enabled information warfare. The problems of nuclear war and climate change are hard enough to solve even when well-intentioned, well-informed parties on all sides share a basic understanding and knowledge of the relevant facts. Yes, they may have different values and different priorities, may act under different constraints, and be able to bring to bear different levels of resources to these problems.

But without shared, fact-based understandings of the blast, thermal, and radiation effects of nuclear explosions, what hope is there for national leaders to reach agreements to reduce the threat of nuclear holocaust [war] or to make good decisions about nuclear weapons use in times of crisis? Without shared, fact-based understandings that rising atmospheric carbon dioxide concentrations caused by human beings result in corresponding increases in global temperature and climatic disruption, what hope is there for national leaders to reach agreements to begin serious efforts at decarbonizing their economies?

Climate change denialism

Climate change denialism can be fairly characterized as cyber-enabled information warfare against the reality of large-scale anthropogenically-induced climate change. In the responses of people resistant to taking action to mitigate climate change, we see a number of psychological factors at work (Zaval and Cornwell 2016). For example, one key element of System 1 thinking is the availability heuristic, with which individuals tend to associate the likelihood of an event with the ease with which they can remember similar events in the past. But the long-term consequences of climate change are unprecedented in recorded human history and obviously people have no personal memories of unprecedented events.

Moreover, climate change is a long-term process whose inexorable progression is easily masked by short-term fluctuations in local weather conditions. For example, public concerns about climate changes correlate with local weather conditions (Krosnick et al. 2006). Climate change deniers are also quick to flag for public attention days that are particularly cold as “evidence” that global warming is not occurring and thus, they claim, discrediting theories of climate change. This illustrates a bias known as attribute substitution, as Kahneman and Frederick (2002) describe, through which individuals substitute salient information (such as the cold temperature today) for information that is more relevant but harder to understand (such as information about global climate change).

People are also subject to a loss-aversion bias, in which they place greater weight on losses than gains of equal value. In 1992, the United States committed itself to the United Nations Framework Convention on Climate Change, although President George HW Bush also stated that “the American way of life is not up for negotiation” – and in 2018, the United States withdrew from the Paris Agreement (which was based on the convention). The argument? That the United States would have to give up too much if it kept to the agreement.

To close this (merely illustrative) exploration of biases relevant to climate change denialism, the optimism bias suggests that people consider themselves exceptions when considering the likelihood of a negative event occurring. That is, bad things may happen to other people, but they won’t happen to me, even though I and those other people are similar in important and relevant ways. In a climate context, the bad things may involve sea level rise or heat waves – and the misperception that “others may suffer from such problems but I won’t” diminishes the power of personal concern as a driver for rational decision making.

Connecting the operation of these cognitive biases to the affordances of modern information technologies is not difficult. For example, Roxburgh et al. (2019) demonstrate how the characteristics of specific weather events (e.g. hurricanes or snowstorms) and “short-term socio-political context can play a critical role in determining the lenses through which climate change is viewed.” Note especially the importance of “short-term socio-political context” – precisely the context that social media shapes.

Elsasser and Dunlap (2013) noted the influential role of a variety of newspaper columnists in advancing denialist arguments and thus amplifying these arguments to a broad segment of the American public. Fewer in number then, essentially all columnists today (of all political leanings) have a social media presence that they use to publicize their work, and in many instances their online presence is driven in significant part by social media and reach many more readers online than in print. Furthermore, subtleties and nuances in their extended written pieces are likely to be lost when they are represented in social media.

Another important element of climate change denialism is the easy accessibility of seemingly-authoritative information that casts doubt on the well-established science of climate change. As reported by The Guardian, a variety of largely secret funding sources distributed $118 million to 102 denialist organizations (Goldenberg 2013). Oreskes and Conway (2011) provide the definitive work on deliberate information campaigns to obscure the scientific truth on a range of issues from smoking to climate change. These denialist organizations have generated a variety of products for public and policy consumption (but – unsurprisingly – not many peer-reviewed scientific articles) that are easily accessible to the public, mainstream media outlets, and policy makers. Their products are broadly disseminated through social media and easily found through customized search, and they are sought by reporters who seeking to cover “both sides” of a controversy that is intellectually equivalent to a “controversy” about whether the earth is round or flat.

Nuclear conflict

On the risks of nuclear conflict, theories and approaches to nuclear deterrence and strategic stability developed prior to the collapse of the Soviet Union in the late 1980’s and early 1990’s rest on the presumption of rationality in national decision makers. In particular, they assume that adversaries are deterred from attacking by a threat of retaliation that would impose costs on the adversary that would outweigh any conceivable benefits that it would gain from an attack (Morgan 2003). Central to this assumption is a rational adversary that can and does make a calculation of expected costs and benefits, compares them, and then acts accordingly.

But the psychologically informed understanding of realworld decision making described above was not accepted widely in the scientific literature until approximately the same time as the collapse of the Soviet Union, and the seminal work in such understanding occurred only in the decade previous to that. What a psychologically-informed understanding of real-world decision making tells us is that the rationality assumption at the base of much traditional thinking on deterrence and strategic stability is untenable, given that humans have evolved to rely on intuitive, reflexive, heuristic System 1 thinking to make decisions, particularly when faced with time pressures, surprise and other obstacles to the deliberate calculation implied by System 2 thinking (Kahneman 2011). Psychology tells us that – more often than not – the fast, intuitive judgements of System 1 often take precedence over the slower, more analytical thinking of System 2.

The challenges posed by reflexive reliance on System 1 thinking are greatly accentuated by characteristics of today’s information environment. Social media networks in particular are optimally designed to stimulate System 1 thinking – emotional, reflexive, immediate – and they rapidly transmit content among like-minded individuals, creating the ideal conditions for public polarization and divisiveness to occur (Pfeffer, Zorbach, and Carley 2014). Multiple narratives rapidly emerge around complex events; citizens splinter into their own informational universes and are unable to agree on an underlying reality. Political leaders themselves are subject to these conflicting narratives and may even be active and influential participants in one or another of them.

It is thus easy to posit that in this information environment, manipulated information – either artificially constructed or adopted by a strong grassroots base – could be used by interested parties to generate pressure on leaders to act. At the same time, leaders themselves are likely to be facing information overload and less able to distinguish analyzed information from their own intelligence sources and other, unvetted information originating from their constituencies.

The coming information dystopia

Nuclear war and climate change are arguably the most important existential challenges today that are compounded by the corruption of the information ecosystem. But even if a single miraculous stroke the laws of physics were changed to make nuclear weapons impossible to build and operate and to immediately eliminate anthropogenic emissions at zero cost, cyber-enabled information warfare could still can lead to an information dystopia. Here are some possible elements:

● Adversaries manufacture numerous graphic videos of American soldiers (complete with sound effects) committing battlefield atrocities, and spread them widely through the Internet. Once upon a time, highquality video forgeries were difficult and expensive to make. AI-based technologies will bring this socalled deepfake capability to the masses, and anyone with imagination, a modicum of technical skill, and a personal computer will be able to distribute reasonably realistic forgeries. Denials will be issued but of course will also not be believed by large fractions of viewers. Even if proof of inauthenticity can be provided, such evidence will not affect the responses of many viewers.

● Political campaigns conduct similar efforts to discredit political opponents (e.g. “showing” an opponent making controversial or disqualifying remarks before an election). But they also use the existence of deepfake technologies to deflect attention from authentic and real evidence of their own political and personal misdeeds. For example, a real video of a candidate punching an old lady who supports his opponent will be dismissed as “one of those deepfakes that anyone could have produced.”

● Financial markets are disrupted by falsified videos of CEOs making announcements regarding company prospects that are much more pessimistic than expected. Attempts to correct the record are drowned out in a subsequent flood of contradictory information, all of which appear at first glance to be authentic.

● Public safety is compromised by reports of local disasters (e.g. explosions of chemical plants that result in the release large amounts of toxic gases). These reports, along with “authentic” video of people choking amidst locally familiar locations (e.g. well-known fields or sport stadiums), cause spontaneous mass evacuations. Contradictory directions for evacuation broadcast using social media result in chaos on the streets and highways.

● Public health is placed at risk when the safety and efficacy of medical treatments known to be safe and effective are publicly questioned through active disinformation campaigns conducted on the Internet and in bookstores. Attempts to provide valid information are met with responses such as “that’s what the pharmaceutical companies and medical establishment want you to think, but just look at what’s happened to our children.”

● Children in schools are threatened by online campaigns to spread rumor, innuendo, and positive or negative information about various students. Conducting such campaigns for pay becomes the business model of entrepreneurs who advertise that they can guarantee admission to selective colleges, boost the social standing of the children of their clients, or take revenge on those who have harmed such children, all in anonymous and untraceable ways.

● Journalists, political leaders, and judges are compromised by artfully forged emails and alterations to other documents that are mixed with entirely authentic leaked emails and documents and are indistinguishable from them.

A world with these elements – and many more comparable ones – will be the inevitable result if and when deployment and use of the tools of cyber-enabled information warfare become widespread. And even more troubling is the fact that not every bit of information needs to be corrupted for this dystopian outcome to occur – it will require only a fraction of it to be corrupted for people to lose faith entirely in “objective” and “trustworthy” sources of information, the result of which will be that people will fractionate into their own information realities.

Fearing the end of the enlightenment

The Enlightenment established reason and reality as the foundational pillars of civilized discourse. In such discourse, logic matters, and a logical contradiction between statement A and statement B means that at least one of those statements is false. The truth of a statement about the world is tested by its correspondence to objective reality rather than by how many people believe it; that is, empirical data are influential. Furthermore, statements known to be wrong or false do not affect conclusions or choices between alternative courses of action.

Cyber-enabled information warfare provides the tactics, tools, and procedures – in short, the means – to replace the pillars of logic, truth, and reality with fantasy, rage, and fear. In a world of ubiquitous cyber-enabled information warfare, communication and information inflame passions rather than informing reason, play to the worst in people’s cognitive architectures rather than the best, and divide rather than unify. Deliberate corruption of the information ecosystem could be seen as an analog of poisoning water supplies that can be done remotely, inexpensively, and anonymously. All of this is just another way of saying that today it is possible to see glimmerings of an anti-Enlightenment that can possibly take root and that would indeed be the end of civilization as we know it.

#### E—Resilience strategies can blunt the effectiveness of hybrid threats and decrease risks

Marovic, Politikon Executive Director, ‘19

[Jovana Marovic, Exeuctive Director, Politikon Network, “Wars of Ideas: Hybrid Warfare, Political Interference, and Disinformation,” NEW PERSPECTIVES ON SHARED SECURITY: NATO’S NEXT 70 YEARS, 11—28—19, https://carnegieeurope.eu/2019/11/28/wars-of-ideas-hybrid-warfare-political-interference-and-disinformation-pub-80419, accessed 4-25-22]

NATO’s success as a collective defense organization lies in its ability to rally twenty-nine member states in defense of any one of them. Cohesion is what makes the alliance strong and unique, but it is difficult to sustain day after day, under constant pressure from adversaries.

One useful way to measure cohesion is in financial terms. Despite a pledge to contribute the equivalent of at least 2 percent of their gross domestic product to defense by 2024, some member states seem likely to miss the target. While this does not prove that the allies disagree on the nature and gravity of the threats before them, it does strongly suggest that some have not fully bought into the agreed priorities.

Many factors are undermining cohesion in NATO. In an era with no single unifying threat, different members inevitably have different interests in diverse centers of power and influence. Allies also diverge on what constitute democratic standards and appropriate responses to competition with non-Western actors.1

It is up to individual countries to safeguard their freedom to respond to a call for help from an ally, address vulnerabilities and gaps in their national systems, and take proactive measures to reduce risks. But the alliance as an organization can help. This is especially true when it comes to understanding and responding to new threats to cohesion. None is more relevant than the hybrid war for hearts and minds that NATO’s adversaries are waging through political interference and disinformation.

ISSUES AT STAKE

While not a new phenomenon, hybrid warfare has been widely mentioned in international discourse since at least 2014. The Russian military intervention in Ukraine and annexation of Crimea showed that NATO and its member states lacked ready-made responses to the emergence of a threat aimed directly at solidarity and cohesion. The experience has prompted allies to rethink, act, and adapt quickly, especially with regard to instruments for protection beyond triggering Article 5 of NATO’s founding treaty, which declares that an attack on one ally is an attack on all.

Hybrid warfare includes a variety of activities and covers the use of different instruments to destabilize a society by influencing its decisionmaking. Frequent instruments include:

Interference in electoral processes: An adversary can use techniques from campaigning through the media and social networks to securing financial resources for a political group to influence the outcome of an election in a direction that favors the adversary’s political interests.

Disinformation and false news: An adversary can create a parallel reality and use falsehoods to fuel social fragmentation. The idea is to disorient the public and make it difficult for a government to seek public approval for a given NATO policy or operation.

Cyber attacks: An adversary can pressure NATO governments into not coming to each other’s aid in times of crisis by threatening devastating cyber attacks aimed at the civilian population. Examples include attacks on networks governing hospitals or electricity and water supplies.2

Drone attacks: These are similar to cyber attacks but on a more limited scale. An adversary can use remotely piloted platforms to inflict misery on civilians by crippling the operations of airports, air ambulances, and police helicopters. Such attacks can also hamper military airspace operations in early phases of a conflict.3

Financial influence: An adversary can make investments, conclude unfavorable energy-supply deals, or offer loans that make a country vulnerable in the long run to political pressure.

Russia is the most frequently cited source of hybrid attacks, particularly disinformation, interference in elections, and cyber attacks.4 It and other states often act via third, nonstate entities such as nationalist, criminal, or terrorist groups. This leaves the attacking state room for deniability, confuses the attacked country, and can prevent a timely and adequate response. Most hybrid operations to date have featured a mixture of mechanisms used by state and nonstate actors, and a clear line between them is difficult to draw.

NATO’s efforts to address hybrid threats have been conducted at two levels: defining strategy at the supranational level and assisting the target countries at the national level. The latter effort will receive a boost when the new counterhybrid support teams on which members agreed in July 2018 fully come into effect. NATO’s Joint Intelligence and Security Division is in charge of hybrid-related research and analysis, while the Public Diplomacy Division tracks disinformation through online instruments. The Emerging Security Challenges Working Group, established in 2012, has a goal to identify and prioritize nontraditional threats.

Because hybrid attacks are a threat to the West as a whole, not just NATO, and because they mostly rely on nonmilitary tools, the alliance has been strengthening its cooperation with the European Union (EU). One useful tool available to both organizations is the joint European Center of Excellence for Countering Hybrid Threats, established in Helsinki in April 2017.

RECOMMENDATIONS

NATO can and should do more to counter hybrid threats, following the proven strategy of prepare, deter, and defend.5

BUILD RESILIENCE BY FOSTERING DEMOCRACY

The first, self-evident recommendation is to deny adversaries the opportunities they exploit for hybrid attacks. The more stable the political systems and economies of NATO countries are, the less suitable ground they represent for hybrid threats. A government that is credible, popular, and trusted will have an easier time winning support for its chosen course of action in NATO than other governments and will be better able to resist disinformation and other forms of interference and blackmail.6

Western Balkan countries seem particularly vulnerable, as their citizens tend to have low trust in the authorities and do not believe that their judiciaries are truly independent. In opinion polls, as many as 70 percent of respondents said that the law did not equally apply to all.7 Democracy and trust have declined in most Western Balkan countries over the last ten years, a trend that overlaps with the crisis of democracy throughout Europe.8

Steps that strengthen democracy and economies are the most effective way of building resilience against hybrid attacks. Corruption deserves particular attention. Not all authoritarian and illiberal governments are corrupt, but most abuse access to public and European funds to give themselves a competitive advantage over political rivals.9 Once on a corrupt path, authoritarians are, in essence, condemned to always seek to remain in power, lest they be prosecuted. It is a vicious circle, and this dynamic between authoritarianism and corruption is not always understood—including by the U.S. and EU leaderships, which does not serve the alliance well.

#### F—Cooperative action on resilience approaches is critical

Speranza, Center for European Policy Analysis director, ‘20

[Lauren Speranza, Director, Trans-Atlantic Defense and Security, Center for European Policy Analysis, “A Strategic Concept for Countering Russian and Chinese Hybrid Threats,” Scowcroft Center for Strategy and Security, Atlantic Council, 7—20, p. 3]

Indeed, traditional security concerns, such as nuclear weapons and conventional defense and deterrence, will not go away for the transatlantic community. Yet, going forward, transatlantic nations and institutions will increasingly need to focus on hybrid and nontraditional threats too.2 This is particularly underscored by the 2020 coronavirus crisis, in which both Russia and China have played various roles. Both China and Russia capitalized on the crisis to wage disinformation campaigns against the West. They promulgated conspiracy theories designed to sow fear about America’s handling of the outbreak and to promote the successes of their own authoritarian regimes. Moscow and Beijing also strategically delivered aid and medical supplies to European countries in attempts to build good will and clout on the international stage. These issues cannot be effectively addressed alone or in a vacuum, making global cooperation and collective action–especially among transatlantic allies—paramount. Even as transatlantic nations and institutions shift priorities in the wake of the coronavirus crisis, key counter-hybrid priorities, such as building resilience, strengthening civil response capacities, and investing in civic education, simultaneously serve priorities for pandemic prevention and response. This is all the more reason to prioritize the counter-hybrid agenda.

# Resilience Aff: Alliance / Cyber Extensions

### Cyber Threat Now: Multiwarrant

#### We face multiple cyberthreats—cyber disruptions, gray zone ops, battlefield force multipliers

Blessing, American Enterprise Institute fellow, ‘22

[Jason Blessing, Visting Research Fellow, American Enterprise Institute and PhD, Political Science, Syracuse University, “Fail-Deadly, Fail-Safe, and Safe-to-Fail: The Strategic Necessity of Resilience in the Cyber Domain,” NATO 2030: TOWARDS A NEW STRATEGIC CONCEPT AND BEYOND, Ed. J.Blessing, K.KjellstromElgin, N.M.Ewers-Peters, School of Advanced International Studies, Johns Hopkins University, 2022, p. 264-266]

The Cyber Threat Landscape

NATO defines cyberspace as the “global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.”13 The domain thus has three main components: (1) the physical layer, such as hardware components or undersea cables that are geographically bound; (2) the logical layer, where elements are manifested in code or data through software, firmware, etc.; and (3) the human layer, consisting of the virtual identities of those individuals interacting with the other layers.14

Cyberspace operations are operations to defend, attack, or exploit computers, their information, and/or networks. Defensive operations look to maintain the integrity, confidentiality, and availability of computers, information, and networks. Offensive operations seek to disrupt, deny, degrade, or destroy information, computers, and/or networks. Operations focused on exploitation intend to monitor, collect, and exfiltrate data from computers and networks without disruption or destruction.15 To a certain degree, operations are dependent on physical infrastructure that supports and enables the digital realm, and they can produce territorial effects. Yet, cyber operations are not territorially bound; they can produce near-instantaneous effects that, whether intended or not, can rapidly spread to networks and systems outside the original target. Targeting itself is not limited to state assets, as the private sector is routinely the victim of malicious activity.

Both state and non-state actors can conduct cyberspace operations.

Non-state actors can include individuals, criminal organizations, terrorist groups, and ‘patriotic hackers’ (some of which can be state-affil- iated or state-sanctioned). State actors primarily include intelligence services and militaries. Operations carried out by states are likely to be more impactful as they are better-financed and better-resourced than non-state actors. While a variety of states can and do make use of cyber operations, NATO Allies emphasized Russia and China as primary threat actors at the 2021 Brussels Summit.16

There are three main ways adversaries can utilize cyber operations.17 First, cyber operations can achieve independent effects in or through the cyber domain. Such operations range from relatively unsophisticated attacks, such as distributed denials of service (DDOS), to the complex deployment of malware by advanced persistent threats (APTs). For example, the 2007 DDOS attacks on Estonia used fairly simple methods to send traffic requests that overwhelmed servers used by the Estonian Parliament, several political parties, institutions in control of the country’s internet infrastructure, and a number of financial firms, news organizations, and communications firms.18 More complex methods were used to produce significant physical damage in the suspected Russian-sponsored compromise of a German steel mill in 2014, in which spear-phishing emails contained malicious attachments that, once opened, accessed and disrupted the industrial controls systems for a blast furnace.19

Second, cyberspace operations can act as a military force multiplier. Adversaries can use cyber tools to ‘prepare the battlefield’ by compromising a target’s communications systems, as was the case for the 2008 Russian incursion into Georgia. As the Russian military prepared for a ground invasion, a variety of Russian-linked non-state actors, including criminal organizations, conducted a series of DDOS attacks that degraded the Georgian government’s communications systems and froze the National Bank of Georgia. The Russian military invasion benefited greatly, as Georgia was unable to coordinate defense efforts and was delayed in procuring war materials from the private sector.20 Cyber operations can also be a force multiplier when used in conjunction with traditional military means. For example, Russia’s invasion and illegal occupation of Crimea has co-deployed cyber tools with kinetic weapons systems in attempts to bolster the Russian military’s effects.21

Finally, attacks and exploitation in and through cyberspace can enable broader grey zone operations22 such as defense industrial espionage and intellectual property theft, compromising critical infrastructure, election meddling, and broader disinformation efforts (see Rebegea and Schmiedl in this volume). Notable examples include cyber operations such as China’s theft of F-35 fighter jet design plans from US defense contractor Lockheed Martin in 2009, Russian infiltration of US power grids in 2009, the 2013 Chinese hack of the US Office of Personnel Management, and Russian election meddling in US and European elections

### Cyber Threat Now: Ukraine Brink

#### [x] Brink – Ukraine invasion –list of threats similar to above

Maigre, 2022

[Merle, senior cybersecurity expert at e-Governance Academy in Estonia. In 2017–2018, she served as director of the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE), “NATO IN A NEW ERA: GLOBAL SHIFTS, GLOBAL CHALLENGES NATO’s Role in Global Cyber Security” German Marshal Fund APRIL 06, 2022 <https://www.gmfus.org/news/natos-role-global-cyber-security> accessed jcp-TM 6/8]

Introduction

What the war in Ukraine says about cyber power is yet not entirely cleared from the fog of war. Many aspects remain uncertain, but given the unpredictability of the Putin regime, the risk of an escalation in hostile cyber exchanges between Russia and NATO states remains high. What is clear is that, as of February 24, 2022, we live in a different world in which the European and global security orders have been shattered.

This brief first explores the challenge that cyber threats pose to NATO allies and how the rapidly evolving cyber-threat landscape can alter the inter- national security environment. Secondly, it looks at developments in cyber defense policy within NATO. Finally, the brief analyzes how NATO needs to adapt to address cyber challenges, studying how allies align their sovereign interests, capabilities, and cyber doctrines with NATO operational requirements and strategic ambitions. NATO is set to issue strategic documents in 2022 that will guide the next decade of its military planning. This will certainly require more transatlantic consultation on political-military matters with an emphasis on cyber security and cyber defense.

The Cyber Challenge to the World and NATO Allies

Malicious cyber activity has increased substantially over the past years while the world has kept turning amid the omnipresent pandemic and now war in Ukraine. States, non-state actors, and criminal groups compete and are increasingly weaponizing sensitive information and infiltrating other countries’ networks to steal data, seed misinformation, or disrupt critical infrastructure.

The coronavirus pandemic further complicated the cyber-threat landscape. In March 2020, attempts to mitigate the spread of the coronavirus led to social distancing measures, travel restrictions, and remote work. In a short span of time, IT security profes- sionals had to respond to the challenges of working from home, such as enterprise data movements when employees accessed cloud-based apps via their home internet, corporate software, videoconferencing, and file sharing.1 Even if hardware and software solutions were in place to secure the organization’s data, there were often no established policies to help employees wade through the jungle of threats and vulnerabilities they faced when moving their workplace out of the traditional office environment.2

According to the FireEye Mandiant Special Report: M-Trends 2021, the top five most targeted indus- tries in 2020 were business and professional services, retail and hospitality, finance, healthcare, and high technology. The main methods used were extortion, ransom demands, payment card theft, and illicit trans- fers. Direct financial gain was the likely motive for 36% of intrusions, and an additional 2% of intrusions were likely perpetrated to resell access. In 2021, data theft remained an important mission objective for threat actors; in 32% of intrusions, adversaries stole data.3

Currently, highly organized, technically proficient criminal syndicates comprise the most significant cyber threat to allies. These groups try to steal data or extort money through ransomware. In 2021, promi- nent ransomware attacks struck Colonial Pipeline, the operator of the largest fuel pipeline on the East Coast of the United States; JBS, the largest meat processing company in North America; and Coop, a major supermarket chain in Sweden. Healthcare was also targeted—in May of the same year, the entire health service system of Ireland was disrupted for weeks, and over the spring and summer, dozens of hospitals in Europe and the United States were locked out of life-critical systems by ransomware attacks.4

Another set of threats comes in the form of bellig- erent state actors that seek to steal sensitive data for espionage. In December 2020, Russian intelligence services infiltrated the digital systems run by US tech firm SolarWinds and inserted malware into its code. During the company’s next software update, the virus was inadvertently spread to about 18,000 clients, including large corporations, the Pentagon, the State Department, Homeland Security, the Treasury, and other US government agencies. The hack went unde- tected for months before the victims discovered vast amounts of their data had been stolen.5

There are also politically motivated cyberattacks mandated by states that interfere in democratic processes and political discourse. In September 2020, the internal email system of Norway’s parliament was hacked.6 Ine Eriksen Søreide, the Minister of Foreign Affairs of Norway, underlined the significance of the attack by calling it an important cyber incident that affected the “most important democratic institution” of the country.7 Norwegian authorities later identified Russia as the actor responsible for the attack, marking the first time that Norwegian authorities had made a political attribution to such an attack.

Since the beginning of this year, Ukraine’s govern- ment has been hit by a series of cyberattacks that defaced government websites and wiped out the data on some government computers. In mid-Jan- uary, hackers defaced about 70 Ukrainian websites, including the Ministries of Foreign Affairs, Defense, Energy, Education, and Science, as well as the State Emergency Service and the Ministry of Digital Trans- formation, whose e-governance portal gives the Ukrainian public digital access to dozens of govern- ment services. The hackers replaced the home pages of about a dozen sites with a threatening message: “be afraid and expect worse.” After a couple of days,however, most of the sites were restored.8 The inter- national hacktivist collective Anonymous has declared “cyberwar” against Russia’s government, claiming credit for several cyber incidents including distrib- uted denial of service attacks that took down Russian government websites and Russia Today, the state- backed news service.9

Around the globe, aging critical infrastructure has long been vulnerable to attack.

The most worrying type of cyberattack is sophis- ticated malware designed by states or state-backed actors that act as “time bombs” in the critical cyber networks of target countries, such as the energy, telecom, and transportation sectors. Around the globe, aging critical infrastructure has long been vulnerable to attack. In 2020, the UK’s National Cyber Security Centre issued a warning of Russian attacks on millions of routers, firewalls, and devices used by infrastruc- ture operators and government agencies.10

On the day of the Russian invasion, ViaSat, a provider of high-speed satellite broadband services, was hacked along with one of its satellites Ka-Sat, whose users included Ukraine’s armed forces, police, and intelligence service. Destructive wiper malware attacks by Russia against Ukraine included Whisper- Gate, discovered in January by Microsoft, in Ukraine’s networks that “provide critical executive branch or emergency response functions”;11 HermeticWizard and IsaacWiper,12 targeting multiple Ukrainian orga- nizations just hours before the Russian invasion began; and CaddyWiper, spotted by researchers at the Slovak internet security company ESET in mid-March.13 All of them were designed to wipe or overwrite critical files on infected systems and leave computer hard drives corrupted and unrecoverable. These incidents demonstrate that, in the words of cyber expert and Silverado Policy Accelerator think tank chairman Dmitri Alperovich, “Cyberattacks have become a theater for great-power conflict in which governments and militaries fight in the hybrid ‘gray zone,’ where the boundaries between peace and war are blurred.”14 The actors navigate a complex web of ambiguous and deeply interconnected challenges, where cyberattacks are not a separate front, but rather an extension of the conflict.

### Cyber Impact: Nuclear Entanglement

#### [x] Cyberattacks risk nuclear escalation—C3I entanglement

Afina et al., Chatham House analyst, ‘20

[Yasmin Afina, Research Assistant, ISP, Calum Inverarity, Research Analyst, ISP, and Beyza Unal, Research Fellow, International Security Program, Chatham House, “Ensuring Cyber Resilience in NATO’s Command, Control and Communication Systems,” Chatham House, Royal Institute of International Affairs, 7—20, p. 2]

Note: C3I = command, control, communications, and intelligence

Summary

 NATO’s nuclear capability is provided by the US and the UK. The modernization of systems and arsenals held by both states is proceeding apace. This has involved – and continues to involve – the integration and use of increasingly sophisticated new technologies within their nuclear programmes, including in their respective command, control and communication (C3) systems.

 Cyber operations targeting NATO members’ C3 systems and their assets, including nuclear assets, are also increasingly sophisticated in nature. While cybersecurity is a serious concern, and there is acknowledgment of the potential magnitude of cyberattacks, documentation available in the public domain indicates the need for NATO and its members to put in place further measures to ensure the cybersecurity of C3 systems, including those of nuclear systems (NC3). This is all the more pertinent given that some Allies’ military capabilities still include legacy systems from the Soviet era.

 The protection of C3 systems requires the adoption of adequate, adaptable and robust cybersecurity measures, in order to ensure the integrity of these systems and to shield them from both internal and external disruption. The following five considerations are of relevance for the protection of NATO’s own C3 systems, and those of its member states: software and network protection; data (integrity) protection; hardware protection; access/security controls; and cybersecurity awareness/security by design. These attest to the need for robust measures beyond the non-kinetic, digital realm to ensure the cybersecurity of NATO’s C3 ecosystem.

 The increasing reliance on C3 assets that may be used for both conventional and nuclear operations raises the prospect of entanglement, and the associated risk of rapid escalation. The potential for unintended escalation is further exacerbated by the threat of cyberattacks and possible new threats emanating from other emerging technologies, including quantum computing. Unknown and unanticipated effects from cyber operations targeted at C3 assets may compromise the legality of these attacks when such assets may be of both military and civilian use simultaneously.

 Measures to prevent misinterpretation and rapid escalation are critical to the security of C3 systems. Such measures could include a clearer understanding of: how adversaries think about command and control; what would constitute a cyberattack in the context of C3 systems; and what would constitute adequate responses to such attacks within the frameworks of international law – particularly international humanitarian law.

 False confidence and false stress are equally problematic. In addition to ensuring the cybersecurity of their existing nuclear planning and NC3 architecture, NATO and Allies must reflect on how these dynamics will affect current understanding, arrangements and strategies surrounding the concept of nuclear sharing. Concerns over legacy infrastructure, in the context of an evolving threat landscape and the modernization of systems with digital means, raise questions with regard to the way forward for the hosting of US nuclear weapons in Europe, as well as for existing nuclear burden sharing agreements.

### Cyber Impact: Nuclear Escalation

#### Tit-for-tat retaliation spirals risk nuclear escalation

Klare, Hampshire College professor, ‘19

[Michael T. Klare, Professor Emeritus, Peace and World Security Studies, Hampshire College and Senior Visiting Fellow Arms Control Association, “Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation,” ARMS CONTROL TODAY, 11—19, <https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation>, accessed 2-24-22]

The danger here is that economic attacks of this sort, if undertaken during a period of tension and crisis, could lead to an escalating series of tit-for-tat attacks against ever more vital elements of an adversary’s critical infrastructure, producing widespread chaos and harm and eventually leading one side to initiate kinetic attacks on critical military targets, risking the slippery slope to nuclear conflict. For example, a Russian cyberattack on the U.S. power grid could trigger U.S. attacks on Russian energy and financial systems, causing widespread disorder in both countries and generating an impulse for even more devastating attacks. At some point, such attacks “could lead to major conflict and possibly nuclear war.”14

These are by no means the only pathways to escalation resulting from the offensive use of cyberweapons. Others include efforts by third parties, such as proxy states or terrorist organizations, to provoke a global nuclear crisis by causing early-warning systems to generate false readings (“spoofing”) of missile launches. Yet, they do provide a clear indication of the severity of the threat. As states’ reliance on cyberspace grows and cyberweapons become more powerful, the dangers of unintended or accidental escalation can only grow more severe.

#### Use-or-lose incentives risk nuclear escalation

Klare, Hampshire College professor, ‘19

[Michael T. Klare, Professor Emeritus, Peace and World Security Studies, Hampshire College and Senior Visiting Fellow Arms Control Association, “Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation,” ARMS CONTROL TODAY, 11—19, <https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation>, accessed 2-24-22]

Although occurring largely in secret, what can aptly be called “an arms race in cyberspace” is underway. Where this might lead is difficult to foresee, but it is certain to involve the development of ever more potent cyberweapons. Each nuclear power will seek to enhance its defenses against future cyberattack. Yet, just as is the case in missile warfare, it is easier and cheaper to devise new offensive cybersystems than defensive ones. In the event of a crisis, then, there will be a strong temptation to employ the new technologies early in the encounter, when they might be used to maximum effect, setting in motion an escalatory process resulting in nuclear weapons use. As noted, the mere fact that disruptive malware is known to have been embedded in the vital command-and-control systems of a nuclear power could lead it to distrust its early-warning and intelligence systems and, in a panicky response to ambiguous signals, assume the worst and launch its nuclear weapons.

#### Cyber attacks cause massive destruction and risk nuclear retaliation

Spector, James Martin Center senior fellow, ‘22

[Leonard Spector, former senior official, US National Nuclear Security Administration and Distinguished Senior Fellow, James Martin Center for Nonproliferation Studies, “Cyber Offense and a Changing Strategic Paradigm,” WASHINGTON QUARTERLY v. 45 n. 1, Spring 2022, p. 39-40]

This reorientation might seem a positive development by possibly lowering the threat of nuclear conflict. But this optimistic conclusion is not clear-cut. To be sure, the destruction from massive cyberattacks against critical infrastructure would be orders of magnitude less than that caused by nuclear war. It is also true that calibrated infrastructure cyberattacks provide additional pre-nuclear rungs to the escalation ladder, possibly making resort to nuclear arms more remote.6 Massive infrastructure cyberattacks, however, could nonetheless cause catastrophic devastation, leading to years of national hardship and considerable loss of life from the collapse of food, water, medical, and other essential systems.7 Moreover, the very fact that such infrastructure attacks avoid the unbounded cataclysm of nuclear war increases the likelihood that this cyber capability could be used, potentially to the great harm of the targeted state. Nor can the threat of retaliation with nuclear arms to an unrestrained cyberattack be ruled out, a possibility the United States, at least, appeared to invoke in the US 2018 Nuclear Posture Review. 8 China and Russia have also implicitly left the door open to responding with nuclear weapons to such an attack.9

#### There are multiple nuclear escalation pathways—spoofing, use-or-lose pressures, escalation spirals

Spector, James Martin Center senior fellow, ‘22

[Leonard Spector, former senior official, US National Nuclear Security Administration and Distinguished Senior Fellow, James Martin Center for Nonproliferation Studies, “Cyber Offense and a Changing Strategic Paradigm,” WASHINGTON QUARTERLY v. 45 n. 1, Spring 2022, p. 38-39]

Many in the national security community fear that such cyber operations carry the potential for dangerous, unpredictable consequences. High on the list of concerns is that offensive cyber tools intended for use against nuclear weapon systems will create uncertainties in potential target countries regarding the integrity of their second-strike nuclear forces. This, it is feared, could create incentives to strike first in a crisis, eroding strategic stability based on certainty of devastating retaliation in kind to a nuclear attack. A related oft-noted worry is that an adversary’s or non-state actor’s cyber tampering with a state’s early warning systems could lead the latter to launch its nuclear forces based on spurious information indicating it was under attack, or on the erroneous assumption that the tampering, which may have in fact been undertaken only to collect intelligence or to interfere with conventional military operations, was precursor to such an attack.3 In the case of a cyberattack against a state’s critical infrastructure, a leading concern is that the state’s response to such attacks cannot be known in advance, but could set in motion a volatile escalatory spiral, leading to conventional conflict and ultimately possible resort to nuclear arms.4

### Cyber Impact: Nuclear War-Equivalent

#### The effects are as bad as a nuclear war

Thompson, Lexington Institute COO, ‘14

[Loren Thompson, Chief Operating Officer, Lexington Institute, former Deputy Director, Security Studies Program, Georgetown University, and PhD, Georgetown University, “Cyber Alliances: Collective Defense Becomes Central To Securing Networks, Data,” FORBES, 9—19—14, <https://www.forbes.com/sites/lorenthompson/2014/09/19/cyber-alliances-collective-defense-becomes-central-to-securing-networks-data/>, accessed 2-24-22]

It isn't hard to see why NATO is worried about threats in cyberspace, given Russia's recent use of on-line attacks against Ukraine and other countries in a style of combat that has come to be called "hybrid warfare." However, a report by the Pentagon's prestigious Defense Science Board released last year suggests that the cyber challenge reaches far beyond the use of botnets and distributed denial-of-service tactics. Describing the extensive vulnerability of U.S. military forces to cyber assault, the report then observed,

The impact of a destructive cyber attack on the civilian population would be even greater with no electricity, money, communications, TV, radio or fuel (electrically pumped). In a short time, food and medicine distribution systems would be ineffective; transportation would fail or become so chaotic as to be useless. Law enforcement, medical staff, and emergency personnel capabilities could be expected to be barely functional in the short term and dysfunctional over sustained periods.

These sustained periods, the science board stated, might last "months or years" as government and industry sought to rebuild damaged infrastructure -- a possibility that led the panel to compare the specter of state-sponsored cyber attacks to the threat of nuclear war. So if you think that 56 million payment cards being compromised at Home Depot is about as bad as cyber threats can get, think again. Civilians and soldiers alike have hardly begun to experience how destructive the coming age of information warfare is going to be.

### NATO Status Quo: Cohesion Low Now

#### Cohesion low now

Speranza, Center for European Policy Analysis researcher ’21

[Lauren Speranza, Director, Translatlantic Defense and Security Program, Center for European Policy Analysis, “American Leadership in NATO: A Rocky Return but a Firm Future,” ICDS DIPLOMAATIA, 12—1—21, <https://icds.ee/en/american-leadership-in-nato-a-rocky-return-but-a-firm-future/>, accessed 4-7-22]

Although America is ‘back’ at NATO, Europe remains unsettled about the credibility and longevity of US commitments to the alliance. A cloud of uncertainty hangs over the alliance’s next Strategic Concept and how the two sides will craft a common agenda to endure the coming decade. The Biden administration, despite a few recent transatlantic missteps, recognises the gravity of this moment and has come prepared with a focused set of priorities for NATO’s future.

Following his successful first trip to Europe, a string of recent US decisions has undermined President Biden’s early pledges to strengthen cooperation with NATO allies. Whether the tacit approval of the Nord Stream 2 pipeline, the chaotic withdrawal from Afghanistan, or the controversial announcement of the AUKUS security pact, these disjointed moves have begun to sow doubt in Europe about America’s willingness and ability to work jointly with Europe, even under an Atlanticist president. While the Biden administration has acknowledged and sought to address these slipups, such unpredictability in the transatlantic relationship has weakened the political cohesion required for building NATO’s next Strategic Concept.

### NATO IL: Cohesion—Cyber

#### [x] Unchecked Russian and Chinese cyber attacks undermine alliance cohesion now

Kramer et al., Scowcroft Center Distinguished Fellow, ‘20

[Franklin D. Kramer, Distinguished Fellow, Scowcroft Center for Strategy and Security and Board Director, the Atlantic Council, Lauren Speranza, Director, Transatlantic Defense and Security, Center for European Policy Analysis, and Conor Rodihan, Assistant Director, Transatlantic Security Initiative, Scowcroft Center for Strategy and Security, “NATO Needs Continuous Responses in Cyberspace,” NEW ATLANTICIST, The Atlantic Council, 12—9—20, <https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/>, accessed 5-23-22]

Russia and China challenge NATO and its members in cyberspace on a daily basis, as part of ongoing hybrid campaigns to undermine the transatlantic community. The Kremlin’s actions have involved intrusions into Allies’ critical infrastructures, manipulating Allies’ elections through hacks and disinformation, and even blocking GPS information critical to NATO activities. The Chinese government has engaged in cyber espionage against Allies’ military capabilities; intellectual property theft related to sensitive technologies, industries, and infrastructure; and disinformation against transatlantic countries, including around the coronavirus. These efforts to weaken NATO countries and Alliance cohesion represent a persistent threat to Allied security.

NATO has recognized the collective dangers of these hybrid attacks in cyberspace. Up to this point, however, the Alliance has taken a reactive approach, responding as if Russian and Chinese cyber attacks are each isolated incidents. But because Russian and Chinese cyber efforts are part of continuous campaigns directed at the overall capability of the Alliance, NATO’s response has been insufficient, failing to reduce or dissuade further attacks. To assure the security of its members going forward, NATO needs its own continuous response campaign to these threats.

### NATO IL: Cohesion—China

#### Chinese influence threatens interoperability, cohesion, and alliance effectiveness

Nietsche et al., CNAS Research Associate, ‘20

[Carisa Nietsche, Research Associate, CNAS Transatlantic Security Program, Jim Townsend, former Deputy Assistant Secretary fo Defense and Adjunct Senior Fellow, CNAS and Andrea Kendall-Taylor, Senior Fellow, CNAS, “Enlisting NATO to Address the China Challenge,” Center for a New American Security, 10—5—20, <https://www.cnas.org/publications/commentary/enlisting-nato-to-address-the-china-challenge>, accessed 4-22-22]

Moving forward, the DoD should enlist NATO in efforts to address the China challenge. As a first step, the United States should work to foster a shared transatlantic assessment of the challenges China poses. As NATO Secretary General Jens Stoltenberg acknowledged, China is moving closer to the alliance. Aside from playing a bigger role in the Arctic, Africa, and cyberspace, China is making investments in new infrastructure and weapon systems.3 Its growing footprint and influence in Europe, as well as its deepening cooperation with Russia, create new challenges for NATO, outlined here.

Second, the Department of Defense should seek new approaches to working with NATO to manage China’s rise. Although the European Union is in many ways better positioned to counter China’s growing influence (through investment screening and export control mechanisms, for example), DoD should more effectively incorporate NATO in its efforts to address the most significant security challenge to the United States.

Challenges China Poses to NATO

China does not pose a direct military threat to most NATO allies. But Beijing’s economic and commercial investments in Europe and its growing technological dominance—in areas ranging from artificial intelligence to cyber and robotics—are creating new challenges that influence NATO’s threat landscape. China’s growing footprint and influence in Europe present NATO with the following challenges:

Eroding NATO cohesion and unity. China is undermining European cohesion by negotiating with European governments bilaterally, through the 17+1 and Belt and Road initiatives. Beijing’s divide-and-rule tactics allow it to use its economic influence to buy political leverage, which strains NATO cohesion. Already, shortly after China invested in Greece’s Piraeus Port, Greece blocked an EU statement in the UN Human Rights Council that criticized China’s human rights record.4 China could use its significant economic influence with other NATO members, such as Montenegro and Italy, to coerce those allied governments away from joining consensus at NATO on issues considered inimical to Chinese (or eventually Russian) interests.

Jeopardizing NATO interoperability. China’s sustained technological prowess and innovation present challenges for both the United States and Europe. If the transatlantic partners pursue different approaches to competing technologically with China—either because of differing risk assessments or by implementing different regulations—this would lead to a transatlantic decoupling of technology systems. For example, if some NATO members opted to include the Huawei kit in their 5G networks, NATO (and the United States) could need to exclude those countries from NATO communications and intelligence networks, including the Federated Mission Network. Similarly, while China is supercharging its artificial intelligence (AI) development, the United States and Europe are implementing AI systems at different rates and proposing divergent regulatory approaches to govern the use of AI, which could threaten the interoperability of these systems.5

Eroding NATO’s military edge. The Chinese Communist Party’s military-civil fusion strategy to build the People’s Liberation Army (PLA) into a world-class military hinges on China’s ability to procure dual-use tools, including semiconductors and robotics technology, from the United States and Europe. China seeks to gain a military edge by bolstering its research and development (R&D) spending, investing in critical technologies, and engaging in unfair trade practices such as intellectual property theft and forced technology transfers to acquire Western capabilities. In 2018, China spent $462 billion per year on R&D funding—more than all of Europe’s R&D budgets combined.6 China’s battle for the military edge is evident in artificial intelligence; it seeks to “become a global leader in AI by 2030,” in order to skip a generation of military technology.7 The Chinese Communist Party is working toward this goal by attempting to manufacture advanced semiconductors, to acquire robotics companies and others that underpin AI technology, and to purchase semiconductor manufacturing equipment. These steps will allow China to build its own domestic capacity.8 Over time, Chinese efforts to harness high technology to improve the lethality of their military forces could erode the U.S. and allied military edge. This edge has always depended on using advancements in military technology to win against adversaries who have more forces and assets.

#### China’s edge threatens alliance cohesion

Morcos, CSIS Visiting Fellow ’21

[Pierre Morcos, Visiting Fellow, Europe, Russia, and Eurasia Program, CSIS, “NATO’s Pivot to China: A Challenging Path,” Commentary, Center for Strategic and Internaiotnal Studies, 6—8—21, <https://www.csis.org/analysis/natos-pivot-china-challenging-path>, accessed 4-23-22]

Allies have faced an increasingly assertive Chinese foreign policy as well. Amid the Covid-19 pandemic, Beijing has notably intensified its disinformation efforts directly targeting NATO countries. Beijing has also tried to leverage its close economic ties with some NATO countries through the Belt and Road Initiative to erode allies’ cohesion and unity in an effort to impede criticism of Beijing’s human rights violations and its violations of Hong Kong’s Basic Law. China actively exploits bilateral ties to impede unified positions within the European Union, making it a very easy step to diminish joint positions at NATO on issues contrary to Chinese interests. This dimension of the China challenge underscores the importance of NATO’s political cohesion toward Beijing.

### NATO IL: Interference

#### [x] Attacks threaten NATO operations—emerging vulnerabilities and democratization of technology

Bellasio & Silfversten, RAND analysts, ‘20

[Jacopo Bellasio, Senior Analyst, Defence, Security and Infrastructure, RAND Europe and Erik Silfversten, Co-Director, Centre for Futures and Foresight Studies, RAND Europe, “The Impact of New and Emerging Technologies on the Cyber Threat Landscape and Their Implications for NATO,” CYBER THREATS AND NATO 2030: HORIZON SCANNING AND ANALYSIS, ed. A.Ertan, K.Floyd, P.Pernik & T.Stevens, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), King’s College London, and William & Mary University, 2020, p. 99]

The technologies highlighted in this paper may contribute to the exacerbation of current trends in the cyber threat landscape and herald so-called grey swan scenarios.5 The increasing availability of powerful, easy-to-use and inexpensive technologies is likely to further stimulate the conduct of malicious activities by a wide array of state and non-state actors. The democratisation and ‘servitisation’6 of technology have enabled consumer access to a wide range of technologies that were previously accessible only by governments. This includes enabling technologies like additive manufacturing and largescale distributed computing, to more niche technological services such as ondemand development of bespoke software-defined radio applications that could be used for disrupting the electromagnetic environment. While most of these activities are likely to entail low-tech tactics, this trend could result in an even greater volume of malicious activities than currently witnessed.

The development of new, complex technological solutions and capabilities may also enable state-sponsored actors to conduct advanced, covert or persistent attacks and activities which could undermine or jeopardise NATO’s missions and day-to-day operations by, for example, exploiting unknown vulnerabilities in the NATO supply chain to gain access to sensitive information. Sophisticated and persistent attacks are likely to be less frequent, making these threats more challenging for NATO to identify, detect, prepare for and manage due to limited exposure to and knowledge of the tactics, techniques and procedures (TTP) employed. The proliferation of connected and embedded systems, particularly through a drive towards the Internet of Things (IoT) and the digitalisation of legacy infrastructure may also increase NATO’s attack surface and the likelihood of vulnerabilities that could be exploited by malicious actors.

#### New technological developments will make the problem even worse

Bellasio & Silfversten, RAND analysts, ‘20

[Jacopo Bellasio, Senior Analyst, Defence, Security and Infrastructure, RAND Europe and Erik Silfversten, Co-Director, Centre for Futures and Foresight Studies, RAND Europe, “The Impact of New and Emerging Technologies on the Cyber Threat Landscape and Their Implications for NATO,” CYBER THREATS AND NATO 2030: HORIZON SCANNING AND ANALYSIS, ed. A.Ertan, K.Floyd, P.Pernik & T.Stevens, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), King’s College London, and William & Mary University, 2020, p. 89]

What cyber threats could emerge over the next decade from new and emerging technologies? How could NATO prepare for and manage them? Recent decades have seen a revolution in Information and Communication Technologies (ICTs) and related technology areas. The development, proliferation, widespread use and embedding of ICTs in contemporary societies have resulted in unprecedented change affecting all aspects of human activity, including military and foreign affairs.

In defence, this has been evident in cyber security and network defence, but has also contributed to the growth of hybrid threats1 and wider threats in the information environment. In this context, NATO and its member states are facing growing challenges from state and non-state actors in cyberspace, with threats to the Alliance’s integrity and military operations and to the day-to-day functioning of its institutions (NATO, 2020a).

In parallel with these developments, we have seen significant advances in a wide array of new and emerging technologies that could have disruptive implications to the nature, scope and potential impact of cyber threats to NATO. The pace of technological change is expected to continue in the next decade and may have profound effects on defence and security matters (Kepe et al., 2018). The rapid pace of change, the complexity and the uncertainty of these developments require an understanding of their implications to ensure NATO’s ability to ensure resilience and manoeuvrability in the cyber domain.

### NATO Impact: Economy

#### Strong transatlantic ties are critical to the U.S. economy

Coffey & Kochis, Heritage Foundation analysts, ‘20

[Luke Coffee, Heritage Foundation institute director and Daniel Kochis, Senior Policy Analyst, Davis Institute, Heritage Foundation, “NATO in the 21st Century: Preparing the Alliance for the Challenges of Today and Tomorrow,” SPECIAL REPORT n. 235, 8—10—20, p. 4]

A stable, secure, and economically viable Europe is in America’s economic interest. For more than 70 years, the North Atlantic Treaty Organization (NATO) and the U.S. military presence in Europe have contributed to European stability, which has economically benefited both Europeans and Americans. The economies of Europe, along with that of the United States, account for approximately half of the global economy. The U.S. and Europe are each other’s principal trading partners. The U.S and Europe are each other’s top source of foreign direct investment. All of this brings untold benefits to the U.S. economy and, by extension, the American worker.

### NATO Impact: Hegemony

#### A strong NATO bolsters the U.S.’s military capabilities—important to our global leadership

Lute & Burns, Harvard researchers, ‘19

[Ambassador Douglas Lute, Senior Fellow, Belfer Center and President, Cambridge Global Advisors and Ambassador Nicholas Burns, Professor, Diplomacy and International Politics, Harvard Kennedy School, “NATO at Seventy: An Alliance in Crisis,” Project on Europe and the Transatlantic Relationship, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2—19, p. 41-42]

As a military alliance, NATO’s most important contribution to American interests is security. Above all, NATO has helped keep the peace in Europe after centuries of division and war. NATO has invested for decades in the ability of its members to operate together—so-called “interoperability”— based on practiced procedures, common standards and NATO’s historically unique integrated military command structure. Many of NATO’s partners also share in this interoperability. This military potential means that when America faces security challenges anywhere, it has ready teammates based on NATO, either with the Alliance as a collective whole or with select allies to form a purpose-built military coalition. Further, NATO allies provide America basing and access rights across Europe; bringing U.S. forces a continent closer to trouble spots in the Middle East, Africa and beyond, and providing improved response times and sustainability. Bases like Lakenheath in the U.K., Ramstein in Germany, Aviano in Italy, Rota in Spain, Souda Bay in Greece and İncirlik in Turkey are strategic assets. NATO allies employ tens of thousands of intelligence personnel, extending the reach of the United States’ eyes and ears.125 In short, NATO reinforces America’s national military strength with increased scale, diversity and geographic position.

NATO is not perfect. This report addresses the array of significant challenges the Alliance must face. At heart, however, Americans must remember that a Europe “whole, free and at peace” is fundamentally in the U.S. interest and NATO is America’s primary bridge across the Atlantic.126 In fact, most Americans continue to support NATO overwhelmingly.127 America by itself enjoys great human capital, vast resources and favorable geographic position. Together with its allies, both in NATO and in East Asia, America holds an unmatched geo-strategic advantage over any potential competitor, today and for the foreseeable future. America’s main strategic competitors, China and Russia, do not compare. Sustaining this strategic advantage by nurturing and investing in alliances, beginning with NATO, is therefore in America’s vital national interest. Allies are the ultimate guarantee of American security and prosperity.

#### Strong relations are key to U.S. leadership and checking rising authoritarianism

Nuland et al., Albright Stonebridge Group senior Counselor, ‘20

[Victoria Nuland, Senior Counselor, Albright Stonebridge Group, Non-Resident Senior Fellow, Brookings Institution, Christian Mölling, Director of Research of the German Council on Foreign Relations, and Sophia Becker, Research Fellow for U.S. Security and Defense Policy at the German Council on Foreign Relations, STRONGER TOGETHER: A STRATEGY TO REVIALIZE TRANSATLANTIC POWER, Belfer Center for Science and International Affairs, Harvard University and German Council on Foreign Relations (DGAP), 12—20, p. 27]

At its core, it is a resource question: Can the U.S. advance its global interests without Europe, or, more precisely, would a world without NATO and strong U.S.–EU relations be cheaper for the U.S. or for Europe? The answer is: no. One of the America’s greatest strategic advantages are its alliances and partnerships. From a European perspective, the most fundamental truth about NATO has not changed since 1949: Europe cannot yet guarantee its own security without the U.S., given the capability gaps in European armed forces. Nor can it address the myriad other security challenges it faces from China, to terrorism, to technological dependence to climate change without effective U.S.–EU cooperation. Finally, if the democratic world is going to mount a successful defense against authoritarian states’ efforts to rewrite global norms in their own favor, the family of NATO and EU nations must make up the core of that defense.

### NATO Impact: Liberal Order

#### Allied coop key to the liberal order—the U.S. can still rebound

Rapp-Hooper, Council on Foreign Relations senior fellow, ‘20

[Mira Rapp-Hooper, Senior Fellow for Asia Studies, Council on Foreign Relations, “China, America, and the Interntional Order After the Pandemic,” WAR ON THE ROCKS, 3—24—20, <https://warontherocks.com/2020/03/china-america-and-the-international-order-after-the-pandemic/>, accessed 6-9-22]

Finally, the United States ought not simply recommit itself to its capable European and Asian allies, but make allied coordination the basis of its strategy going forward — against traditional military threats, as well as those that may be less visible and just as deadly. As is more evident by the day, the alternative is a system in which Washington is increasingly sidelined. If China exits this epochal crisis as a confident leader it will not be the ineluctable result of a structural shift; Beijing will have Washington’s calamitous domestic mismanagement and myopic foreign policy to thank for it. If, as part of its own recovery, however, the United States can return itself to a strategy that seeks domestic security and prosperity through international cooperation, it stands a chance of helping to build new forms of order that prevent the next crisis. The prospect feels dimmer but is not yet lost.

#### Reforming NATO bolsters the liberal international order

von Voss, German Council on Foreign Relations officer, ‘19

[Alicia von Voss, Program Officer, Security, Defense and Armaments Program, German Council on Foreign Relations (DGAP), “NATO’s Future Role in the Multilateral Rules-Based Order,” NEW PERSPECTIVES ON SHARED SECURITY: NATO’S NEXT 70 YEARS, 11—28—19, <https://carnegieeurope.eu/2019/11/28/nato-s-future-role-in-multilateral-rules-based-order-pub-80412>, accessed 4-25-22]

If NATO sees itself as an alliance that supports the liberal international order as much as the defense of Europe, it must prepare to help its partners counter—or, better still, preempt—the challenge to this order from China and Russia. That order is worth defending for the simple reason that it remains the best framework for a system comprising many players.

That said, institutions such as NATO that reflect the past will need to adjust to the new reality of global power distribution. Institutions have to solve problems for people to consider them relevant.17 When those problems and circumstances change, so should policies. For NATO, this means that the alliance may need to make contingency plans to relieve U.S. forces in the Atlantic, the Middle East, and Africa if they are required in the Pacific. The alliance may also need to strengthen its support to the EU in Eastern European countries that are being actively courted by Chinese and Russian diplomacy backed up by promises of developmental projects.

NATO can also shape the emerging global order by holding steady to, and universalizing, the principles and practices that make it successful: being a magnet for countries in transition to representative government, protecting countries that share the alliance’s values, and working hard to mold national interests into cooperative internationalism.18 More specifically, NATO needs to strengthen partnerships with like-minded countries such as Argentina, Australia, Chile, Japan, Mexico, New Zealand, and South Korea. The alliance needs to find ways to penalize Russia and China for assaults against weaker states. And NATO must effectively motivate countries in transition, such as Ukraine, to keep adopting better governance and rule of law practices that align with the coalition’s expectations.

Finally, NATO can help forge the coming multilateral world order because it has the capacity to constantly evolve and adjust to new security environments. The allies should apply that spirit of adaptability to support reform of the UN Security Council, which is woefully unrepresentative, and strengthen the UN’s powers to enforce rules that have been adopted by consensus. Stronger institutions help free societies prosper and constrain illiberal challengers.

Fortunately for NATO, the alliance is representative, and its members are empowered, active, and used to finding mutually agreeable solutions. That is why NATO is both perpetually in crisis and the most successful security alliance in modern history.19

### NATO Impact: Multiwarrant

#### Strong NATO undergirds the global system and allows us to address multiple threats

Gallagher, U.S. Representative and Dueck, George Mason professor, ‘19

[Mike Gallagher, U.S. Representative, Wisconsin & Colin Dueck, Professor, Schar School of Policy and Government, George Mason University, “The Conservative Case ofr NATO, NATIONAL REVIEW, 1—30—19, <https://www.nationalreview.com/2019/01/nato-western-military-alliance-bolsters-american-interests/>, accessed 5-3-22]

“The Conservative Case for NATO”.

The conservative case for NATO is not that it strengthens liberal world order. Rather, the conservative case for NATO is that it bolsters American national interests. In an age of great-power competition, as identified by the Trump administration, America’s Western alliance provides the U.S. with some dramatic comparative advantages. The United States, Canada, and their European allies have a number of common interests and common challenges with regard to Beijing, Moscow, terrorism, cyberattacks, migration, nuclear weapons, and military readiness. NATO is the one formal alliance that allows for cooperation on these matters. It is also the only alliance that embodies America’s civilizational ties with Europe — a point forcefully made by President Trump when he visited Poland in 2017. Properly understood, NATO helps keeps America’s strategic competitors at bay, pushing back on Russian and Chinese influence. In all of these ways, the U.S. alliance system in Europe is a bit like oxygen. You may take it for granted, but you’ll miss it when it’s gone.

### NATO Impact: Russia War

#### Cohesion checks Russia attack

Hall & Sandeman, London School of Economics researchers, ‘21

[Jonny Hall, PhD Candidate, International Relations, London School of Economics and Political Science and Hugh Sandeman, Visiting Senior Fellow, LSE Ideas and Project Head of Global Strategies, “NATO and the Future Character of Warfare,” Strategic Update, LSE IDEAS, London School of Economics, 9—21, p. 12]

This limit to NATO’s cohesion is central to Russian thinking about future warfare in Europe. Russian caution about the ability to prevail against a united NATO alliance in a prolonged conflict is consistent with a focus on the initial stages of conflict, and on exploiting the potentially divisive political impact on NATO of a sudden outbreak of hostilities followed by a rapid fait accompli. Any such operation would likely be designed to fragment NATO as swiftly as possible, undermining the coherent political and military response needed for rapid reinforcement, general mobilisation, timely escalation, and the restoration of deterrence.

Russia would seek to impose its own rules of warfare in any conflict with NATO, as it did in Crimea.26 It could exploit NATO’s lack of nuclear deterrence in Europe, where Russia has developed and exercised the forces and strategies needed for threatening to use nuclear weapons, for the purposes of sudden escalation. Alternatively, Russia could deploy calibrated kinetic terror against a NATO state or part of a state, to demonstrate the costs of a wider war. Cyber sabotage could also be widely used for the same purposes. All these actions—in line with the strategies of unpeace and information warfare—would be aimed at fragmenting the unity within NATO that would be necessary for a coherent political and military response.27 The fundamental objective would be a realignment of political forces in Europe, rather than seizing and holding territory. The importance of speed in bringing pressure to bear on NATO, and in achieving rapid military and political impact, was demonstrated in the Russian mobilisation of troops and armour on the eastern border of Ukraine in April 2021.

In contrast to the West, Russia has explicitly linked resilience to the possibility of war, reflecting a close integration of the political and military aspects of security. It has sought to instil among the Russian public a degree of resilience to the possible impact of conflict, by means of domestic propaganda and warnings concerning the ongoing dangers of nuclear war.28 In this respect, Russia appears to be focused as much on characteristics of war that remain unchanged, as it is on technological and other determinants of future warfare.

### NATO Impact: Stability

#### NATO is necessary to address several global threats

Netherlands Ministry of Foreign Affairs, ‘22

[Netherlands Mnistry of Foreign Affairs, “What Does NATO Do? Foreign Affairs in Plain Language,” 3—21—22, <https://www.government.nl/latest/news/2022/03/21/what-does-nato-do-netherlands-safety>, accessed 6-4-22]

Safety and security in the Netherlands

A safer world also means a safer Netherlands. Why? Take for instance terrorism, nuclear weapons or cyberattacks. These threats have one thing in common: they don’t stop at borders.

So our own safety and security often starts abroad. That’s why it’s important to have good relations with other countries. And to protect stability in the world together. The Ministry of Foreign Affairs works hard to do this. NATO also plays an important role. But what exactly is NATO?

What is NATO?

NATO stands for ‘North Atlantic Treaty Organization’. It is a military alliance of 30 countries in Europe and North America. Its headquarters is in Brussels. The Netherlands is a member of NATO. NATO was set up in 1949, not long after the end of the Second World War. Its aim: to protect the security and freedom of all the countries that are members (the Allies). And right now, that Alliance is perhaps more important than ever.

Worldwide security challenges

The world is a less safe place than before. Even in areas near the Netherlands. Take for instance the war in Ukraine started by President Putin. Or China: a growing global economic and military power that is flexing its muscles more and more often. Technological developments also lead to new threats, like cyberattacks. Or the use of modern weapons, like drones, that can attack targets without humans having to risk their lives.

And climate change can also lead to more conflicts, or make conflicts worse. Countries need each other so they can prevent and combat these global threats.

NATO and diplomacy

NATO is a defensive military alliance. You might think NATO is all about military action. But there is another very important step that comes first. NATO’s main priority is diplomacy. By talking to each other and with other countries, we try to solve conflicts without using force.

Within NATO, the Allies work together and make agreements. For instance on protecting democratic values. Examples are: being able to hold free and fair elections, equal rights for everyone, and freedom of expression.

Within NATO, military and non-military experts meet to exchange information about what is happening in the world. In this way, NATO prepares itself for the challenges and threats of today and of the future. With military and diplomatic action.

NATO in the world

NATO also helps other countries – that aren’t members of NATO – with their security. For instance by helping them train their soldiers. NATO soldiers can also be sent to deal with a crisis. This is important for the Netherlands too. Because the world is becoming more and more closely connected. And our safety and security is also connected to that of other countries.

### NATO Solvency: Cyber Cooperation

#### Cyber cooperation helps address rifts that threaten alliance cohesion

Nuland et al., Slbright Stonebridge Group senior Counselor, ‘20

[Victoria Nuland, Senior Counselor, Albright Stonebridge Group, Non-Resident Senior Fellow, Brookings Institution, Christian Mölling, Director of Research of the German Council on Foreign Relations, and Sophia Becker, Research Fellow for U.S. Security and Defense Policy at the German Council on Foreign Relations, STRONGER TOGETHER: A STRATEGY TO REVIALIZE TRANSATLANTIC POWER, Belfer Center for Science and International Affairs, Harvard University and German Council on Foreign Relations (DGAP), 12—20, p. 26]

The tense atmosphere between Washington and European capitals has exacerbated internal rifts in the Alliance—some of which are as old as NATO itself. Because collective deterrence and defense are entirely built on the credibility of each member’s commitment to Article 5 of the North Atlantic Treaty, these divisions risk rendering the Alliance ineffective and vulnerable to external threats. The EU continues to be plagued by NorthSouth and East-West tensions. Post-Brexit, the UK is also recalibrating its relationships with the EU, NATO and the U.S.

Tensions on issues beyond the military realm from trade to China to technology further undercut the transatlantic commitment to raise and maintain defense spending to the NATO standard of 2% of GDP, with Germany the leading backslider on its 2024 pledge. This problem will be exacerbated by the deep recession on both sides of the Atlantic precipitated by COVID-19 and the high cost of recovery.

Recent European calls for strategic autonomy have raised hackles in Washington and also revived the specter of NATO–EU rivalry without yet increasing military capability. While the creation of the European Defense Fund is promising, Europeans will be hard-pressed to increase defense spending until their economies fully recover. The EU lost 20% of its military throw-weight when the UK exited and remains far from autonomous in all but modest-sized operations. However, the U.S. will not get more security help from Europe by browbeating Allies in public or fear-mongering about European autonomy.

Washington will be more successful in maintaining spending levels and addressing capability gaps through targeted mentoring of individual Allies and partners and offers of co-development of key systems. In particular, Washington should help Allies keep pace in addressing the security challenges posed by adversaries’ cyber weapons and advancements in AI, quantum computing and autonomous and space weapons. At the same time, the U.S. should welcome any level of autonomy that Europe can achieve in keeping itself safe. The more Europeans can do on their own, the less the U.S. burden for their defense.

### NATO Solvency: Resilience Strategies

#### Resilience aid key to cohesion

Pernik & Jermalavičius, International Centre for Defence & Security analysts, ‘16

[Piret Pernik and Tomas Jermalavičius, Research Fellows, International Centre for Defense and Security “Resilience as Part of NATO’s Strategy: Deterrence by Denial and Cyber Defense,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. 101]

NATO also sets its emphasis on infrastructure, civil preparedness, continuity of services, accumulation of reserves and ensuring access to them as well as on various procedures facilitating rapid crisis response .Its major concern is that the Alliance has come to rely heavily on the private sector when moving, deploying and sustaining its forces; therefore it devotes much attention to civilian capabilities and civil-military interaction. This is understandable given its role as a “military responder” and “force multiplier” in military conflicts.Just asthe EU, it should not, however, neglect its role in helping countries—both allies and partners—maintain their ability to reform themselves in the face of adversity.After all, astheWarsaw Summit statement states, “The foundation of our resilience lies in our shared commitment to the principles of individual liberty, democracy, human rights, and the rule of law.”7 Should this commitment fall apart, the Alliance’s cohesion, solidarity and very existence will be endangered.

#### Resilience key to NATO—weakest link

Hall & Sandeman, London School of Economics researchers, ‘22

[Jonny Hall, PhD Candidate, International Relations, London School of Economics and Political Science and Hugh Sandeman, Visiting Senior Fellow, LSE Ideas and Project Head of Global Strategies, “NATO’s Resilience: The First and Last Line of Defence,” Strategic Update, LSE IDEAS, 5—22, London School of Economics p. 9-10]

The tendency to conflate Article 3 resilience obligations and the wider responsibilities of the “baseline” requirements was carried over into the Strengthened Resilience Commitment. The 2021 Summit Communiqué spoke of NATO adopting “a more integrated and better coordinated approach, consistent with our collective commitment under Article 3 of the North Atlantic Treaty, to reduce vulnerabilities and ensure our militaries can effectively operate in peace, crisis and conflict”.20 It was agreed that “allies will develop a proposal to establish, assess, review and monitor resilience objectives to guide nationally-developed resilience goals and implementation plans”. 21 Each individual ally was to decide how to do this.

Apart from the potentially troublesome issue of how numerous national resilience goals may or may not aggregate into “collective resilience”, there is a challenge of how to create common standards when resilience remains the responsibility of individual members. This problem is particularly apparent in terms of concerns about “weak links” within NATO. When outlining the forthcoming Strategic Concept, Secretary General Stoltenberg noted in his discussion of resilience that “this must be a collective effort … because we are only as strong as our weakest link”.22 Concerns about “weak links” within NATO have grown in the post-Cold War era. Not only has NATO relied on internal cohesion around the significance of liberal values to provide its continuing rationale after the dissolution of the Soviet Union,23 but the diffusion of power in the contemporary international security environment means that American military might cannot alone provide the balancing force it once did. This makes national resilience all the more important.

#### [x] Resilience is critical to NATO’s effectiveness—must be able to respond to outside attacks

Psychogiou, Finabel researcher, ‘22

[Vasiliki Psychogiou, Finabel research intern, “Cyberspace: Is NATO Doing Enough?” Finabel—European Army Interoperability Centre, Info Flash, 2—22, p. 4]

NATO remains associated with more classical military operations outside its territory. However, today’s nonconventional threats can originate just as easily from within and outside NATO’s borders (Shea, 2020). Thus, NATO needs to constantly enhance its resilience capacity to better achieve early warning of attacks, best limit the damage and recover as quickly as possible (Shea, 2020). NATO can also share its leadership and decisionmaking with civilian actors outside the conventional military chain of command (Shea, 2020). Coherent policies with a common denominator that the Allies are all willing to support can empower NATO’s posture (Shea, 2020; NATO, 2021; NATO, 2020; Deschaux-Dutard, 2021; Brent, 2019; Shea, 2020).

### NATO Solvency: Tech Independence

#### Independent tech capabilities key to resisting Chinese influence in NATO

Nietsche et al., CNAS Research Associate, ‘20

[Carisa Nietsche, Research Associate, CNAS Transatlantic Security Program, Jim Townsend, former Deputy Assistant Secretary fo Defense and Adjunct Senior Fellow, CNAS and Andrea Kendall-Taylor, Senior Fellow, CNAS, “Enlisting NATO to Address the China Challenge,” Center for a New American Security, 10—5—20, <https://www.cnas.org/publications/commentary/enlisting-nato-to-address-the-china-challenge>, accessed 4-22-22]

\* China’s penetration of Europe through its high-tech capabilities and low-tech acquisition of ports and rail lines can pose problems for NATO, including slowing military mobility, providing Beijing (and possibly Russia, at some point) with intelligence on allied force movements, and compromising NATO command and control. Undue Chinese influence in some allied capitals can also be used to coerce those governments from joining consensus at NATO on issues considered inimical to Chinese (or Russian) interests.

\* To combat this influence, NATO must make sure that allies are able to fill their capability gaps through homegrown solutions, not purchases of Chinese technology. NATO should also work with the European Union, including to jointly develop a review mechanism that considers Chinese purchases of critical infrastructure in Europe and supply chain security.

# Resilience Aff: Russia / Hybrid Extensions

### Hybrid Status Quo: Current policy Fails

#### Current efforts are inadequate—we need a coordinated policy

Speranza, Center for European Policy Analysis director, ‘20

[Lauren Speranza, Director, Trans-Atlantic Defense and Security, Center for European Policy Analysis, “A Strategic Concept for Countering Russian and Chinese Hybrid Threats,” Scowcroft Center for Strategy and Security, Atlantic Council, 7—20, p. 10-11]

Indeed, all of these efforts, among others, have helped transatlantic policymakers and publics better understand hybrid threats, build new tools to combat them, and develop the legal frameworks and mandates to take action, especially at the tactical level. Yet, even these efforts have failed to deter Russia and China from using hybrid activities. Despite the utility of many of these transatlantic efforts, the whole is less than the sum of its parts for three overarching reasons.

First is the lack of understanding. Transatlantic governments have each compiled different threat assessments based on their individual experiences with hybrid activities, which has complicated the formation of a common understanding of hybrid threats. Due to a lack of integrated analytical capabilities, information-sharing obstacles, and sensitivities around nations revealing their vulnerabilities, the transatlantic community has yet to develop a full understanding of the impacts of hybrid activities and how they connect across contexts. Relatedly, nations and institutions often hesitate to use real-world scenarios when exercising responses to hybrid threats out of fear of publicly failing to navigate them. Opting for imagined scenarios, which often lack sufficient nuances and complexities, inhibits their ability to identify shortfalls and learn which approaches work. All of this has severely limited the effectiveness of transatlantic counter-hybrid efforts thus far.

Second is the lack of sufficient resources. On the whole, transatlantic counter-hybrid efforts remain far too under-resourced in terms of budgets and appropriate personnel. For example, the EU’s East StratCom Task Force has a dedicated budget of just three million euros with only sixteen staff to cover counter-disinformation efforts across the entire EU.34 Similarly, NATO’s quick-response CHSTs are not resourced to be standing forces, so they require significant time to recruit required expertise (think of white-hat hackers, as opposed to one of NATO’s many policy experts), let alone form and deploy. Even when counter-hybrid efforts are well-funded in accordance with stated policy, complex governmental and institutional budget requirements often prevent funds from flowing to specific places where they are needed most. Insufficient resourcing limits the scope of these efforts and their larger strategic effect. In the face of widespread, pervasive, and diverse hybrid activities, this is a huge obstacle.

Third is the lack of coordination on the national and international levels. Cross-cutting hybrid threats often touch numerous parts of governments, requiring tireless coordination among various agencies on everything from intelligence to responses. The national interagency process in most countries also lacks adequate involvement from civil society and the private sector when it comes to counter-hybrid efforts. If not effective at the national level, coordination at the international level is more difficult for the thirty different countries inside NATO or the EU. Inter-institutional cooperation between NATO and the EU becomes almost impossible then, especially given long-standing political and bureaucratic obstacles plaguing their relations. This forces nearly all coordination to be informal, relying on pragmatic personalities and creative solutions among officials to achieve results. On top of everything, there is no single platform to convene relevant authorities from NATO, the EU, their nations, the private sector, and civil society to coordinate. As a result, transatlantic counter-hybrid efforts have remained largely disjointed, producing a patchwork effect.

In light of this, next-level actions are needed to address the knowledge, resource, and coordination gaps outlined above. An enhanced approach is required to meaningfully deter and limit Russia’s and China’s further use of hybrid actions. In the wake of the coronavirus crisis, the need for NATO and EU nations to focus on domestic political, health, and economic agendas will make coordination on hybrid issues more difficult. At the same time, the crisis underscores that hybrid issues—including those around pandemics—cannot be solved alone. This provides a stronger impetus for cooperation among core transatlantic allies. What is needed now is a much more comprehensive, coherent, and forward-leaning transatlantic strategy for countering Russian and Chinese hybrid threats.

### Hybrid Status Quo: Threat Now

#### Hybrid threats will only grow—we need to step up our response

Speranza, Center for European Policy Analysis director, ‘20

[Lauren Speranza, Director, Trans-Atlantic Defense and Security, Center for European Policy Analysis, “A Strategic Concept for Countering Russian and Chinese Hybrid Threats,” Scowcroft Center for Strategy and Security, Atlantic Council, 7—20, p. 1]

Tackling hybrid threats, particularly from state actors such as Russia and China, remains one of the greatest challenges for the transatlantic community. Hybrid threats have gained more traction among policymakers and publics across Europe and the United States, especially in a world with COVID-19. The recent coronavirus pandemic has thrust hybrid activities to the center of transatlantic debates. Both China and Russia capitalized on the crisis to wage disinformation campaigns against the West, while strategically delivering aid to European countries in attempts to build good will on the international stage. Yet, even as hybrid activities have accelerated, limited progress has been achieved in countering them or deterring competitors from using them. Over the last five years, Euro-Atlantic nations and institutions, such as NATO and the European Union (EU), have taken important steps to respond to hybrid issues. But as hybrid threats become more prominent in the future, policymakers must move toward a more coherent, effective, and proactive strategy for countering Russian and Chinese hybrid threats.

### Hybrid Impact: Credibililty / Global War

#### Disinformation threatens conflict escalation and undermines U.S. credibility

Kavanagh & Rich, RAND analysts, ‘18

[Jennifer Kavanagh and Michael D. Rich, RAND analysts, TRUTH DECAY: AN INITIAL EXPLORATION OF THE DIMINISHING ROLE OF FACTS AND ANALYSIS IN AMERICAN PUBLIC LIFE, RAND Corporation, 2018, p. 218-219]

Policy uncertainty that seems to derive, at least in part, from Truth Decay could also have diplomatic implications. Allies and adversaries that are uncertain about whether to trust prior policy positions taken by U.S. leaders, or that are unable to determine whether a commitment (or, in the case of an adversary, a threat) is authentic, could act in ways that run counter to U.S. interests. For example, an ally that lacks confidence in the strength of a U.S. commitment might turn to another partner for additional support, depriving the United States of a potentially important political or economic relationship. An adversary that believes a prior U.S. position is not an accurate reflection of U.S. intent might challenge the United States and contribute to an escalation of hostilities. Such institutions as the North Atlantic Treaty Organization and the post–World War II alliance structure have reduced some of the uncertainty surrounding diplomatic commitments, but, in the first half of 20th century, there were no such guarantees, and uncertainty was considerably higher. Should Truth Decay contribute to an increase in this uncertainty, it is possible that the risk of unintentional escalation and even conflict would increase.

Finally, as alluded to previously, Truth Decay alongside polarization (one of its drivers) can further exacerbate policy uncertainty with additional domestic and international implications. Policies that are based not on shared and commonly accepted facts but on selective adoption and rejection of facts may be subject to rapid change and reversal when congressional leadership or the presidency changes hands or parties. Polarization exacerbates this tendency, as it increases the ideological distance between policymakers on each side of the spectrum and increases the chances of “policy whiplash” when legislative or executive power shifts from one party to the other. At the domestic level, rapid policy reversals may lead to any number of negative consequences, including financial loss for individuals or corporations, wasted resources at the government and individual level, and instability in economic, health care, or insurance markets that have direct implications for individual constituents. In addition, policy reversals may further undermine trust in key institutions. At the international level, policy reversals compromise U.S. credibility, can harm alliances and partnerships, and risk triggering escalation that may lead ultimately to full blown conflict.

### Hybrid Impact: Democracy—Internal

#### Successful Russian hybrid warfare undermines democracy and the international liberal order

Homeland Security News Wire, ‘17

[staff, “Russian’s Interference in U.S., European Elections Could Be ‘Act of War’: NATO Commander,” HOMELAND SECURITY NEWSWIRE, 3—3—17, <https://web.archive.org/web/20190221152350/http://www.homelandsecuritynewswire.com:80/dr20170303-russias-interference-in-u-s-european-elections-could-be-act-of-war-nato-commander>?, accessed 6-3-22]

Bradshaw, who will become NATO commander later this month, said Russia posed a “hybrid threat” to NATO members.

“It’s not just the threat of overt military attack, but it’s a raft of other measures, including covert, paramilitary, and non-military activities, some of which will be coordinated by the intelligence arms of Russia,” General Bradshaw added.

“And we as NATO need to have our antenna tuned to the signs that this sort of hostile activity is going on.”

He accused the Kremlin of “showing a proclivity to disobey the rules of international relations” with its military incursion into Crimea and alleged backing for rebels in eastern Ukraine.

“We need to put in place thoroughly effective and convincing deterrence so that everybody knows where the red lines are,” General Bradshaw said.

“We are effectively building and sustaining military capability so that we never have to use it.”

Bradshaw’s comments come against the backdrop of growing calls in the United States for a thorough investigations of the Russian government’s broad campaign to secure the election of Donald Trump as U.S. president – and the nature and scope of contacts between several Trump’s surrogates and high-level campaign aides and operatives of the two Russian intelligence services – the FSB and the GRU. These two organizations were behind the hacking campaign against the computer systems of the Democratic Party and the Hillary Clinton’s campaign.

The unanimous conclusion of the seventeen agencies making up the U.S. intelligence community was that “We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election,” in the words of a report released by the Office of the Director of National Intelligence.

“Russia’s goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton and harm her electability and potential presidency.

“We further assess Putin and the Russian Government developed a clear preference for President-elect Trump.”

A recent report by the House of Commons Foreign Affairs Committee said the “rise of fake news” emanating from Russia was a cause of growing concern, pointing to the role of state-owned outlets Russia Today and Sputnik in spreading Russian propaganda and fake news masquerading as journalism.

European intelligence agencies have said that Russia’s success in helping elect Trump to the presidency of the United States has emboldened Moscow to replicated in Europe the methods it used in its interference in the U.S. presidential campaign. European security services have already seen signs of Russia’s hacking and disinformation campaign aiming to help far-right, ethno-nationalist, and populist politicians win the coming elections in France, the Netherlands, and Germany.

As is the case with Trump, these politicians – Marine Le Pen and the National Front in France, the AfD (Alternative für Deutschland) in Germany, and Geert Wilders and his Party of Freedom in the Netherlands – aim to weaken the West by undermining or dismantling the two central pillars of Western post-Second World War security and prosperity – the system of military alliances, including NATO, and the liberal international economic order, including the EU and the WTO.

Not coincidentally, as is the case with Trump, the three European political movements being helped by Russia are openly pro-Russian and critical of Western economic and political sanctions taken to punish Russia for its actions in Crimea and Ukraine.

#### Democratic erosion undermines the global order—risks war and an inability to solve other existential threats

Beck, MPS, Stellenbosch University, ‘20

[Cassidi Beck, “The Rise of Strongmen Leaders: A Threat to Global Security,” MPS Thesis, Faculty of Arts and Social Sciences, Stellenbosch University, supervised by Dr. Derica Lambrechts, 3—20, p. 81-86]

With the rise of Strongmen like Orban, Putin and Erdogan, where these populists have accessed government, a subsequent erosion of liberal democratic principles has been followed (Albertazzi & Mueller, 2013:350). Authoritarian countries are openly challenging global rules and ideas about freedom and making the case that their socio-political systems work better than liberal democracy. These Strongmen pose a “substantial negative effect on democratic quality” (Huber & Schi`mpf, 2017:146 as they “increasingly reject liberal values” (Cederman, 2019:61).

Even if one disagrees with Francis Fukuyama’s thesis, there is still evidence that highlights that, despite its shortcomings, democracy inherently has important tenants that other regimes do not offer. Democracy stresses the intrinsic importance of transparency, civil liberty, rule of law, horizontal accountability, and minority rights. It guarantees fundamental rights and civil liberties – freedom to pursue one’s legitimate interests, to hold political, social and cultural beliefs, and to be able to express them without interference from the state (Albertazzi & Mueller, 2013:350; Mounk & Fao, 2018). High-minded defenders of liberal democracy argue that there is something uniquely legitimate about the political system. Its democratic element, they claim, ensures citizens’ equality, while its liberal element ensures citizens’ freedom. As such, the genius of liberal democracy is that it can honour both these values simultaneously. It allows each citizen access in the public sphere while giving them the ability to have a private life; “only liberal democracy can fulfil some of the deepest and most universal human aspirations” (Mounk, 2018:129-130).

Thus, in conclusion, the use of Fukuyama’s original essay The End of History and the Last Man is not to disagree with or critique his thesis. It is rather a reflection on his thesis and posits that political events currently arising pose an obstacle to this perceived future. Rather, to highlight that current events, specifically the rise of political Strongmen, are incompatible with a future that was believed to be marked by democracy, stability and security. The turbulence of current geopolitics does not have to be read as a rebuttal of Fukuyama’s original thesis, however, an assessment of Strongman leadership and the fluctuations such leadership may bring towards geopolitics are an important contrast to what Fukuyama predicted. The next section will examine more specifically the possible outcomes these Strongmen could have on geopolitical security – the ramifications of their tendency to erode democratic institutions, to violate human rights, promote nationalistic populism and break the principle of sovereignty and international law.

4.3. The Strongman’s Ramifications for Geopolitical Security

Although the rise of the Strongman and their illiberal democracy offers an alternative to democracy, their actions, policies and leadership style indicate that they pose a risk to geopolitical security. In an increasingly connected and globalised world, what appears to be local in nature is in fact global in impact as most elements contain global dimensions (Kaldor, 2001). These rising and existing Strongmen across the globe and their leadership style has the potential of negative ramifications for global security. The actions undertaken by leaders such as Putin, Orban and Erdogan towards democratic institutions, human rights and international law, as well as their nationalistic populism will likely have a far-reaching impact. As noted in Chapter Three, in a regional capacity these leaders have not only undermined their nations’ democracy but have also created an environment of hostility and insecurity. Reflecting on Chapter Three, the next section will examine how these Strongmen’s ability to create regional instability could possibly lead to geopolitical instability and insecurity.

4.3.1. A New Global Order

US Hegemony or “the American century” was born amid the collapse of the Berlin Wall in 1989 and the end of the Cold War (King, 2017:215; Zakaria, 2019:10). Following the collapse of communism, it seemed the West’s model of liberal democracy and free-market capitalism, supported by a clear set of US-sponsored international rules, would spread across the globe. Under the guise of the Washington Consensus, it laid the foundations for recommendations on how nations should interact with one another on the premise of creating wealth and championing liberal democracy (Banos, 2017:92; Rose, 2019:11). In the advocating of the Washington Consensus, the foundation of international law was said to be based on the principles of mutual respect for sovereignty and territorial integrity; non-aggression towards others, non-interference in the internal affairs of others, equality and mutual benefit, peaceful co-existence, respect for human rights and basic freedoms and national self-determination (Banos, 2017; King, 2017; Rose, 2019:11).

However, politically and economically, the West’s vision has seemed to reach its limits, as geopolitical and ideological rivals undermine the foundations of the liberal world order (Frankopan, 2018:52; Kazan & Park, 2019; Russell-Mead, 2018:15). Mounting opposition from emerging superpowers, increasing resistance to globalisation and the core tenants of liberal democracy from emerging political movements, and the rise of political Strongmen across the world, could lead to the creation of a new world order. This rebalancing of power with Strongmen at the helm could have potential implications for global security, as nations like Russia, Hungary and Turkey forge their own political orthodoxy (Banos, 2017:121; Frankopan, 2018:147; Weiss, 2019:92).

Evidence suggests that the new world order, one not championed by a liberal consensus, could potentially lead to a more insecure geopolitical future. This argument extends from the Strongman’s tendency to reject the international rules-based system, as previously noted by Putin, Erdogan and Orban’s dismissal of international law, treaties and the core principle of sovereignty. While the new world order will still be based on a foundation of rules, scholars argue that with Strongmen becoming more prominent and powerful, the resulting new norm will be characterised by geopolitical competition, doubts about security commitments to allies, challenges to the fundamentals of the global trading regime and the abandoning of the promotion of freedom and democracy; these will become the defining features of a new foreign policy (Daalder & Lindsay, 2018:72; Haass, 2019:30; Kazan & Park, 2019). As Orban, Putin and Erdogan have shown, there will be little regard for democratic institutions and tenants, civil rights and political freedoms will be restrained while international law and the principle of sovereignty will hold little value. This could have the potential of escalating rivalries and thus create unstable implications for global security (Frankopan, 2018:144).

This new global order could also potentially see the end of important international institutions and treaties, such as the Trans-Atlantic partnership, the EU, the World Trade Organisation and the International Monetary Fund. International institutions are important as they provide the framework within which countries can happily engage with each other and, help co-ordinate the actions of different countries in order to set stable expectations (Blackwill & Harris, 2016:74; Frankopan, 2018:237). Treaties and international institutions also help to foster security as they provide frameworks through which countries interact, creating cooperation, helping to foster mutual understanding and stability (Haass, 2019:30; Frankopan, 2018:222; King, 2017:225). They also help foster global security as through their creating of cooperation they help to ensure a global response to the creation of solutions for global problems.

Many global issues and threats such as climate change, the refugee crisis, growing terrorism and rising socioeconomic inequalities require the harmonizing of domestic and foreign policies and the willingness of countries to work together. Therefore, without established and agreed upon institutions, the way in which states interact with each other could potentially be characterised as strained and difficult. Future security threats demand a more pluralistic response that can be best accomplished by combining resources (Drozdiak, 2017:91; Frankopan, 2018:74). Prosperity and well-being may depend on global solutions. However, under the guise of leaders like Orban, Putin and Erdogan, many politicians and governments are taking steps to diminish co-operation with each other, disengaging from bilateral agreements and international co-operation. Instead these leaders erode confidence in international institutions and perceptions of stability as they “operate on a tornado of impulses” (Frankopan, 2018:157). As the Strongman is more likely to choose aggression and isolationism over collaboration and cooperation, the world could possibly descend into further conflict as frictions are elevated (Haass, 2019:30; Kazan & Park, 2019; King, 2017:244).

A world order led by Russia under Vladimir Putin, with the support of Turkey’s Erdogan and Hungary’s Orban, would possibly be one characterised by competition over cooperation, protectionism rather than free trade, authoritarianism rather than democracy. Henceforth, evidence suggests that the possible thawing of the liberal democratic world order could be problematic to geopolitical security (Mounk, 2018:114).

An extension of this new global order and how it could potentially lead to increased geopolitical security is that the Strongman’s disregard for democratic norms is contributing to a growing sense of license among autocrats worldwide (Diamond, 2019:20). As more Strongmen come to power and are able to enact their policies, their ‘successful run’ at authoritarianism is making it easier for it to thrive elsewhere. Albright (2018:246) argues that herd mentality is powerful within international affairs and if one leader can follow a specific form of leadership, other leaders around the world are likely to observe and mimic. Thus, with growing assertiveness, disregard for international law yet few consequences and increased economic success, more leaders are turning towards the ‘Strongman playbook’. Strongmen such as Putin, Orban and Erdogan look to others for help in endorsing their regime, favouring one’s authoritarian adversaries over democratic allies (Albright, 2018:246; Mounk, 2018:2). Nudging followers away from the consensus and support for democratic norms, these leaders portray an image that this type of illiberal, autocratic leadership is acceptable (Lendvai, 2017:198). Once where a nation may have consistently held another nation and its leadership in discontent, once in power, the strongman may reverse this decision and instead seek to build a trusting, cooperative relationship (Kearns, 2018:4). For instance, despite the actions of some states towards the negation of human rights and democracy, Russia under Putin has increasingly used its power status to shield other authoritarian states from international demands to protect human rights and block interventions that would force governments to end abuses (Weiss, 2019:95). By allowing nations to continue with their erosion of human rights and political freedoms of its citizens without consequences, it signals to other authoritarian states and Strongman leaders that their actions are acceptable. This then can potentially lead to the possibility of an increased scale across the globe of human rights abuses as autocratic states are not fearful of harmful consequences. Henceforth, this could have serious implications for geopolitical security as more states negate human rights.

When these actions come from democratic countries that have before been strong advocates of democracy, this reversal can have a harmful effect (Albright, 2018:218), particularly in countries where there are already few checks on executive power. The issue with a leader showing these characteristics, especially in a free, liberal and democratic society, is that it signals to other leaders all over the world with these autocratic tendencies are acceptable. If one leader can argue that the press always lies, or the democratic institutions are erroneous, it becomes difficult to fault another across the globe when they make the same claim (Albright, 2018:5; Nance, 2018).

For example, on the invasion of the Ukraine and the illegal annexation of Crimea, leaders across the globe praised Russia’s decision. The leader of the Hungarian fascist party Jobbik praised Putin and Greece’s Golden Dawn praised Russia for defending Ukraine from “ravens of international usury” and France’s Front National lauded Putin’s courageous position against the international lobby (Snyder, 2018:149). With Putin’s actions, and the endorsement he received from other nations, the impression is given that breaking international laws and sovereignty is acceptable.

Together, these Strongmen are creating an alliance of nations led by strong authoritarian leaders who will increasingly pose a risk to the liberal, democratic world order as democratic states fail to stand up to this alliance or prove to be more successful (Lendvai, 2017:214; Nance, 2018). The current world order has not completely eroded but is spearheaded by the rise of Strongmen into political power. The possibility of a new global order emerges – one that appears to create significant geopolitical insecurity. While the Washington Consensus may be faulted, it did help foster a global environment of cooperation and consideration between states, while helping to promote the principles of liberal democracy. A stable world order requires a stable distribution of power and broad acceptance of the rules that govern the conduct of international relations (Haass, 2019:22). However, what the Strongmen champion poses a risk to increased geopolitical insecurity as their policies and ideologies are often centred on conflict, isolationism and protectionism. Instead, they foster a world of unbalanced power and the formulation of their own rules. Further, as more and more nations create a coalition of Strongmen, it will become increasingly difficult to not only stand up to them but also to foster democracy and stability (Kazan & Park, 2019). In a world of ‘complex interdependence’ (Rose, 2019:19), nations cannot fully operate in isolation and such attitudes that fail to acknowledge this and instead foster relationships based on self-interest can only create instability.

### Hybrid Impact: Democracy—Impacts

#### Spread of totalitarianism risks extinction

Farquhar, University of Oxford scholar, ‘17

[Sebastian Farquhar et al., Project Manager, Future of Humanity Institute, University of Oxford, EXISTENTIAL RISK: DIPLOMACY AND GOVERNANCE, Global Priorities Project, 2017, p. 9-10]

During the twentieth century, citizens of several nations lived for a time under extremely brutal and oppressive regimes. Between them, these states killed more than one hundred million people, and sought total control over their citizens. Previous totalitarian states have not been particularly durable chiefly due to the problem of ensuring orderly transition between leaders, and to external competition from other more liberal and successful states. However, there is a non-negligible chance that the world will come to be dominated by one or a handful of totalitarian states. If this were to happen, external competition would no longer threaten the durability of such states to the same extent. Moreover, improvements in certain forms of technology may make it easier for totalitarian states to maintain control, for example by making surveillance much easier. Global totalitarianism could exacerbate other existential risks by reducing the quality of governance. In addition, a long future under a particularly brutal global totalitarian state could arguably be worse than complete extinction.

#### Democracy is key to solving a laundry list of impacts

Chollet et al., German Marshal Fund of the United States Executive VP, ‘17

[Derek Chollet et al., Executive Vice President and Senior Advisor, Security and Defense Policy, German Marshall Fund of the United States, with 9 additional authors, BUILDING ‘SITUATIONS OF STRENGTH’: A NATIONAL SECURITY STRATEGY FOR THE UNITED STATES, Brookings Institution, 2—17, p. 3-4]

We believe that abandoning traditional U.S. support for the international order would be a serious strategic error that would leave the United States weaker and poorer, and the world more dangerous. It would encourage revisionist states to destabilize Europe, East Asia, and the Middle East. It would reduce global economic growth and leave us vulnerable to a new financial crisis. And it would damage efforts to tackle shared challenges like terrorism, nuclear proliferation, and climate change that have very real— and potentially very damaging—impacts here at home. The last time an unraveling of an existing international order occurred was in the 1930s, and the result was depression and world war. Indeed, much of the violence and disorder we see in the world today results from the weakening of the current order. Moreover, the existing order must be assessed relative to the plausible alternatives. The best case outcome in light of an American retreat from the international order is a spheres of influence system whereby China dominates much of East Asia, Russia dominates much of Eastern and Central Europe, and the United States is preeminent in its own hemisphere and possibly Western Europe. Spheres of influence approaches to international order are inherently unstable, largely because the lines of demarcation are contested. It is a configuration prone to great power conflict. And the process of transition from an open global order where small nations have rights to a more imperial model would be particularly fraught.

### Hybrid Impact: Liberal Order—Internal

#### [x] Russian hybrid strategies weaken the alliance and threaten the U.S.-led international order

Speranza, Center for European Policy Analysis director, ‘20

[Lauren Speranza, Director, Trans-Atlantic Defense and Security, Center for European Policy Analysis, “A Strategic Concept for Countering Russian and Chinese Hybrid Threats,” Scowcroft Center for Strategy and Security, Atlantic Council, 7—20, p. 13-15]

For Russia, hybrid warfare is a set of means for it to roll back the post-Cold War settlement and undermine the predominantly US-led, rules-based international order to regain clout as a major player on the global stage. The Kremlin’s key objectives to that end include: dividing and weakening NATO and the EU, both of which the Kremlin sees as a threat; subverting pro-Western governments and institutions; promoting pro-Russia policies; expanding Russia’s sphere of influence (geographically, economically, politically, etc.); and establishing a “moral equivalence” between Russia and the West.3 Moreover, hybrid activities help the Kremlin pursue these goals in a more effective and realistic way. Its leaders recognize Russia cannot necessarily counter or outright compete with the West militarily, technologically, or economically. By employing hybrid methods as part of an overarching strategy of intimidation, however, the Kremlin can have significant influence over international affairs.4

Russia’s hybrid toolkit is multi-level and often country specific, which has made it highly effective and difficult to combat. In its most widely known example, Russia used below-threshold force to illegally invade eastern Ukraine and annex Crimea. The Kremlin has also used proxies and privately contracted forces to influence the outcome of conflicts abroad, from Syria to Libya. Other examples of Russia’s low-level uses of force include attempted assassinations of pro-Western leaders and the use of deadly chemical attacks to target political enemies on foreign soil. In terms of cyber and operational activities, Russia has conducted reckless and dangerous cyberattacks, infiltrated critical infrastructure in the United States, and manipulated gas pipelines, electric grids, and financial systems in Eastern Europe and beyond to increase its leverage abroad.

With respect to political subversion and economic coercion, Russia has interfered in elections in the United States and across Europe in attempts to divide transatlantic populations and influence the outcomes toward candidates the Kremlin views as favorable to Russia. Other tools and tactics include: bribing officials in foreign countries; financing anti-European parties in Central and Eastern Europe to promote pro-Russian narratives; and investing in strategic sectors in foreign countries to maximize dependency on Russia. On the information-warfare front, the Kremlin has orchestrated widespread disinformation campaigns and strategic hack-and-release efforts designed to sow doubt, create chaos, and sway public opinion in its favor on key policy issues.

While Russian hybrid activities can be traced much further back than these examples—including to the major cyberattacks in Estonia in 2007 and the Russo-Georgia conflict in 2008—they have been steadily increasing since the Kremlin’s illegal annexation of Crimea in 2014. Looking ahead, several elements could impact the future course of Russia’s hybrid actions. First are the constitutional changes that Russian President Vladimir Putin has pushed through national courts to reset presidential term limits.5 The reforms allow Putin to remain in power until 2036, or possibly for life, pending a final national referendum.6 With his grip on power soon to be cemented, Putin is likely to attempt more aggressive hybrid actions, knowing the domestic political risks for him are low.

Another factor is the 2020 coronavirus pandemic, which has triggered a global recession and a drastic decline in demand for oil so critical to Russia’s energy-reliant economy. In early 2020, Russia and Saudi Arabia, the world’s biggest crude producers, failed to agree to mutual production cuts in response to the crisis, fueling a price war that further hurt Russia’s economy.7 Economic, public health, and social pressures inside Russia could push the Kremlin to temporarily scale back its ambitions in the short term. However, at the same time, uncertainty and anxiety around the pandemic could create more fertile conditions for Russia’s hybrid activities beyond its borders, especially as Euro-Atlantic governments take extraordinary domestic measures to respond.8 In the long term—even as the pandemic subsides, oil prices rebound, and the global economy begins to recover—conditions will remain difficult for Russia, whose economy has suffered from stagnation and sanctions from the West. These dynamics may lead Putin to be more assertive with hybrid strategies abroad with the aim of appealing to nationalist sentiments at home in order to quell domestic political tensions.

Further emboldening Putin is the lack of traditional US leadership and pushback that has helped to keep Russia in check. US President Donald Trump has instead tried to appeal to Putin, describing his own policy as “getting along with Russia” and reducing perceived or actual consequences of hybrid actions against the United States. Political allegations of the Trump campaign “colluding” with Russia to affect US elections9 have further divided the American public toward Russian aims, creating more fertile ground for the Kremlin’s malign influence.10 Compounding this is fraying transatlantic solidarity, whether the USGermany feud over defense spending or French President Macron’s comments that NATO is “braindead.”11 These divisions not only constrain the West’s response to Russia’s hybrid actions, but also expose cracks in the Alliance that Putin is all too eager to exploit.

Together, these factors indicate that as long as Putin remains in power, the Kremlin will likely continue escalating hybrid activities, short of an all-out war with NATO, to push boundaries and test what is acceptable going forward. In the relative near term, the transatlantic community must plan according to Russia’s current trajectory on hybrid issues, which demands a more proactive and widespread approach.

### Hybrid Impact: Liberal Order—Great Power War

#### Spread of authoritarian nationalism prevents us from stopping global wars and climate catastrophes

Orts, Wharton School professor, ‘18

[Eric Orts, Professor, Wharton School, University of Pennsylvania,”Foreign Affairs: Six Future Scenarios (and a Seventh),”, 6—27—18,

<https://www.linkedin.com/pulse/foreign-affairs-six-future-scenarios-seventh-eric-orts>]

7. Fascist Nationalism. There is another possible future that the Foreign Affairs scenarios do not contemplate, and it’s a dark world in which Trump, Putin, Xi, Erdogan, and others construct regimes that are authoritarian and nationalist. Fascism is possible in the United States and elsewhere if big business can be seduced by promises of riches in return for the institutional keys to democracy. Perhaps Foreign Affairs editors are right to leave this dark world out, for it would be very dark: nationalist wars with risks of escalation into global nuclear conflict, further digital militarization (even Terminator-style scenarios of smart military robots), and unchecked climate disasters.

The global challenges are quite large – and the six pieces do an outstanding job of presenting them. One must remain optimistic and engaged, hopeful that we can overcome the serious dangers of tribalism, nationalism, and new fascism. These "isms” of our time stand in the way of solving some of our biggest global problems, such as the risks of thermonuclear war and global climate catastrophe.

#### The liberal order is under threat, risking war and poverty—U.S. needs to get its act together

Brands, Johns Hopkins professor, ‘22

Hal Brands, Henry A. Kissinger Distinguished Professor of Global Affairs, School of Advanced International Studies, Johns Hopkins University, “American Can’t Retreat from the World,” PERSUASION, 1—26—22, <https://www.persuasion.community/p/america-cant-retreat-from-the-world>, accessed 6-12-22]

The current moment feels so precarious because the key pillars of the old order are under strain. After World War II, the United States sought to ensure its own freedom, prosperity, and security by creating a larger international system in which America and likeminded countries could flourish. That system, commonly known as the liberal international order, required the United States to bear extraordinary burdens. It also delivered extraordinary benefits: averting global wars of the sort that plagued the early 20th century, lifting billions of people out of poverty, and creating an environment in which democratic values could spread more widely than ever before. Yet that system is now being challenged from without and within.

An ambitious, totalitarian China and a vengefully resurgent Russia are expanding their influence at the expense of America and its allies. Authoritarian models of governance are advancing and democracy is eroding. America’s own competence and commitment are in doubt, after the aggrieved unilateralism of the Trump presidency and the debacle of Afghanistan. Meanwhile, a witch’s brew of polarization, tribalism, and surging domestic illiberalism have cast deep uncertainty over the future of American democracy.

These domestic strains are troubling enough in their own right, but they also have pernicious impacts on foreign affairs. After January 6, people in many democratic countries believe that America’s political system is broken. The moral prestige that lubricates American global influence is in shorter supply. American allies wonder about the prospect of a Trump resurrection, and fear that extreme polarization will make U.S. foreign policy erratic for years to come.

It is no surprise, then, that counsels of retrenchment have been proliferating: Surely America will have to deal with its own demons before it can deal with China, Russia, and a host of other rivals. Yet if the United States must indeed get its act together, it doesn’t follow that it needs to beat a geopolitical retreat.

### Hybrid Impact: Misinformation

#### Misinformation is an existential threat—makes it impossible to solve the many challenges facing us

Lin, CISC Senior Research Scholar, ’19

[Herbert Lin, Senior Research Scholar, Center for International Security and Cooperation and Fellow, Hoover Institution, Stanford University, “The Existential Threat from Cyber-Enabled Information Warfare,” BULLETIN OF THE ATOMIC SCIENTISTS v. 75 n. 4, 2019, p. 189-194]

Corruption of the information ecosystem has become an existential threat to civilization as we know it because prosperity and advancement depend on a secure information infrastructure and environment that provides human beings with contextualized, reliable, trustworthy information when and where it is needed. Information is as much a part of human ecology and the essence of being human as DNA (itself a form of information!) is a part of the evolutionary processes in biological systems.

Today, chaos reigns in much of the information ecosystem on which societies depend. In many forums for political and societal discourse, national leaders shout about fake news, by which they mean information they do not like. These same leaders lie shamelessly, calling their lies truth, or perhaps “truthful hyperbole.” Acting across national boundaries, these leaders and their surrogates exacerbate existing divisions, creating rage and diminishing confidence in elections and democratic institutions. Using unsupported anecdotes and sketchy rhetoric, denialists undermine well-established science about climate change and other urgent issues. Established institutions of the government, journalism, and education – institutions that have traditionally provided stability – are under attack precisely because they have provided stability.

The founding of the Bulletin predates by several decades the widespread availability of computers, the Internet, smart phones, search engines, and social media. Few could imagine in 1945 a technological environment that affords today’s high-speed and widespread connectivity, high degrees of anonymity, insensitivity to distance and national borders, easy and customized information searches, democratized access to publishing capabilities, inexpensive production and consumption of information content (including and increasingly importantly emotionally evocative video and audio content), disintermediation of established information sources, and ubiquitous, always-on, always-available access to information sources through mobile devices.

Such advances in information technology have heralded the arrival of the information age, a world in which taking near-immediate advantage of information opens up enormous opportunities in both the private and public sectors for improved delivery of existing products and services and, perhaps more important, the creation of entirely new products and services. Products and services can be customized to individual needs and preferences on a large scale and at more affordable costs. Transactional friction can be tremendously reduced. Through the Internet of Things, actuators and sensors can be connected to process control computers to optimize the behavior and function of physical systems. Everywhere that information can be used to create and improve new and existing functionality (that is, essentially everywhere), one can find or imagine new information technologies to do so.

At the same time, advances in information technology have a dark side. The same increases in the volume and velocity of information have created a louder and more chaotic information environment that stimulates fast, angry, reflexive, intuitive, and visceral thinking, reaction, and action in people and thus displaces more complex, reflective, and rational thought. In a chaotic environment of information overload, people are more likely to use mental shortcuts as a way to reduce the cognitive burden that such an environment places on their thinking.

In recent years, we have seen how the Internet, social media, and mobile devices (and other technologies) can be used by foreign adversaries to interfere in elections and to disrupt the democratic process. We have seen:

● Social media exploitation of cognitive biases to increase their impact and reach – short messages of 280 characters and emotionally evocative video/ audio clips are nearly ubiquitous and much more the norm than they ever were two decades ago.

● Disintermediation of established information sources that reduces the role and influence of those previously responsible for providing factual information and proliferates information sources. The US Supreme Court noted in Associated Press v. US (1945) that “the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public, that a free press is a condition of a free society.” Today, modern information technology has enabled the creation of a larger number of information sources than the 1945 US Supreme Court could possibly have imagined.

● Search engines that return highly visible results for queries based in large part on the popularity of those results and the inferred desires of the user for specific information rather than their actual importance to those queries. Such functionality also makes it easier than ever for people to find information online “by doing their own research,” thus indulging in their confirmation biases by selectively finding and attending only to information that confirms one’s beliefs. Search engine optimization techniques enable gaming of search algorithms to promote the visibility of false, misleading, or worthless information. ● Many-to-many connectivity that enables the formation of echo chambers and media bubbles that reinforce pre-existing beliefs.

● Large-scale data mining that allows adversaries to sift huge amounts of personal data on individuals to identify and target those most susceptible to customized, inflammatory, false, malign, or misleading messages – and also to keep such messages away from public view.

● Near-immediate data transfer, which enables propaganda and other malign information to spread far and wide quickly, while efforts to correct false information are more expensive, often fall short, and frequently fail altogether.

● Inauthentic voices that are largely indistinguishable from authentic ones. Macedonian entrepreneurs discovered ways to monetize an affinity of Trump voters for fake news (Subramanian 2017). Paid human employees of the Internet Research Agency created and spread false information on behalf of the Russian government prior to the 2016 U.S. election (MacFarquhar 2018). And automated “bots”–accounts purportedly associated with human users but in fact managed entirely or mostly by machines – add further chaos to the information environment.

Is this state of information affairs really new? Haven’t adversaries of all stripes always employed propaganda and lies – otherwise known as information warfare (or at least a big part of it) – to advance their interests?

Yes. Information warfare indeed has a long pedigree that reaches into the past for at least the three millennia since the Trojan Horse enabled Greek warriors to breach the walls around the city of Troy. Much more recently, the rise of the Nazi regime in Germany relied on propaganda. As Hitler (1925, 155–56) wrote:

[I]ts purpose must be . . . to attract the attention of the masses and not by any means to dispense individual instructions to those who already have an educated opinion on things or who wish to form such an opinion on grounds of objective study – because that is not the purpose of propaganda, it must appeal to the feelings of the public rather than to their reasoning powers. . . . The art of propaganda consists precisely in being able to awaken the imagination of the public through an appeal to their feelings, in finding the appropriate psychological form that will arrest the attention and appeal to the hearts of the national masses. . . . The receptive powers of the masses are very restricted, and their understanding is feeble.

But more so today than at any earlier point in human history, human beings are vulnerable to information warfare. At the same time that new information technologies have led to an increase in the volume and velocity of information available on Earth by many orders of magnitude in the past few decades, the cognitive architecture of the human mind is more or less unchanged on the time scale of centuries or even millennia.

On human cognition

Research in the fields of cognitive and social psychology has formalized what Hitler knew intuitively. We now understand that human cognitive processing capability is not unlimited; humans have finite cognitive resources that can be “used up” under mentally stressful circumstances. Findings from the same cognitive psychology that has transformed neoclassical economics into behavioral economics (and resulted in three Nobel Prizes in economics) have made clear the “bounded rationality” of human thought and the simultaneous existence in every individual of the capability to engage in two types of cognitive processing.

Specifically, heuristic dual-system cognitive theory posits that human beings have two systems for cognitive processing – an intuitive, reflexive, and emotionally driven mode of thought (often designated as System 1) and a slower, more deliberate, analytical mode of thought (often designated as System 2). Kahneman (2011) provides a primer on System 1 and System 2 thinking. (See Petty and Cacioppo 1986; Chaiken 1987 for other variants of dual-system cognitive theory; see Kruglanski and Thompson 1999 for a contrary view on dual-system cognitive theory.)

System 1 is designed to operate rapidly, but it can do so because it does not take account of all available information and is thus more prone to error (also called bias). System 2 operates more slowly but is more likely to take into account the available information and is less prone to error. People engaging in System 1 information processing respond more emotionally and less rationally or critically than in System 2 processing.

Most important, System 1 thinking is the default mode of thought for human beings – it uses smaller amounts of cognitive resources, relies on simple gutbased judgments, and is used more often when humans are under stress. For most situations encountered in everyday life, System 1 thinking is adequate and produces mostly valid and useful outcomes, but it often fails when a situation requires complex inferences for understanding. For such situations, System 2 thinking, which is effortful and consumptive of cognitive resources, is more often appropriate – and when individuals fail to use System 2 when it is appropriate to do so, they are easily misled.

Most individuals are capable of both System 1 and System 2 thinking; thus, the important operative question is the circumstances under which they select one or the other type of thinking. Psychology has accumulated considerable evidence relevant to this question.

For example, Taber and Lodge (2006) show that an individual tends to be less critical of information that is favorable to his or her position than of information that is not favorable – that is, he or she is more likely to engage in System 1 thinking for favorable information. People have a confirmation bias in their information seeking and processing behavior – they preferentially seek out information that is consistent with their beliefs and they are highly critical of (or ignore) information that contradicts their beliefs. In a meta-analysis of 91 studies, Hart et al. (2009) considered two motivations for how an individual might select information to consume – the desire to gain an accurate understanding of reality and the desire to feel validated in his or her beliefs. These two motivations conflict when an accurate understanding of reality does not validate one’s beliefs, and such a situation motivates the question of which of these motivations is more powerful. Hart et al. concluded that both motivations drive human informationseeking behavior, thus moderating each other to a certain extent, but that on balance, humans do exhibit a tendency towards the validation of their beliefs. People are also subject to belief perseverance (a.k.a. a continuing influence effect) – a cognitive bias through which individuals do not revise beliefs based on erroneous information even when they know for sure that such information is erroneous (Lewandowsky et al. 2012).

Maintenance of an individual’s social identity is an important influence on his or her invocation of System 1 or System 2 thinking. Evidence suggests that individuals tend to adopt the views of the peer groups that are most salient to them, even if the “objective” or “factual” information available to them contradicts those views. (Asch 1951 performed the classic “conformity experiments” that demonstrated this phenomenon in the early 1950s.) Uncritical System 1 thinking is active in processing information that is consonant with the beliefs and attitudes of those peer groups. Critical and skeptical System 2 thinking is active in processing information that is dissonant to those groups’ beliefs. These effects (that individuals tend to accept salient group norms) are even more pronounced in an anonymous environment, such as that which characterizes much online interaction (Postmes et al. 2001).

Lastly, there is evidence that emotion and motivation affect cognition. For example, people who are angry tend to rely more heavily on simple heuristic cues (suggestive of System 1 thinking) than those who are not angry (Bodenhausen, Sheppard, and Kramer 1994). Individuals are more likely to stereotype people (a form of System 1 thinking) when that stereotype is consistent with their desired impression of those people; conversely, when the stereotype is inconsistent with their desired impression, individuals tend to inhibit the use of this stereotype (Kunda and Sinclair 1999). Negative emotions (such as those induced by the receipt of information incongruent with a person’s prior beliefs) can improve the ability of a person to reason logically, thus enabling him or her to negate or discount that information (Goel and Vartanian 2011).

In the new information environment, exploitation of human cognitive architecture and capabilities – which are largely unchanged from what existed millennia ago – provides the 21st century information warrior with cyber-enabled capabilities that Hitler, Stalin, Goebbels, and McCarthy could have only imagined. By exploiting cognitive limitations, the perpetrators of cyber-enabled information warfare have learned to exacerbate prejudices, biases, and ideological differences; to add heat but no light to political discourse; and to spread widely believed “alternative facts” in advancing their political positions.

Russian interference in the 2016 US presidential election has dominated news headlines ever since. But interference by authoritarian countries in the elections of democratic states – as undesirable and threatening as it may be – is hardly the only negative consequence of cyber-enabled information warfare. The problems of nuclear war and climate change are hard enough to solve even when well-intentioned, well-informed parties on all sides share a basic understanding and knowledge of the relevant facts. Yes, they may have different values and different priorities, may act under different constraints, and be able to bring to bear different levels of resources to these problems.

But without shared, fact-based understandings of the blast, thermal, and radiation effects of nuclear explosions, what hope is there for national leaders to reach agreements to reduce the threat of nuclear holocaust [war] or to make good decisions about nuclear weapons use in times of crisis? Without shared, fact-based understandings that rising atmospheric carbon dioxide concentrations caused by human beings result in corresponding increases in global temperature and climatic disruption, what hope is there for national leaders to reach agreements to begin serious efforts at decarbonizing their economies?

Climate change denialism

Climate change denialism can be fairly characterized as cyber-enabled information warfare against the reality of large-scale anthropogenically-induced climate change. In the responses of people resistant to taking action to mitigate climate change, we see a number of psychological factors at work (Zaval and Cornwell 2016). For example, one key element of System 1 thinking is the availability heuristic, with which individuals tend to associate the likelihood of an event with the ease with which they can remember similar events in the past. But the long-term consequences of climate change are unprecedented in recorded human history and obviously people have no personal memories of unprecedented events.

Moreover, climate change is a long-term process whose inexorable progression is easily masked by short-term fluctuations in local weather conditions. For example, public concerns about climate changes correlate with local weather conditions (Krosnick et al. 2006). Climate change deniers are also quick to flag for public attention days that are particularly cold as “evidence” that global warming is not occurring and thus, they claim, discrediting theories of climate change. This illustrates a bias known as attribute substitution, as Kahneman and Frederick (2002) describe, through which individuals substitute salient information (such as the cold temperature today) for information that is more relevant but harder to understand (such as information about global climate change).

People are also subject to a loss-aversion bias, in which they place greater weight on losses than gains of equal value. In 1992, the United States committed itself to the United Nations Framework Convention on Climate Change, although President George HW Bush also stated that “the American way of life is not up for negotiation” – and in 2018, the United States withdrew from the Paris Agreement (which was based on the convention). The argument? That the United States would have to give up too much if it kept to the agreement.

To close this (merely illustrative) exploration of biases relevant to climate change denialism, the optimism bias suggests that people consider themselves exceptions when considering the likelihood of a negative event occurring. That is, bad things may happen to other people, but they won’t happen to me, even though I and those other people are similar in important and relevant ways. In a climate context, the bad things may involve sea level rise or heat waves – and the misperception that “others may suffer from such problems but I won’t” diminishes the power of personal concern as a driver for rational decision making.

Connecting the operation of these cognitive biases to the affordances of modern information technologies is not difficult. For example, Roxburgh et al. (2019) demonstrate how the characteristics of specific weather events (e.g. hurricanes or snowstorms) and “short-term socio-political context can play a critical role in determining the lenses through which climate change is viewed.” Note especially the importance of “short-term socio-political context” – precisely the context that social media shapes.

Elsasser and Dunlap (2013) noted the influential role of a variety of newspaper columnists in advancing denialist arguments and thus amplifying these arguments to a broad segment of the American public. Fewer in number then, essentially all columnists today (of all political leanings) have a social media presence that they use to publicize their work, and in many instances their online presence is driven in significant part by social media and reach many more readers online than in print. Furthermore, subtleties and nuances in their extended written pieces are likely to be lost when they are represented in social media.

Another important element of climate change denialism is the easy accessibility of seemingly-authoritative information that casts doubt on the well-established science of climate change. As reported by The Guardian, a variety of largely secret funding sources distributed $118 million to 102 denialist organizations (Goldenberg 2013). Oreskes and Conway (2011) provide the definitive work on deliberate information campaigns to obscure the scientific truth on a range of issues from smoking to climate change. These denialist organizations have generated a variety of products for public and policy consumption (but – unsurprisingly – not many peer-reviewed scientific articles) that are easily accessible to the public, mainstream media outlets, and policy makers. Their products are broadly disseminated through social media and easily found through customized search, and they are sought by reporters who seeking to cover “both sides” of a controversy that is intellectually equivalent to a “controversy” about whether the earth is round or flat.

Nuclear conflict

On the risks of nuclear conflict, theories and approaches to nuclear deterrence and strategic stability developed prior to the collapse of the Soviet Union in the late 1980’s and early 1990’s rest on the presumption of rationality in national decision makers. In particular, they assume that adversaries are deterred from attacking by a threat of retaliation that would impose costs on the adversary that would outweigh any conceivable benefits that it would gain from an attack (Morgan 2003). Central to this assumption is a rational adversary that can and does make a calculation of expected costs and benefits, compares them, and then acts accordingly.

But the psychologically informed understanding of realworld decision making described above was not accepted widely in the scientific literature until approximately the same time as the collapse of the Soviet Union, and the seminal work in such understanding occurred only in the decade previous to that. What a psychologically-informed understanding of real-world decision making tells us is that the rationality assumption at the base of much traditional thinking on deterrence and strategic stability is untenable, given that humans have evolved to rely on intuitive, reflexive, heuristic System 1 thinking to make decisions, particularly when faced with time pressures, surprise and other obstacles to the deliberate calculation implied by System 2 thinking (Kahneman 2011). Psychology tells us that – more often than not – the fast, intuitive judgements of System 1 often take precedence over the slower, more analytical thinking of System 2.

The challenges posed by reflexive reliance on System 1 thinking are greatly accentuated by characteristics of today’s information environment. Social media networks in particular are optimally designed to stimulate System 1 thinking – emotional, reflexive, immediate – and they rapidly transmit content among like-minded individuals, creating the ideal conditions for public polarization and divisiveness to occur (Pfeffer, Zorbach, and Carley 2014). Multiple narratives rapidly emerge around complex events; citizens splinter into their own informational universes and are unable to agree on an underlying reality. Political leaders themselves are subject to these conflicting narratives and may even be active and influential participants in one or another of them.

It is thus easy to posit that in this information environment, manipulated information – either artificially constructed or adopted by a strong grassroots base – could be used by interested parties to generate pressure on leaders to act. At the same time, leaders themselves are likely to be facing information overload and less able to distinguish analyzed information from their own intelligence sources and other, unvetted information originating from their constituencies.

The coming information dystopia

Nuclear war and climate change are arguably the most important existential challenges today that are compounded by the corruption of the information ecosystem. But even if a single miraculous stroke the laws of physics were changed to make nuclear weapons impossible to build and operate and to immediately eliminate anthropogenic emissions at zero cost, cyber-enabled information warfare could still can lead to an information dystopia. Here are some possible elements:

● Adversaries manufacture numerous graphic videos of American soldiers (complete with sound effects) committing battlefield atrocities, and spread them widely through the Internet. Once upon a time, highquality video forgeries were difficult and expensive to make. AI-based technologies will bring this socalled deepfake capability to the masses, and anyone with imagination, a modicum of technical skill, and a personal computer will be able to distribute reasonably realistic forgeries. Denials will be issued but of course will also not be believed by large fractions of viewers. Even if proof of inauthenticity can be provided, such evidence will not affect the responses of many viewers.

● Political campaigns conduct similar efforts to discredit political opponents (e.g. “showing” an opponent making controversial or disqualifying remarks before an election). But they also use the existence of deepfake technologies to deflect attention from authentic and real evidence of their own political and personal misdeeds. For example, a real video of a candidate punching an old lady who supports his opponent will be dismissed as “one of those deepfakes that anyone could have produced.”

● Financial markets are disrupted by falsified videos of CEOs making announcements regarding company prospects that are much more pessimistic than expected. Attempts to correct the record are drowned out in a subsequent flood of contradictory information, all of which appear at first glance to be authentic.

● Public safety is compromised by reports of local disasters (e.g. explosions of chemical plants that result in the release large amounts of toxic gases). These reports, along with “authentic” video of people choking amidst locally familiar locations (e.g. well-known fields or sport stadiums), cause spontaneous mass evacuations. Contradictory directions for evacuation broadcast using social media result in chaos on the streets and highways.

● Public health is placed at risk when the safety and efficacy of medical treatments known to be safe and effective are publicly questioned through active disinformation campaigns conducted on the Internet and in bookstores. Attempts to provide valid information are met with responses such as “that’s what the pharmaceutical companies and medical establishment want you to think, but just look at what’s happened to our children.”

● Children in schools are threatened by online campaigns to spread rumor, innuendo, and positive or negative information about various students. Conducting such campaigns for pay becomes the business model of entrepreneurs who advertise that they can guarantee admission to selective colleges, boost the social standing of the children of their clients, or take revenge on those who have harmed such children, all in anonymous and untraceable ways.

● Journalists, political leaders, and judges are compromised by artfully forged emails and alterations to other documents that are mixed with entirely authentic leaked emails and documents and are indistinguishable from them.

A world with these elements – and many more comparable ones – will be the inevitable result if and when deployment and use of the tools of cyber-enabled information warfare become widespread. And even more troubling is the fact that not every bit of information needs to be corrupted for this dystopian outcome to occur – it will require only a fraction of it to be corrupted for people to lose faith entirely in “objective” and “trustworthy” sources of information, the result of which will be that people will fractionate into their own information realities.

Fearing the end of the enlightenment

The Enlightenment established reason and reality as the foundational pillars of civilized discourse. In such discourse, logic matters, and a logical contradiction between statement A and statement B means that at least one of those statements is false. The truth of a statement about the world is tested by its correspondence to objective reality rather than by how many people believe it; that is, empirical data are influential. Furthermore, statements known to be wrong or false do not affect conclusions or choices between alternative courses of action.

Cyber-enabled information warfare provides the tactics, tools, and procedures – in short, the means – to replace the pillars of logic, truth, and reality with fantasy, rage, and fear. In a world of ubiquitous cyber-enabled information warfare, communication and information inflame passions rather than informing reason, play to the worst in people’s cognitive architectures rather than the best, and divide rather than unify. Deliberate corruption of the information ecosystem could be seen as an analog of poisoning water supplies that can be done remotely, inexpensively, and anonymously. All of this is just another way of saying that today it is possible to see glimmerings of an anti-Enlightenment that can possibly take root and that would indeed be the end of civilization as we know it.

### Hybrid Impact: Multilateralism / Populism—2AC / 1AC

#### Hybrid tactics spur populism and undermine cohesion

Lawless, University of Denver MA, ‘20

[Scott Lawless, defense consultant, Booz Allen Hamilton and M.A. International Security, University of Denver,“American Grand Strategy for an Emerging World Order,” SECURITY STUDIES QUARTERLY, Summer 2020, p. 130-131]

The liberal order faces political challenges that involve unconventional political warfare to weaken democratic regimes as well as a “clash of social models” between liberal and neo-authoritarian states.16 Political warfare “refers to the employment of military, intelligence, diplomatic, financial, and other means short of conventional war to achieve national objectives.”17 Its current “hybrid” adaptation is unconventional in that it involves tactics such as the weaponization of traditional and social media, sophisticated propaganda, and the widespread use of disinformation campaigns to sway public opinion, discredit liberal politicians, and sow distrust for democratic institutions. Russia, for instance, is actively “exploit[ing] European and transatlantic fissures and support[ing] populist movements to undermine European Union and NATO cohesion.”18 Meanwhile, China is targeting the United States’ companies, government, and allies as part of its ongoing cyber-espionage campaign to steal trade secrets, intellectual property, and advanced technology. What’s more, the political order is experiencing a clash of social models in which states such as Russia and China “believe in the virtues of a strong central government and disdain the weaknesses of the democratic system.”19 Thus, collective political convergence has never been realized because autocratic leaders “concluded that if the liberal order succeeded globally, it would pose an existential threat to their regimes.”20

#### Populism guts EU effectiveness and global multilateralism

Kandel, Sorbonne Associate Researcher and Gondaud ‘19

[Maya Kandel, Associate Researcher, Université Sorbonne Nouvelle Paris 3 and Caroline Gondaud, French policy planner, “Populism, the European Elections, and the Future of E.U. Foreign Policy,” WAR ON THE ROCKS, 6—11—19, <https://warontherocks.com/2019/06/populism-the-european-elections-and-the-future-of-e-u-foreign-policy/>, accessed 5-9-22]

\*\*edited for language

Most European populists don’t want to kill the European Union anymore. This has perhaps been the most concrete consequence of Brexit, which has made exiting the body much less appealing. In the recent European Parliament election, not a single party put exiting the European Union at the top of its priority list. Rather, the major European populist parties, from France to Italy to Hungary, now want to use their power in the new European Parliament to transform the European Union from the inside. The feasibility of such an endeavor is, of course, questionable, given how much the agendas of the various countries’ populist parties differ, especially on migration and fiscal issues.

The key outcome of the election was not necessarily a populist surge but the decline of the center-left and center-right parties, in the context of a huge rise in voter participation (over 50 percent, compared to 43 percent in the previous 2014 election). The center-left party S&D (Group of the Progressive Alliance of Socialists and Democrats) got 150 seats (down from 187), the center-right party European People’s Party (or Christian Democrats) 179 (down from 216). The populist forces (whose political group is still in the process of being created) will hold 73 seats, and 102 if we include the United Kingdom’s Brexit party, which received fewer votes than expected. In this context, the role of “kingmaker” will be probably played by a new centrist coalition aggregating the liberal votes of ALDE (Alliance of Liberals and Democrats for Europe) and those of Macron’s “Renaissance” list (up to 107 seats). But, like the populist forces, this new centrist coalition will be divided on key issues such as budgetary discipline. Defining an operational political platform among this group’s members could be highly problematic.

In a nutshell, the parliament emerging from the elections is more fragmented and less likely to build stable coalitions than before — even if two-thirds of the seats ultimately went to pro-European parties. We can expect lengthy discussions among the factions over the nomination of the European Commission president, who is supposed to be from the party that obtained the largest number of votes. If the EPP and the S&D agreed with this rule, the centrists of ALDE and Macron’s list firmly oppose it. In the longer term and particularly when it comes to foreign policy, some ad hoc coalitions on specific issues, like trade agreements and commercial policy more generally, could be expected. Still, if the rise in voter turnout is good news for European democracy, the volatility of coalitions is less welcome news for European foreign policy and for the European Union’s capacity to act as a global player.

The major risk is probably of stalling E.U. policymaking by blocking the possibility of compromise that is at the heart of any E.U. policy. That would risk further strengthening nationalist governments, and further undermining European citizens’ confidence in European institutions, by proving their major talking point: that the European Union is an inefficient bureaucracy unable to protect them. Thus, the most dangerous outcome of populist influence in the European Parliament is that the European Union will become ~~paralyzed~~ [frozen ]and irrelevant on the international scene, assuming the European populists are not able to develop a coherent project aimed at founding an alternative European Union. If the E.U. decision-making process is ~~paralyzed~~ [frozen ], it will stall the union’s historical role in multilateral forums and further undermine confidence in the European project. The very relevance of the European Union – and of multilateralism as a way of enacting policy change — is at stake.

#### Multilateral cooperation is the only way to solve existential threats—even imperfect solutions are critical

Muggah, Igarape Institute Co-Founder, ‘19

[Robert Muggah, Co-Founder, SecDev Group and Co-Founder, Igarape Institute, “’Good Enough’ Global Cooperation Is Key to Our Survival,” WORLD ECONOMIC FORUM, 7—17—19, <https://www.weforum.org/agenda/2019/07/the-future-is-ominous-global-cooperation-is-key-to-our-survival/>, accessed 3-9-22]

The future feels more threatening and ominous than ever. The sense of doom and gloom is deepening, not least in the West. The daily news headlines do not help. We are told that tensions between the US and North Korea, Iran, Russia or China could flare-up into a global conflagration.

We are informed that the rise of AI will eliminate most jobs and potentially humans. We are witnessing how social media is dividing societies and undermining liberal democracy. And we are reminded almost hourly about how climate change is leading to mass extinction.

Any one of these issues is enough to make us throw in the towel in despair. That would be precisely the wrong thing to do. While these and other threats are real and daunting, none of them are absolutely guaranteed. In fact, the only certainty we have in an era of exponential change is the guarantee that our future is uncertain.

This unremarkable insight is hardly cause for celebration. And it is most definitely not a call for complacency. If anything, it is a reminder that we have the responsibility to do everything we possibly can to build a world that prevents these calamitous events from occurring.

Some modesty is called for. The truth is that we have never been particularly good at predicting the future. To the contrary, some of our smartest thinkers have been extremely good at getting things spectacularly wrong.

For more than a century social scientists have missed the "big events" that changed the course of history. Most of them were stunned by the start of the First and Second World Wars, shocked by the end of the end of the Cold War, and caught unawares with everything from 9/11 to the 2008 financial meltdown, the Arab Spring, Brexit and the election of Donald Trump. It is important to acknowledge our limited capacity for prognostication and adjust our behaviour and expectations accordingly.

Back in 1989, the future looked bright and promising. Liberal democracy and market capitalism had prevailed. The US was the lonely super power. Few analysts anticipated the spectacular rise of China and India much less the explosive market turmoil in 1997 and 2008, the return of reactionary nationalism and the rise of anti-globalism. And yet what is astonishing is how quickly all this tumult has been accepted not just as if it were inevitable, but that it constitutes the "new normal".

So is the future dark and dystopian as growing numbers of westerners – especially Americans and Europeans – are inclined to believe? The answer is it might be, but this is far from a foregone conclusion.

It is worth underlining that people living in the west and the east have never had it so good. While hard to believe, across virtually every metric of human progress we are living the best years of the roughly 200,000 year history of homo sapiens. And despite recent signs of push-back against globalization and democracy, there has never been more global cooperation or a larger number of people living in democratic countries in history.

To survive the next century, even more global cooperation is essential. Going it alone is not an option. The only way to tackle the biggest existential threats is for nation states, along with companies, cities and civil societies, to develop common understandings of their shared challenges and work together to craft pragmatic solutions. The 2030 Sustainable Development Goals are a positive expression of global collaboration, a reminder of our awesome potential for collective action.

We must advance ambitious, innovative and radical ideas. But we should simultaneously reform and renew, rather than abandon, international institutions, from the United Nations and World Trade Organization to the G20 and development banks, including new ones like the Asian Infrastructure Investment Bank. Effective cooperation requires reinforcing, not weakening, regional alliances and arrangements as the world transitions to a multi-polar order.

There is no shortage of daunting existential global dangers that require multilateral responses. These range from radical action to mitigate and adapt to climate change, to regulating AI and the proliferation of weapons of mass destruction.

The priority list is long and growing, including ensuring inclusive growth and reducing gaping inequalities, preventing pandemics and superbugs, regulating genetic and biological engineering, developing rules to manage cyber security, managing migration and refugee flows and ensuring enforceable trade rules for the 21st Century global economy. Yes, the world is more complex and messier than in the past. Get used to it.

The business of building global cooperation has never been easy. It requires a common baseline of facts, the ability to understand the viewpoints of the "other", enlightened leadership and the forging of trust to achieve collective responses that may well be sub-optimal.

It requires the foresight and wisdom to operate not just in the national, but also the regional and international interest. At a time of digitally-enabled fake news, sharpening polarization, and rising populism, this is not straightforward. But when all citizens everywhere are facing potentially civilization-ending threats, multilateralism is not an option – it is a necessity.

More than ever, we must strive to achieve optimum solutions while recognizing that the outcomes will almost certainly be imperfect, and it may sometimes feel like we are muddling through. But like it or not, good enough global cooperation is key to our common survival.

### Hybrid Impact: Multilateralism / Populism—Economy Impact

#### Populism causes economic turmoil and erodes democratic checks and balances

Funke et al., Kiel Institute researcher, 20

[Manuel - Researcher at the Kiel Institute for the World Economy, Moritz Schularick is Professor of Economics at the University of Bonn, Professor and Head of "International Finance and Global Governance" Kiel Institute, 2020, Populist leaders and the economy, ECONtribute Discussion Paper, No. 036, <https://www.econstor.eu/bitstream/10419/226836/1/ECONtribute-036-2020.pdf>]

Our evidence points to significant medium- and long-term economic costs of populism, while we find no decline in income inequality. Fifteen years after the start of a populist episode, the average level of real GDP per capita and consumption is more than 10 percentage points lower compared to a synthetic placebo counterfactual of countries without populists in power. Interestingly, the decline in GDP growth in history (pre-1990) is driven by left-wing populists that emphasize distributional and social issues, while in recent decades it is increasingly driven by right-wing populists whose rhetoric typically focuses on cultural and religious topics. A clear result is that both variants of populism are equally bad for the economy.

Declining economic fortunes under populists are a robust result that we find to hold regardless of region, era, or ideology. It is true in samples that exclude Latin America, in a contemporary and historical sample, and for left- and right-wing populists. This core finding is also robust to cases involving the World Wars or specific outlier cases marked by hyperinflation, civil war, and other extreme events. We can equally rule out that economic disruptions, such as financial crises, in the years before the populist gains power drive the economic decline under populist leaders.

When exploring the channels, three explanations are supported by the data: First, economic nationalism, in particular protectionist trade and investment policies. Import tariffs rise on average ten percentage points compared to the non-populist counterfactual. Populists typically deliver on their promises of fostering economic nationalism and protectionism (Rodrik 2018, Guiso et al. 2018), but with high costs. Second, there is evidence for unsustainable macroeconomic policies, similar to the original discussion by Dornbusch and Edwards (1991). Fiscal policy often does not satisfy an inter-temporal budget constraint as populist governments typically do not react to rising debt ratios by adjusting the primary balance, thereby putting debt dynamics on an unsustainable path (Bohn 1998). Third, democratic checks and balances decline, the independence of the judiciary and press freedoms often fall after populists come to power. Functioning democratic institutions contribute to long-term growth through innovation, economies of scale, education, and capital accumulation (Acemoglu et al. 2005, 2019). Populism erodes these institutional advantages of democracies.

### Hybrid Impact: Multilateralism / Populism—War Impact

#### Unchecked populism threatens global stability

Drezner, Tufts University Interational Politics Professor, ’17

[Daniel, Professor, International Politics, Tufts University, “The Angry Populist as Foreign Policy Leader: Real Change or Just Hot Air,” FLETCHER FORUM OF WORLD AFFAIRS v.41 n. 2, Summer 2017, p. 29-34]

Leaders who rise to power in lower-probability scenarios are also likely to have a greater appetite for risk in foreign affairs. This matters, as Jeff Colgan notes: “risk tolerance leads to aggression in international affairs because it increases the perceived payoff of risky gambles.”17 Populist leaders more closely resemble revolutionaries than more established politicians. And as Colgan warns, “the ambition of revolutionary leaders also contributes to aggression. Ambition makes it more likely that a leader will reject the status quo internationally as well as domestically.”18 We can see this kind of ambition on display among elected populists. Hugo Chávez persistently proposed radical alternatives to the Washington Consensus. One longtime friend of Viktor Orbán noted, “he has always wanted to upset the status quo, to become a change-maker.”19 Orbán himself, in a meeting with Polish Law and Justice Party head Jaroslaw Kaczynski, proposed a “cultural counter-revolution” in Europe.20 Donald Trump’s inaugural address categorically rejected the postwar liberal order, arguing in favor of an “America First” approach to international relations. Populists are therefore more likely to pursue high-risk, revisionist foreign policies.

Populist leaders also care about recognition by others, and will be quick to anger if that recognition is not forthcoming. Populists build their legitimacy on their support from “their” people, but part of that support comes from displays of dominance over others. Russian president Vladimir Putin is well-known for his over-the-top efforts to look strong and powerful. These range from his shirtless photos to videos of him weightlifting to scoring eight goals in an exhibition game with former NHL All-Stars.21 In Erdoğan’s first two years as Turkey’s president, the government has prosecuted more than 1,800 cases of Turkish citizens insulting him—including a former Miss Turkey.22 Donald Trump has insulted anyone who has criticized him since he started running for president, ranging from erstwhile GOP rivals to federal judges to media outlets to a former Miss Universe to Meryl Streep.

When dealing with domestic rivals and critics, such displays of dominance are an easy strategy for elected leaders to pursue. Populist leaders engage in such behavior to project their strength and mastery over the political fates. It is tricky to do this on the international stage, however. Populist leaders will therefore be more concerned than most politicians about the personal respect afforded to them by others. At the international level, this leads to one of two outcomes: recognition by other heads of state, or a denunciation of leaders who fail to confer such recognition. If populists cannot exploit the respect conferred by others, they will be quick to reject and delegitimize the leaders who spurn them.

We can see this kind of pattern at work in how populist leaders have reacted to setbacks on the global stage. Vladimir Putin began his tenure in office with a much warmer attitude towards the West. During the first decade of this century, however, Putin lost an ally during Ukraine’s Orange Revolution, and witnessed NATO expanding to Russia’s borders. It was at this point that Putin began adopting a more hostile attitude towards the West. After President Obama cancelled a meeting with Duterte, the Filipino president responded with a series of tirades insulting the American president.23 In Trump’s first week as president, he faced pushback from the Mexican president Enrique Peña Nieto on his policies for the southern border. In response, Trump tweeted that Peña Nieto should not bother coming to Washington. The Mexican president responded by canceling his visit.

Populists do not possess a monopoly on anger in politics, but most populists tend to project anger as part of their leadership style. Based on their pathway to power and their philosophy of governance, it should not be surprising that they are commonly associated with that emotion. As previously noted, populist parties do particularly well after financial crises. They are adept at exploiting the (often justified) anger that voters possess towards authorities that were in charge when the crisis happened. Former UKIP leader Nigel Farage warned of “political anger” if the United Kingdom did not follow through on Brexit. In a press conference blasting the United States, Duterte said, “If you Americans are angry with me, then I am also angry with you.”24 During one of the GOP primary debates, Donald Trump explicitly stated, “I will gladly accept the mantle of anger.” Trump famously refuses to apologize when he makes controversial or problematic statements.25 Numerous press reports suggest that Trump lost his temper with the Australian prime minister in their first phone conversation.

This wave of populist anger reverses a centuries-long western effort to contain that emotion in international relations.26 Recent scholarship on emotions in world politics suggest that sustained levels of anger carry risks in world politics. Anger was valorized in societies with strong honor cultures and warrior castes, biologically conditioning citizens towards that feeling. Furthermore, as Neta Crawford notes, “threats that evoke anger (if they are associated with perceived insults) tend to decrease the perception of a threat and simultaneously heighten risk-taking behaviors on the part of those who feel angry.”27 This is particularly true if populist leaders find ways to institutionalize anger and resentment through new laws, executive orders, or bureaucratic structures.

This tendency towards angry rhetoric can be exaggerated through misperception and mistranslation. Conventional foreign policy leaders are prepped to stay within the lanes of “accepted” diplomatic discourse, so that observers can detect subtle shifts in phrasing as a foreign policy signal. In contrast, populists scorn diplomatic language as exercises in sophistry and hypocrisy. They rely on language designed to appeal to their base, which increases the likelihood that outside observers misconstrue their words. Angry tirades from leaders like Trump, Duterte, or Iran’s Mahmoud Ahmadinejad have been mistranslated—and usually in a direction that paints the leader as more bellicose than intended.28 Populist leaders will be reluctant to correct such misperceptions, because that would require them to engage in the diplomatic discourse they have derided.

Displays of righteous indignation might play well with a populist leader’s domestic base. The international effect of angry outbursts, however, is to narrow the zone of cooperation between countries. If a leader unleashes an angry tirade against another country, that is sure to gain considerable public attention in both nations. This automatically raises the “audience costs” for both leaders. The larger the audience that is paying attention to any dispute, the greater the political costs a leader can suffer if they back down in that dispute.29 Displays of temper make it harder for the populist to compromise, but it will also make it more politically difficult for the object of the tirade to make any concessions. Through effects on leaders and populations, provocations make negotiations more costly and conflict escalation more likely.30

Perhaps the most important intellectual trait that populist leaders share is their tendency to think like hedgehogs. According to the classical Greek poet Archilochus, “a fox knows many things, but a hedgehog one important thing.” Isaiah Berlin popularized that quote, arguing that intellectuals could be divided into foxes and hedgehogs. This works for decision-makers as well. Foxes will possess the necessary metacognition to adapt to new facts and new circumstances; hedgehogs will rely on their core beliefs, fitting the world into their preexisting worldview.31 Populists are hedgehogs: the one big thing that they know is to reject the elites and technocrats who heretofore governed their country.

As Philip Tetlock observed more than a decade ago, foxes and hedgehogs have different strengths when it comes to thinking about the world.32 Foxes are much better than hedgehogs in their predictive accuracy about world events; simply put, foxes are better at incorporating new information and updating how they think about the world. Hedgehogs are better than foxes at anticipating big and unexpected events happening in the world, such as the collapse of the Soviet Union, the 9/11 terrorist attacks, and the 2008 financial crisis. Anticipating those events requires an assuredness about the way the world works that hedgehogs are more likely to possess.

The effects of these different intellectual styles on foreign policy are straightforward. As hedgehogs, populists are more likely to have their expectations confounded in world politics. At the same time, populist foreign policy leaders will face psychological and domestic political barriers to admitting error or reversing a failing policy. Any public recognition of a misstep demonstrates a leader’s fallibility—which is problematic for leaders who claim that they can divine the general will of the people. At the same time, as hedgehogs, populists will be reluctant to take any action that deviates from the way that they think the world works.

Stepping back, we can proffer some tentative predictions of how populist foreign policy leaders will behave in the coming years. Populist foreign policy leaders are likely to reject the pre-existing liberal international order and espouse a strong form of ethnic nationalism. They might try to create alternative international arrangements to the status quo, but these efforts are likely to be Potemkin efforts, with more pomp and circumstance than substance. Populist leaders will have greater appetites for risk and ambition on the global stage. These heads of state will crave recognition from their fellow world leaders, and be quick to anger if they are spurned in this area. These displays of anger could become institutionalized and will increase the audience costs of all the involved actors, making cooperation less likely. And populists are less likely to correctly perceive how the world works, and more likely to hold firm with policies that are not viewed as working terribly well.

One disturbing conclusion to draw from this particular constellation of traits is that populist leaders are more likely to foment international crises. Breaking with pre-existing global governance structures can guarantee a crisis escalation. An international crisis can trigger rally-round-the flag effects within the domestic population and make it easier for a leader to suppress domestic dissent. At the extreme, one could envision populists threatening or launching diversionary wars to appeal to a nationalist base in times of trouble. Vladimir Putin employed this tactic. In early 2014, he was still reeling from protests over his return to the Russian presidency, and a slowdown in the Russian economy. He responded by annexing the Crimea after the fall of his ally in Ukraine, and bankrolling a secessionist conflict in Eastern Ukraine. These efforts caused his public support to skyrocket even though the Russian economy contracted in 2014 and 2015.

It should be stressed that these are all probabilistic statements. Many of these traits are hardly unique to populists; other heads of state are likely to display some subset of these leadership traits. Still, this combination of attributes suggest that the world is experiencing an increase in the number of revisionist, risky, and violent actions in world politics.

### Hybrid Impact: Russia War

#### NATO-Russia hybrid war escalates—it is an existential threat

Healey, Columbia research scholar, ‘22

[Jason Healy, Senior Research Schol, School for International and Public Affairs, Columbia University, “Preventing Cyber Escalation in Ukraine and After,” WAR ON THE ROCKS, 3—9—22, <https://warontherocks.com/2022/03/preventing-cyber-escalation-in-ukraine-and-after/>, accessed 5-19-22]

There are multiple ways cyber conflict around the Ukrainian invasion might escalate into a direct conflict between Russia and NATO, possibly as a result of either side’s offensives.

First, Russian offensive cyber operations might spark a wider war. President Vladimir Putin has declared sanctions “are akin to a declaration of war” and may see aggressive cyber attacks as the perfect response, particularly since they are reversible and non-lethal. Russia has been entangled with Western economies for decades, especially in the realms of energy and finance. But now, as ties are being severed quickly and viciously, Russia no longer has to fear the backlash if its cyber forces were to disrupt Western banks or liquified natural gas terminals. If you are dealt out of the game, why not just flip the table?

Russia’s cyber generals may be just as enthusiastic as their Army counterparts. They may assure Putin their forces are ready for battle and can quickly and bloodlessly get the West to back down. Putin could be convinced disruptive attacks against the West are no big deal, a low-cost signal that the West should de-escalate or just the next natural move in a non-escalatory intelligence contest. After all, U.S. research found that in response to cyber attacks, “Americans are less likely to support retaliation with force” compared to a more traditional strike.

This can lead to escalation in two ways. The United States — along with countries like the United Kingdom, France, and the Netherlands — might well decide to defend forward against such attacks. Gen. Paul Nakasone, the commander of U.S. Cyber Command, has insisted his forces “must take this fight to the enemy, just as we do in other aspects of conflict.” His then-deputy has also argued that the United States “cannot cede any territory” to adversaries as the “Russians will keep pushing until we push back on them.”

Worse, Dmitri Alperovitch recently warned that if Russia launches cyber attacks after “[h]aving already exhausted the power of economic sanctions, America and its European allies would have few choices other than to respond to these attacks with offensive cyber-strikes of their own.” Such dynamics can feed a spiraling escalation in cyberspace that might take on a life outside of the control of policymakers.

Second, Western offensive cyber operations might spark war. U.S. cyber espionage and operations against Putin, his cronies, or Russia’s military forces will appear far more ominous to Putin if he believes they are aimed at regime change. Could Putin turn the other cheek if the United States were to electronically raid the cryptocurrency wallets of Russia’s sanctions-avoiding kleptocrats? He might feel the need to escalate his own cyber operations as part of his own version of defending forward.

Escalation could happen on the battlefield as well. According to the New York Times, teams from U.S. Cyber Command are “in place to interfere with Russia’s digital attacks and communications.” Other teams are almost certainly collecting digital intelligence on the location and intent of Russian combat forces. The United States is sharing such intelligence with the Ukrainians but apparently not yet providing any real-time targeting. That may change soon, as the United States seeks to alleviate intensifying attacks on civilians. And with his KGB-bred paranoia, Putin might already see the presence of U.S. defensive and intelligence teams operating on or against Russian military networks as evidence of direct U.S. involvement in the war. Confirming his apparent belief that Ukraine is just a NATO puppet, this might force a response, either inside or outside of cyberspace.

Further, if Western governments have infiltrated Russia’s operational military networks, they may feel pressure to disrupt those networks to prevent civilian massacres. Because cyber capabilities are billed as non-lethal, reversible, and non-escalatory, tub-thumping newspapers may push decision-makers to take shots they might not otherwise: “We can’t create a no-fly zone but can use cyber capabilities to prevent civilian harm.” Some well-meaning national leaders may succumb to this pressure, potentially causing a larger conflict.

Future Risks

Even if Russia and the West avoid direct conflict this time, they might not be so lucky the next. As relations worsen, future disruption of critical Western infrastructure by Russian intelligence, such as the NotPetya and Olympic Destroyer attacks, are less likely to be viewed as mere crimes. Repeated crises bordering on war may further erode the tacit agreements and relative restraint of quieter times. After repeated iterations of intensifying cyber operations, both Russia and the West may feel their backs to the wall with few options left other than military force when the next crisis — physical or cyber — emerges. Under extreme conditions, some of the same characteristics that lead cyber capabilities to be a pressure release might have the opposite effect, a mechanism that Bob Jervis and I have described as the Escalation Inversion.

If Putin believes a direct conflict with NATO is likely and expects its adversaries to take measures to reduce vulnerabilities, he could conclude that the best possibility for success is to launch a massive preemptive cyber attack. Since the U.S. military may seem otherwise unbeatable, this may lead Russia to “compensate with audacity in order to redress the balance.” The more the United States brags about its overwhelming offensive cyber advantage, but frets over weak defenses, the more any adversary might feel the need to target the United States as early and as hard as possible.

If Russia fears war with the United States may happen on Saturday, it might feel the need to get in its cyber punches on Friday. If the United States thinks the same, it may need to start on Thursday. Cyber capabilities may be to World War III as mobilization timelines were to World War I.

Since a cyber sucker punch may also seem less escalatory, adversaries could be tempted to take risks they would not otherwise. In this situation, the sense that cyber is a pressure-release valve becomes positively dangerous: If the system is seen to be stable, then there is less reason to act with restraint, thereby making it less stable. Fortunately, the good news is leading U.S. policymakers appear attuned to this risk.

Avoiding Escalation

How can Washington reduce the risk of cyber attacks escalating into a direct conflict with Russia? First, by recognizing it. Cyber conflict may be an intelligence contest or a pressure release in peacetime and something quite different during or after a major war in Europe. Cyber war may be far easier to stumble into when states fear the wolf at their door.

Second, escalation control requires a better understanding of political psychology — specifically the mindset and desperation of one inscrutable, increasingly isolated, and blood-covered tyrant. There were more than enough expert commentators who believed that Putin would never invade Ukraine because it objectively seemed so irrational. Assessments of cyber escalation must also cover seeming irrationality, including the misperceptions, mistakes, and miscalculations that can lead even the most rational leaders to get caught up in an escalatory spiral that is no longer under their control.

Third, preventing escalation requires military and intelligence leaders to understand and respect cyber capabilities. Cyber capabilities are not “magic invisible weapons” but rather real weapons with massive, cascading consequences. They have a range of advantages and restrictions that sober-minded national leaders should approach as they would any other weapon.

Finally, even if we dodge a bullet this time, we should not become complacent. Personally, I would put the chances of cyber conflict escalating into a Russia–NATO war at less than 10 percent. With luck, escalation will not happen, and I will be written off as a “cyber catastrophist.” “Cyber doesn’t work like that,” we will tell ourselves. “Remember the lessons of the Ukrainian cyber non-war. Cyber doesn’t escalate. It isn’t useful on the battlefield or for coercing other states.”

This will hopefully continue to be true for weeks or even years. But the world is in the first few decades of an information age that will continue for a long time. The existential stakes of cyber conflict rise as more countries become more digitized and more reliant on vulnerable information technology.

#### [x] Hybrid warfare escalates—strong incentives for both Russia and NATO states

Kulesa, European Leadership Network Research Director, ‘18

[Lukasz Kulesa, Research Director, European Leadership Network, “Envisioning a Russia-NATO Conflict: Implications for Deterrence Stability,” EURO-ATLANTIC SECURITY REPORT, 2—18, p. 5-8]

“Hybrid” scenarios: trigger for conflict?

One can envisage a number of “hybrid” scenarios of Russia-NATO conflict where operations which started in the cyber, economic, criminal, or “active measure” domains, below the threshold of conflict, trigger a military response or are followed by the physical use of force. As noted in the discussion on the definitions of a conflict, the threshold between crisis and military conflict may not be explicitly stated or otherwise clear to all sides; and it may also be ignored during a crisis. This aspect is especially relevant in the current period of increased interference in the internal affairs of NATO countries attributed to Russia and of the high volume of information ‘warfare’ between Russia and NATO countries.

Russia remains vigilant about foreign interference in its internal affairs and the threat of subversion leading to a severe destabilization of the regime. In the past, Moscow has made accusations about foreign sponsorship of Chechen and radical Islamic terrorists targeting Russia, and has alleged the existence of training camps on the territories of NATO states for activists planning colour revolutions in Ukraine and Belarus. In the extreme circumstances of a crisis, if the Russian leadership became convinced that a non-military campaign against it (which might also involve cyber activities and what Russia calls attempts to instigate colour revolutions) had intensified, this could lead to a military response.

With regards to NATO, some of its members’ views mirror the Russian assessment that we are already in a state of conflict, in which the boundary between peace and war is blurred, and that their defences are being actively attacked through nonmilitary means. They are thus concerned about a scenario in which Russia initiates an attack that moves swiftly from non-military to military means. This scenario should be not dismissed. At the same time, one needs to be wary of interpreting all disturbing developments as part of a grand Russian plan culminating in a provocation or use of force. So there should be prudence before any country presses the “panic button” at the national or NATO / European Union level. There should also be close analysis of early warning indicators related to the gravity, intensity and diversity of incidents and to connections between them. The overall political context and state of the RussiaNATO relationship would also be important: what would be the political and strategic reasons for Russia to move from sub-threshold to abovethreshold activities?

Individual NATO countries would have a decisive role in how some of the “hybrid” scenarios would play out. An Ally can choose to play down or up the importance of certain developments and incidents; it can seek NATO and/or EU support, decide to respond individually (including through actions that are escalatory), or use a mix of both approaches. The Ally’s overall reputation and patterns of international behaviour can matter for determining whether its “frontline” intelligence and assessments are to be trusted. But given the danger of alliance entrapment, NATO also needs to have multiple channels for corroborating the evidence and assessing developments.

Escalation: Can a NATO – Russia conflict be managed?

Once a conflict was under way, the “fog of war” and rising unpredictability would inevitably set in, complicating the implementation of any predetermined theories of escalation, deescalation and inter-conflict management. The actual dynamics of a conflict and the perceptions of the stakes involved are extremely difficult to predict. Simulations and table-top exercises can give only limited insights into the actual decisionmaking processes and interactions.

Still, Russian military theorists and practitioners seem to assume that a conflict with NATO can be managed and controlled in a way that would bring it to a swift end consistent with Russian aims. The Russian theory of victory would seek to exploit weak points in an Alliance war effort. Based on the conviction that democracies are weak and their leaders and populations are risk-averse, Russia may assume that its threats of horizontal or vertical escalation could be particularly effective. It would also try to bring home the notion that it has much higher stakes in the conflict (regime survival) than a majority of the NATO members involved, and thus will be ready to push the boundaries of the conflict further. It would most likely try to test and exploit potential divisions within the Alliance, combining selective diplomacy and activation of its intelligence assets in some NATO states with a degree of selectivity in terms of targets of particular attacks.

Any NATO-Russia conflict would inevitably have a nuclear dimension. The role of nuclear weapons as a tool for escalation control for Russia has been thoroughly debated by experts, but when and how Russia might use (and not merely showcase or activate) nuclear weapons in a conflict remains an open question. Beyond catch phrases such as “escalate to de-escalate” or “escalate to win” there are a wider range of options for Russian nuclear weapon use. For example, a single nuclear warning shot could be lethal or non-lethal. It could be directed against a purely military target or a military-civilian one. Detonation could be configured for an EMP effect. A “false flag” attack is also conceivable. These options might be used to signal escalation and could significantly complicate NATO’s responses.

Neither NATO nor its member states have developed a similar theory of victory. Public NATO documents stipulate the general goals for the Alliance: defend against any armed attack and, as needed, restore the full sovereignty and territorial integrity of member states. It is less clear how far the Alliance would be willing to escalate the conflict to achieve these goals, and what mechanisms and means it would use while trying to maintain some degree of control over the conflict.

The goals and methods of waging a conflict with Russia would probably have to be limited in order to avoid a massive nuclear exchange. Such limitations would also involve restrictions on striking back against targets on Russian territory. But too narrow an approach could put too much restraint on NATO’s operations: the Russian regime’s stability may ultimately need to be threatened in order to force the leadership into terminating the conflict. NATO would thus need to establish what a proportional self-defence response to Russian actions would involve, and to what extent cyber operations or attacks against military targets in quite different parts of Russia would be useful as tools of escalation to signal NATO’s resolve. Moreover, individual NATO Allies, especially those directly affected by Russia’s actions, might pursue their individual strategies of escalation.

With regards to the nuclear dimension in NATO escalation plans, given the stakes involved, this element would most likely be handled by the three nuclear-weapon members of the Alliance, with the US taking the lead. The existence of three independent centres of nuclear decision-making could be exploited to complicate Russian planning and introduce uncertainty into the Russian strategic calculus, but some degree of “P3” dialogue and coordination would be beneficial. This coordination would not necessarily focus on nuclear targeting, but rather on designing coordinated operations to demonstrate resolve in order to keep the conflict below the nuclear threshold, or bring it back under the threshold after first use.

Relying on concepts of escalation control and on lessons from the Cold War confrontation might be misleading. The circumstances in which a Russia -NATO conflict would play out would be radically different from the 20th century screenplay. Moreover, instead of gradual (linear) escalation or salami tactics escalation, it is possible to imagine surprizing “leap frog” escalation, possibly connected with actions in different domains (e.g. a cyberattack against critical infrastructure). Flexibility, good intelligence and inventiveness in responding to such developments would be crucial.

Conflict termination

Russian and NATO assumptions regarding conflict termination would most likely not survive the first hours of an actual conflict. Both sides are capable of underestimating the resolve of the other side to prevail in a conflict and the other side’s willingness to commit the necessary resources and endure the costs, especially once both sides start committing their political capital and resources and the casualties accumulate.

With regards to Russia, Moscow would most likely be approaching the conflict with a clearer concept of its war aims and thus develop better-formed views on conflict termination. It would seek to establish escalation dominance and confront NATO with a binary choice of either accepting defeat or further intensification of fighting. Such intensification might involve a move to the nuclear level, but Russia would also have conventional escalation options, such as conventional deep strikes.

At the same time, it should be highlighted that Russia is unlikely to start a conflict which involves a high degree of uncertainty about its final outcome and carries a risk of military defeat. Russia cannot safely assume that US-led NATO would act with restraint, nor could it be sure that the Alliance would be ready to surrender and terminate a conflict early. For internal reasons Russia cannot afford to lose a “big war”, so the most prudent option would generally be not to initiate such a conflict in the first place. Such logic could, however, get lost in some of the hybrid scenarios and scenarios of an inadvertent outbreak of a conflict.

On the NATO side, conflict termination has not been the focus of close attention, as the Alliance has concentrated in recent years on strengthening deterrence and probing the issue of defence. As one of the workshop participants put it, “NATO is in the deterring Russia business not in the winning a war with Russia business”. This is not a new problem. War termination proved to be a difficult subject for the Alliance in the Cold War, as it involved delicate questions about maintaining NATO’s political cohesion and dealing with the consequences of major nuclear exchanges. Nevertheless, NATO’s ability to persevere in a conflict should not be underestimated. Opinions that NATO would collapse following a Russian first strike seem to be based more on stereotypes about the weakness of Western democracies than on any insight into how Alliances actually operate during wartime, especially when fighting a defensive war that is perceived as just. Still, it may be assumed that NATO would have major difficulty in setting and implementing any conflict termination strategy based on the intensification of military pressure on Russia, especially beyond the immediate theatre of operations. Individual Allies, first and foremost the US, might have to take a lead in that.

### Russia Impact: A2 “Russia Peaceful / Not Revisionist”

#### Russia is revisionist—NATO is not to blame for its behavior

Gotz, Uppsala University scholar & Merlen, University of Kent scholar, ‘18

[Elias Gotz, Institute for Russian and Eurasian Studies, Uppsalla Univeristy and Camille-Renaud Merlen, School of Politics and International Relations, Univeristy of Kent, “Russia and the Question of World Order,” EUROPEAN POLITICS AND SOCIETY v. 20 n. 2, 2019, pp. 133-153, Taylor&Francis]

The ‘defensive Russia’ perspective is not entirely convincing either, for at least three reasons. First, the claim that Russia is a staunch defender of principles like state sovereignty and non-interference in internal affairs is problematic. Granted, Moscow consistently emphasizes these norms in official policy documents and promotes them in diplomatic forums. In practice, however, Russia has violated such principles repeatedly within the post-Soviet space. Examples are Russia’s takeover of Crimea, its meddling in south-eastern Ukraine, and its longstanding support for separatist regions in Georgia (Abkhazia and South Ossetia) and Moldova (Transnistria). As Lo (2015, pp. 71–72) rightly remarks, ‘there is a stark disconnect between its [Russia’s] formal allegiance to the “primacy of international law” and the territorial integrity of nation-states, and a highly selective approach toward implementing such principles.’ Likewise, Bolt and Cross (2018, p. 30) note that, ‘while Russia professes to champion sovereignty and non-intervention as standards for the world order, these guidelines somehow do not apply to Moscow’s own behaviour in its immediate neighbourhood.’ In other words, there is a gap between Moscow’s rhetoric and actions, which does not square with the ‘defensive Russia’ perspective. Second, it appears questionable whether Russia’s assertive foreign policy is a natural and almost automatic response to aggressive encroachments, both normative and geopolitical, from Western powers. For example, it is highly debatable whether Russia’s takeover of Crimea was a pre-emptive move, as some claim, to block NATO from establishing a naval base there (for contrasting views, see Milne, 2014, March 5; Motyl, 2015). Likewise, there was little risk that NATO would offer post-Yanukovych Ukraine a Membership Action Plan. According to then-Russian President Medvedev’s own account, the alliance seemed to have understood the dangers of eastward enlargement and given up on it after the 2008 war in Georgia (Reuters, 2011). The financial crisis of that same year and the ensuing Greek debt crisis further contributed to enlargement fatigue among many EU member states. Consequently, there was little prospect for Ukraine (or any other post-Soviet state, for that matter) to join either of these two organizations in the short to medium term. Moreover, European militaries had downsized since the end of the Cold War, while the US was engaged in its so-called pivot to Asia. If anything, the direct threat posed by NATO to Russia was therefore dwindling. Against this background, it is difficult to interpret Moscow’s takeover of Crimea and activities in eastern Ukraine as a purely defensive response to external pressures. Thirdly, it is unclear why the West – and not Russia – should adjust its status ambitions and policies. As Freire (2011) demonstrates, Russia is a status overachiever relative to the power resources (economic, demographic, and military) that it controls. This means that Russia punches above its weight and occupies an extremely prominent position in world politics – at least in comparison to other countries with a roughly equal amount of material capabilities such as Japan, Brazil, or India. None of these countries is a permanent member of the UN Security Council, for example. This raises the question of how many great-power privileges must Russia be granted before its outsized status ambitions are satisfied. More generally, it is questionable whether the creation of a modern-day concert of great powers, similar to the Concert of Europe in the second half of the nineteenth century, is possible or even desirable. As Rynning (2015, p. 552) observes, not only is concerted power in Europe unlikely, but its pursuit could be dangerous in so far as it could herald the type of unrestrained or flexible balance of power politics that presaged the great wars of the twentieth century. Kagan (2017) likewise asserts that, a return to spheres of influence would not calm international waters. It would merely return the world to the condition it was in at the end of the nineteenth century, with competing great powers clashing over inevitably intersecting and overlapping spheres. In essence, both the policy prescriptions derived from the ‘defensive Russia’ perspective and its explanations of Moscow’s international conduct require some elaboration.

#### Russia’s behavior proves it is revisionist

Grygiel, Catholic University professor, ‘20

[Jakub Grygiel, Associate Professor, Catholic University of America, Fellow, Institute for Human Ecology, “Vladimir Putin’s Encirclement of Europe,” NATIONAL REVIEW, 3—19—20, <https://www.nationalreview.com/magazine/2020/04/06/vladimir-putins-encirclement-of-europe/>, accessed 9-29-21]

Russian propaganda, going back to czarist and Soviet times, often claims that Western powers are encircling Russia, forcing Moscow to be belligerent against its wishes. Russia is the perennial victim of aggressive foreign powers trying to keep Moscow locked in the steppes and, in the worst case, to install themselves in the Kremlin. Undoubtedly, Russia has been invaded repeatedly in the past: Mongol hordes, Napoleon, and Hitler all tried to extend their power over it. But now claims of a potential repetition of such invasions by Russia’s Western neighbors ring hollow. Neither Europe nor the United States has any interest in controlling Russian lands. On the contrary, it is Russia that has managed to extend its reach along a front from the Baltic to the Mediterranean and is projecting power to the Arctic and the Atlantic. Europe is being encircled by Russia — not the other way around.

Russia asserts that it is under siege by the West. Western antagonism, the argument goes, is evident in NATO’s addition of new members, including the latest one, Montenegro, which joined in 2017; in the U.S. and EU support for various “color revolutions” that erupted across a belt of countries from Ukraine to North Africa and the Middle East; and in the U.S.-led wars in the Middle East. In a 2019 speech, General Valery Gerasimov, the chief of the Russian general staff, accused the United States of conducting a “policy of expanding the system of military presence directly at Russia’s borders.” Such a Western policy of encirclement supposedly forces Moscow to lash out to defeat the “Trojan horse” of “color revolutions” and the various military offensives allegedly targeting Russia.

The claim of encirclement serves well to justify Putin’s neo-imperial policies. Russia’s wars in Georgia (in 2008) and in Ukraine (ongoing since 2014), its support for Bashar al-Assad in Syria, and the various forms of political warfare it carries out in Europe and the United States are considered responses to a consistent Western offensive. In brief, Western powers, led by the U.S., are reawakening a sense of deep insecurity in Russia, perennially fearful of another Mongol invasion from the east or of a new Napoleon or Hitler penetrating deep into Muscovite lands from the west. These claims are repeated by those in the West who are opposed to NATO enlargement, to an American engagement in Central Europe or involvement in the wider Middle East, or to any policy that seeks to impose costs on Russian misbehavior. From this point of view, Russia is aggressive because we made ~~her~~ [them] so.

The geopolitical map, however, tells a different story. Not only is the argument that Russia is being encircled deeply flawed and factually incorrect (starting from the misconception of NATO as an offensive alliance), but it also completely misses the main developments of the past few years.

Along Europe’s eastern frontier, from the Baltic to the Black Sea, Russia has a sizeable military presence and has demonstrated its willingness to invade and control territories (e.g., South Ossetia in Georgia; Crimea and eastern Ukraine). It has entrenched itself in Syria in order to buttress Assad, returning to a position of influence in the Middle East that it has not held since the late 1970s. It has developed a partnership of sorts with Erdogan’s Turkey, convincing it to buy S-400 air-defense systems and thereby making that country an ever less reliable U.S. ally. It has built or upgraded seven military bases in the Arctic region, gaining control of one of the key shipping arteries between Europe and Asia, estimated to be 40 percent faster than shipping through the Suez Canal. In a surprising show of force in late 2019, Russia surged ten submarines into the North Atlantic, demonstrating a capability that had been dormant since the late Cold War. And in recent months it has increased its engagement in the messy war in Libya, becoming a key player in direct competition with Turkey in the political dynamics of this Mediterranean area.

The effect of these Russian actions is that Europe is now facing a consistent pressure along a crescent that goes from the Baltic to the Mediterranean, combined with a latent military threat from the North Atlantic and the Arctic. In itself, the existence of an unstable outer zone on the margins of the European Union and NATO is not new. The wars in the Middle East and North Africa and the fragility of the states located between NATO (and the EU) and Russia have multiple long-term causes, and those domestic and regional dynamics are distinct from one another and unfolding with their own tempos and rationales. The war in Libya, for example, has its own causes and developments, which are different from those of, for example, Russia’s invasion of Ukraine or the conflict in Syria.

Over the past few years, however, Russia’s interventions in these regions have imparted a geopolitical cohesion to what previously had been separate zones of instability. Russia is now a central player along the length of this volatile frontier. European security is increasingly at the mercy of Russia, and not just along the tense but geographically limited Central European frontier that historically separated the core of Europe from Moscow’s westward imperial aspirations.

This is an enormous success for Moscow, for which the Obama administration, eager to “reset” relations with Russia and to charm this revanchist power into a progressive community of “responsible nations,” bears much blame. In Ukraine, the Obama administration refused to counter the Russian invasion and did not provide lethal defensive weapons to the Ukrainian army. In Syria, Obama never enforced the “red line” crossed multiple times by Assad, who used chemical weapons against his own population as Washington demonstrated unwillingness to oppose him and his Iranian and Russian supporters. In Libya, the U.S. infamously “led from behind,” a euphemistic catchphrase for the abdication of American leadership. And, more broadly, encouraging the Arab Spring without the determination to manage its outcomes created an image of the U.S. as a reckless agent of upheaval. Russia then could offer its services to the embattled authoritarian regimes, for instance in Syria, to restore order and maintain continuity. The unexpected but now real outcome is the geopolitical encirclement of Europe by Russia.

Russia can now exercise some influence over the flow of migrants from Syria and North Africa (through Libya), exacerbating at will a problem that has bedeviled European political leaders over the past several years. By abetting further violence by the Assad regime, for instance, Russia contributes to pushing thousands of people out of Syria, giving it the power to blackmail Europe in a tactic similarly adopted by Turkey. The approach is brutally simple: Threaten to flood Europe with migrants (through Greece for those coming from Syria, through Italy for those coming from Libya) to obtain some benefit such as money (as Turkey does) or economic and political alignment (as Russia seems to want) in exchange for keeping European borders sealed. Given the demographic pressures from sub-Saharan Africa, the state that has the ability to control the population flow into Europe wields long-term influence over the security and the domestic politics of much of the European continent. Russia has positioned itself to be that power while simultaneously keeping military pressure on Europe’s eastern frontier. In Ukraine, Russia continues to wage war and occupy Crimea. And Russian military exercises regularly train for offensive actions against Moscow’s European neighbors.

To deal with such a geopolitical encirclement, European states are adopting increasingly separate policies. Never short of big ideas, President Macron of France is leading the charge to open the doors to Putin and “normalize relations.” More business-like, Germany is trying to have it both ways, keeping energy deals with Moscow alive while not wanting to follow the openly pro-Russian approach of the French. Italy, the country most immediately affected by Russia’s foray into Libya, from which most of its migrants arrive, is deeply unhappy with the other two European powers, and with France in particular because Paris together with Moscow supports the opposing side in the Libyan war while Italy and Turkey are behind the U.N.-approved government. In the end, however, Italy, more interested in stopping the flow of migrants than in competing for natural resources in Libya, is likely to support a soft approach toward Russia. The Central European EU and NATO members are at best perplexed and at worst deeply worried by their Western allies’ friendly overtures toward Russia. And this is just one aspect, centered on Russia, of the various intra-European rifts.

There are no European solutions to these growing divisions. The European Union is a complex but fragile and inefficient political construction that, in a geopolitical competition with a risk-taking imperial Russia seeking to expand its influence over the European continent, is incapable of achieving strategic coherence among its members. It has no meaningful answer to Russia’s presence in Libya, in Syria, or in the eastern Mediterranean, to Russian occupation of Crimea and eastern Ukraine, or to Moscow’s diplomacy attracting European leaders with promises of peace and stability and economic engagement. There are of course renewed attempts to energize an EU security policy with various initiatives (such as the Permanent Structured Cooperation on defense, the European Defense Fund, and the Coordinated Annual Review on Defense) aimed at increasing intra-EU military cooperation and development. But these efforts often give the impression that the EU is seeking “strategic autonomy” from the United States rather than addressing the security threats around its frontiers.

Moreover, no matter how many new coordinating efforts are launched by the EU or even NATO, the hard truth is that only a few European states are willing to take security seriously, devoting the necessary resources and mustering the national will to compete with Russia. The military capabilities of most European states remain atrophied. The fear that stronger European states would be a threat to Russia, exacerbating an already tense relationship, is misplaced. A militarily powerful Estonia or Poland will not invade Russia, and a sizeable European military contingent in the wider Mediterranean basin has no means of threatening Moscow. More broadly, the purpose of larger European military capabilities would not be to counter Russian forces directly in every location in which they are present, but rather to be able to stabilize North Africa and parts of the Middle East while enhancing deterrence on Europe’s eastern frontier. By doing so, Europe could remove some of the opportunities that Russia used to insert itself into a belt of weak and divided states.

### Russia Solvency: Resilience—General

#### [x] Resilience strategies are vital to addressing emerging hybrid threats—we need to prioritize them

Speranza, Center for European Policy Analysis director, ‘20

[Lauren Speranza, Director, Trans-Atlantic Defense and Security, Center for European Policy Analysis, “A Strategic Concept for Countering Russian and Chinese Hybrid Threats,” Scowcroft Center for Strategy and Security, Atlantic Council, 7—20, p. 3]

Indeed, traditional security concerns, such as nuclear weapons and conventional defense and deterrence, will not go away for the transatlantic community. Yet, going forward, transatlantic nations and institutions will increasingly need to focus on hybrid and nontraditional threats too.2 This is particularly underscored by the 2020 coronavirus crisis, in which both Russia and China have played various roles. Both China and Russia capitalized on the crisis to wage disinformation campaigns against the West. They promulgated conspiracy theories designed to sow fear about America’s handling of the outbreak and to promote the successes of their own authoritarian regimes. Moscow and Beijing also strategically delivered aid and medical supplies to European countries in attempts to build good will and clout on the international stage. These issues cannot be effectively addressed alone or in a vacuum, making global cooperation and collective action–especially among transatlantic allies—paramount. Even as transatlantic nations and institutions shift priorities in the wake of the coronavirus crisis, key counter-hybrid priorities, such as building resilience, strengthening civil response capacities, and investing in civic education, simultaneously serve priorities for pandemic prevention and response. This is all the more reason to prioritize the counter-hybrid agenda.

#### Capacity building and interoperability initiatives are vital to solve

Aronsson and Swaney, research Fellows, INSS, ‘21

[Lisa Aronsson, Research Fellow, INSS and Brett Swaney, Assistant Research Fellow, Institute for National Strategic Studies, National Defense University, “Three Priorities for NATO Partnerships in a Contested World,” NEW ATLANTICIST, 6—14—21, <https://www.atlanticcouncil.org/blogs/new-atlanticist/three-priorities-for-nato-partnerships-in-a-contested-world/>, accessed 4-6-22]

First, NATO should ensure that capacity-building and additional resilience support remain priorities. China is using its economic leverage to expand its security cooperation, and Beijing, along with Russia, is undermining Alliance credibility. Some partners have become testing grounds for hybrid attacks. Capacity-building helps counter that by strengthening partner institutions and resilience, and a sense of shared security. The Partnership Interoperability Initiative protects hard-earned interoperability with some partners, and the Defence and Related Security Capacity Building (DCB) Initiative already supports Georgia, Iraq, Jordan, Moldova, and Tunisia. The NATO Parliamentary Assembly has recommended more attention to Ukraine, the Western Balkans, and areas with weak institutions or where democracy is undermined. Civil emergency planning through NATO’s Euro-Atlantic Disaster Response Coordination Centre is also valuable.

Capacity-building programs are also a path to NATO interoperability for partners, which remains a major driver for cooperation with NATO—even among neutral countries that may never contribute to a NATO military operation. This is because NATO provides internationally recognizable military standards and the ability to plug-and-play into European Union (EU), United Nations, or other multilateral operations. NATO interoperability certification is in demand among partners, as are its robust programs for education, training, and exercises. These activities promote defense and security sector reform, strengthening institutions and transparency. NATO should work to overcome constraints on partner participation in exercises, especially for Japan, South Korea, Australia, and New Zealand. Cooperative security depends on NATO’s centrality as an international standard-setter, a position that cannot be taken for granted.

#### Cooperation is vital to addressing emerging hybrid threats

Smith, Hybrid CoE, ‘21

[Hanna Smith, Hybrid Center of Excellence, “Hybrid Threats to Allied Decision-Making,” NATO DECISION-MAKING IN THE AGE OF BIG DATA AND ARTIFICIAL INTELLIGENCE, ed. S.Lucarelli, A.Marrone & F.N.Moro, 2021, p. 54-55]

\*\*edited for language

Since hybrid threats are designed to interrupt effectiveness of the SEES model at some point, by trying to create cognitive errors such as those arising from group thinking, 2 mirror imaging or applying unconscious confirmation bias, they can challenge organizations like the European Union (EU) and NATO even more than a state. The multilateral setting – with several, connected national interests – can be more vulnerable to hybrid threat activities. The things that can go wrong in the SEES model are especially vulnerable in a multilateral setting, unless there is a comprehensive approach, willingness to exchange information, joint understanding on resilience, and mechanisms to counter and respond in place.

The way Moscow and Beijing think about interference and influence is different from countries with a democratic system. For the EU and NATO, both Russia and China are difficult states to deal with. China is seen in the EU as a global partner, competitor and systemic rival. It has not been on NATO’s radar before the 2019 London Summit, but the Report “NATO 2030” delivered by the Group of Expert appointed by the Alliance’s Secretary General states that “NATO must devote much more time, political resources and action to the security challenges posed by China” (2020: 12). Russia has been viewed by the West as a systemic rival for much longer, but it has also been considered part of the European cultural heritage in the EU. For NATO, Russia has been the greatest military power in the East, which has conflicts of interest with NATO. For the moment, open military conflict is not viewed as very likely neither for Moscow nor for Beijing, although it is not excluded. This leaves the door open to hybrid threats, a mechanism that has roots in authoritarian strategic culture but also has national specificities. The things that can go wrong in the SEES model are challenged by the new information environment being manipulated according to the tactics of hybrid threats. Even if the EU is not a military alliance, while NATO is, both organizations are challenged in similar ways by hybrid threats. Given several factors, including overlapping membership, it is clear that weakening one will also weaken the other. Therefore, in the landscape of hybrid threats, the EU and NATO are considered as a united target by hostile actors – and they can also best counter and respond to these threats if working together.

Against this backdrop, here follow some recommendations aimed to policy-makers and expert communities

in both NATO and EU countries:

 The importance of analysis is growing. Too much effort has been put into collecting data, and not enough into training analysts. Older analysts need to be trained about the new information environment and its functioning. In turn, the younger generation needs to be trained on history, context and connections. Central elements in training are understanding the psychology of the adversary, the assessments of motivations, and rationales.

 The cultural context of information is lost in the volume of information. International cooperation, especially on the part of an alliance like NATO, needs to be lifted to a new level. This does not only concern joint situational awareness about hostile actors, but also involves understanding partners and their perspectives. Without that mutual understanding among allies and partners, divergences can become over politicized and decision-making ~~paralyzed~~, [frozen] which is what the actors behind hybrid threats want.

 There is a need for more effective training in the use of open-source intelligence, focusing on the sources and tools for finding information, including the biases they may have. In addition, more knowledge is needed to be able to detect linkages between actions. Hybrid threat activities start in a settled way, often on a very legal basis, and the potential for such activities to turn into hostile acts needs to be recognized.

 Military communities should reach out more often to non-military expert communities. To counter hybrid threats, a multidisciplinary approach needs to be taken, which really means combining different disciplinary fields and expertise coming from practitioners, academics and the private sector.

 Sharing the vocabulary is important when building situational awareness. Civil-military cooperation is needed here. The civilian side uses different words than the military and sometimes, even if the understanding of a concept would be shared, actors do not understand due to the use of different terms, and discussions can turn into an unnecessary battle of words.

#### Resilience strategies can blunt the effectiveness of hybrid threats

Marovic, Politikon Executive Director, ‘19

[Jovana Marovic, Exeuctive Director, Politikon Network, “Wars of Ideas: Hybrid Warfare, Political Interference, and Disinformation,” NEW PERSPECTIVES ON SHARED SECURITY: NATO’S NEXT 70 YEARS, 11—28—19, https://carnegieeurope.eu/2019/11/28/wars-of-ideas-hybrid-warfare-political-interference-and-disinformation-pub-80419, accessed 4-25-22]

NATO’s success as a collective defense organization lies in its ability to rally twenty-nine member states in defense of any one of them. Cohesion is what makes the alliance strong and unique, but it is difficult to sustain day after day, under constant pressure from adversaries.

One useful way to measure cohesion is in financial terms. Despite a pledge to contribute the equivalent of at least 2 percent of their gross domestic product to defense by 2024, some member states seem likely to miss the target. While this does not prove that the allies disagree on the nature and gravity of the threats before them, it does strongly suggest that some have not fully bought into the agreed priorities.

Many factors are undermining cohesion in NATO. In an era with no single unifying threat, different members inevitably have different interests in diverse centers of power and influence. Allies also diverge on what constitute democratic standards and appropriate responses to competition with non-Western actors.1

It is up to individual countries to safeguard their freedom to respond to a call for help from an ally, address vulnerabilities and gaps in their national systems, and take proactive measures to reduce risks. But the alliance as an organization can help. This is especially true when it comes to understanding and responding to new threats to cohesion. None is more relevant than the hybrid war for hearts and minds that NATO’s adversaries are waging through political interference and disinformation.

ISSUES AT STAKE

While not a new phenomenon, hybrid warfare has been widely mentioned in international discourse since at least 2014. The Russian military intervention in Ukraine and annexation of Crimea showed that NATO and its member states lacked ready-made responses to the emergence of a threat aimed directly at solidarity and cohesion. The experience has prompted allies to rethink, act, and adapt quickly, especially with regard to instruments for protection beyond triggering Article 5 of NATO’s founding treaty, which declares that an attack on one ally is an attack on all.

Hybrid warfare includes a variety of activities and covers the use of different instruments to destabilize a society by influencing its decisionmaking. Frequent instruments include:

Interference in electoral processes: An adversary can use techniques from campaigning through the media and social networks to securing financial resources for a political group to influence the outcome of an election in a direction that favors the adversary’s political interests.

Disinformation and false news: An adversary can create a parallel reality and use falsehoods to fuel social fragmentation. The idea is to disorient the public and make it difficult for a government to seek public approval for a given NATO policy or operation.

Cyber attacks: An adversary can pressure NATO governments into not coming to each other’s aid in times of crisis by threatening devastating cyber attacks aimed at the civilian population. Examples include attacks on networks governing hospitals or electricity and water supplies.2

Drone attacks: These are similar to cyber attacks but on a more limited scale. An adversary can use remotely piloted platforms to inflict misery on civilians by crippling the operations of airports, air ambulances, and police helicopters. Such attacks can also hamper military airspace operations in early phases of a conflict.3

Financial influence: An adversary can make investments, conclude unfavorable energy-supply deals, or offer loans that make a country vulnerable in the long run to political pressure.

Russia is the most frequently cited source of hybrid attacks, particularly disinformation, interference in elections, and cyber attacks.4 It and other states often act via third, nonstate entities such as nationalist, criminal, or terrorist groups. This leaves the attacking state room for deniability, confuses the attacked country, and can prevent a timely and adequate response. Most hybrid operations to date have featured a mixture of mechanisms used by state and nonstate actors, and a clear line between them is difficult to draw.

NATO’s efforts to address hybrid threats have been conducted at two levels: defining strategy at the supranational level and assisting the target countries at the national level. The latter effort will receive a boost when the new counterhybrid support teams on which members agreed in July 2018 fully come into effect. NATO’s Joint Intelligence and Security Division is in charge of hybrid-related research and analysis, while the Public Diplomacy Division tracks disinformation through online instruments. The Emerging Security Challenges Working Group, established in 2012, has a goal to identify and prioritize nontraditional threats.

Because hybrid attacks are a threat to the West as a whole, not just NATO, and because they mostly rely on nonmilitary tools, the alliance has been strengthening its cooperation with the European Union (EU). One useful tool available to both organizations is the joint European Center of Excellence for Countering Hybrid Threats, established in Helsinki in April 2017.

RECOMMENDATIONS

NATO can and should do more to counter hybrid threats, following the proven strategy of prepare, deter, and defend.5

BUILD RESILIENCE BY FOSTERING DEMOCRACY

The first, self-evident recommendation is to deny adversaries the opportunities they exploit for hybrid attacks. The more stable the political systems and economies of NATO countries are, the less suitable ground they represent for hybrid threats. A government that is credible, popular, and trusted will have an easier time winning support for its chosen course of action in NATO than other governments and will be better able to resist disinformation and other forms of interference and blackmail.6

Western Balkan countries seem particularly vulnerable, as their citizens tend to have low trust in the authorities and do not believe that their judiciaries are truly independent. In opinion polls, as many as 70 percent of respondents said that the law did not equally apply to all.7 Democracy and trust have declined in most Western Balkan countries over the last ten years, a trend that overlaps with the crisis of democracy throughout Europe.8

Steps that strengthen democracy and economies are the most effective way of building resilience against hybrid attacks. Corruption deserves particular attention. Not all authoritarian and illiberal governments are corrupt, but most abuse access to public and European funds to give themselves a competitive advantage over political rivals.9 Once on a corrupt path, authoritarians are, in essence, condemned to always seek to remain in power, lest they be prosecuted. It is a vicious circle, and this dynamic between authoritarianism and corruption is not always understood—including by the U.S. and EU leaderships, which does not serve the alliance well.

#### NATO action builds cohesion in members states’ responses to hybrid threats

Marovic, Politikon Executive Director, ‘19

[Jovana Marovic, Exeuctive Director, Politikon Network, “Wars of Ideas: Hybrid Warfare, Political Interference, and Disinformation,” NEW PERSPECTIVES ON SHARED SECURITY: NATO’S NEXT 70 YEARS, 11—28—19, https://carnegieeurope.eu/2019/11/28/wars-of-ideas-hybrid-warfare-political-interference-and-disinformation-pub-80419, accessed 4-25-22]

SHARE BEST PRACTICES

NATO provides a platform from which allies can work when coping with individual problems and vulnerabilities. The alliance can also help identify particular challenges, sometimes before the governments concerned do, and can play a role in early warning. This matters because rapid decisionmaking is sometimes the key to success in hybrid warfare.

THINK AND SPEAK COHERENTLY

NATO is meeting the hybrid challenge with twenty-nine member states experiencing very different sociopolitical realities and often using different concepts. A unified vocabulary and strategy would limit the misunderstanding of threats, improve collaboration, and make the sharing of lessons learned more effective—so would an agreement on the prioritization of tasks and responsibilities and a shared understanding of NATO’s role.

This would greatly help individual countries to build compatible and comparable national strategies. Many of these strategies, including that of the youngest member Montenegro, are in early stages of preparation, but divergences are already becoming evident. Those that have been completed—such as Slovenia’s 2018 regulation on cyber and information security or Croatia’s 2017 National Security Strategy, which partly deals with hybrid challenges—have largely opted for different approaches.

NATO member states must send a unified message inside and out. As strategic communication is a mind-set, it has to be built together carefully and fundamentally.12 NATO’s communication strategy should be a result of joint efforts and hence a common instrument against all threats, not just hybrid ones, at all levels.

### Russia Solvency: Resilience—International Norms

#### The plan is key propagating liberal cyber norms

Pernik & Jermalavičius, International Centre for Defence & Security analysts, ‘16

[Piret Pernik and Tomas Jermalavičius, Research Fellows, International Centre for Defense and Security “Resilience as Part of NATO’s Strategy: Deterrence by Denial and Cyber Defense,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. 106-107]

Due to interdependencies of communication and information systems, and critical infrastructures, resilience can only be developed through an integrated approach.Disruptions of host nation and coalition partner networks and critical infrastructure upon which NATO depends can degrade NATO’s ability to conduct operations. Secondly, projecting cyber defense beyond NATO’sterritory would help to define global cybersecurity norms and behaviors around liberal democratic values. In recognising this indivisibility of security, the NATO-EU Joint Declaration,signed in Warsaw, stresses the need to “foster the resilience of our partners” through individually tailored projects. 13 Indeed, NATO should project its soft side of cyber power in its neighborhood and globally with an aim to expand secure, open and free cyberspace and advocating democratic liberal values in cyberspace.

NATO has a wide range of cooperation formats with more than 40 partners. These partnerships can be leveraged and further expanded according to cyber defense needs of individual partners. 14 For example, in the existing framework of the Partnership for Peace Planning and Review Process, Georgia, Moldova, Iraq, Jordan have included cyber defense aspects into their capacity-building packages. 15 Non-NATO nations also participate in Smart Defense projects such as Multinational Cyber Defense Capability Development (MNCD2), which focuses on sharing technical information, situational awareness and creating a cyber security assessmentteam. 16They have participated at NATO cyber defense and crisis management exercises, and at technical exercises run by the NATO Cooperative Cyber Defense of Excellence.It is possible to include cyber defense issues in their consultations with NATO bodies (28+ meetings) and through staff-to-staff talks. Lastly, NATO educational bodies provide training courses on strategic, operational and technical levels to partners with requisite security clearances.

### Russia Solvency: Resilience—Russian Attack

#### Resilience strategies vital to deterrence a Russian attack

Larsen, CSS Senior Researcher, ‘22

[Henrik Larsen, PhD, Senior Researcher, Center for Sexurity Studies, Swiss Federal Institute of Technology Zurich, “NATO Must Get Resilience Right to Withstand Russia and China,” LAWFARE, 5—22—22, <https://www.lawfareblog.com/nato-must-get-resilience-right-withstand-russia-and-china>, accessed 5-23-22]

Second, NATO needs to identify which aspects of resilience it is positioned to lead. The most pertinent issue seems to be reducing Russian temptations to destabilize its eastern territory, notably Estonia and Latvia with significant Russian-speaking minorities, and the Lithuanian-Polish border toward the Kaliningrad exclave. Russia-instigated gray zone conflict on NATO territory seems more likely than a large-scale conventional war, especially given the poor performance of Russian forces in Ukraine. Russia still prefers to rely on disinformation and subversion to stir ethnic and political discord and may also return to using special operations incursions as a destabilization strategy, as it did during its seizure of Crimea in 2014. NATO needs to deter Russia across multiple domains of warfare by structuring and training a part of its future forces for gray zone eventualities that may precede Russia’s application of large-scale kinetic force. Integrating preparations to combat gray zone tactics into NATO’s conventional planning would allow it to implement a stronger, more crisis-ready resilience concept. NATO’s cyber defense capabilities are obviously relevant against Russian attempts to disrupt allied or national functions that may precede a conventional attack. And NATO should also work to deny hostile powers the capacity to neutralize or jam NATO and reconnaissance satellites.

#### Resilience key to checking Russian hybrid threat

Pernik & Jermalavičius, International Centre for Defence & Security analysts, ‘16

[Piret Pernik and Tomas Jermalavičius, Research Fellows, International Centre for Defense and Security “Resilience as Part of NATO’s Strategy: Deterrence by Denial and Cyber Defense,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. 101-102]

As noted by Jamie Shea,NATO’s and EU’sroles in buttressing resilience of most vulnerable and exposed countries often overlap, 8 particularly in such areas as cyber security, strategic communication, civil preparedness and countering Russia’s hybrid warfare. Although Russia’s hybrid warfare techniques have been extensively analysed,it is difficult to anticipate when, where and what types of stressors will be created and exploited by Moscow—or any other adversaries—in order to coerce target countries. Russia’s approach typically combines both applying a long-term pressure (e.g., hostile propaganda and economic warfare) and opportunistically administering short-term sudden shocks, making it impossible to identify only a single set of capacities needed to cope with its hybrid strategy. A broad-based resilience of potential targets—allies and partners alike— which addresses a wide range of vulnerabilities to both chronic and acute stressors is of vital importance if NATO, in cooperation with the EU, seeks to deny Moscow the achievement of its political and strategic objectives in relation to the Alliance and its partners.

Equally important is a proper appreciation by the Alliance that Russia will constantly aim to undermine NATO’s legitimacy and credibility, so that individual nations feel helpless and having no choice but to acquiesce to Moscow’s geopolitical demands. The efforts of the Alliance—through its strategic communication, public diplomacy and outreach—to ensure high levels of trust in and support to its core tasks, policies and strategies among the general public of the allies and partners, as well as constant reassurance that “no one will be left behind” in the face of adversity, are fundamental to countering this. It is as much about the upstream effort of NATO to remain legitimate, relevant, visible, cohesive and credible as about downstream buttressing of the most exposed or vulnerable nations (so-called “forward resilience”).

# Resilience: China Advantage [Embargoed]

### Advantage X: China

#### A—Chinese hybrid efforts threaten NATO while locking in Chinese tech leadership

Varner, Inter-University Seminar of the Armed Forces Fellow, ‘20

[Joe Varner, Fellow of the Inter-University Seminar on Armed Forces and Society and the Conference of Defence Associations Institute, “The Dynamic Russia-China Duo: Russia and China Are Actively Working to Subvert NATO Security in an Era of Political War,” DIPLOMAT & INTERNATIONAL CANADA, 4—3—20, <https://diplomatonline.com/mag/2020/04/the-dynamic-russia-china-duo-russia-and-china-are-actively-working-to-subvert-nato-security-in-an-era-of-political-war/>, accessed 5-29-22]

China’s strategic objectives in Europe are geared to maintaining Chinese economic, political and military power and keeping the Chinese Communist Party in power at home. The goal is not just access to markets, but to split European Union members from one another to prevent unified positions against China and to break NATO and EU cohesion. It is important to note that China’s intention is to replace the post-Second World War (1939-1945) Liberal rules-based order and security architecture with its own Beijing-centric order. China has been hostile to NATO since its embassy was accidentally bombed by NATO forces during the Kosovo War (1998-1999). The Chinese Communist Party’s goal is to separate the United States from NATO and NATO states from one another. There is one major difference between the Russian and Chinese approach to subverting NATO. China still wants access to the EU’s economies, whereas Russia’s view is dominated by an environment of total great-power conflict.

Chinese attempts to subvert Europe include divide-and-rule tactics with Southern and Central European countries. China has negotiated bilateral deals with several EU countries, including the 17+1 group of Albania, Bosnia and Herzegovina, Bulgaria, Croatia, the Czech Republic, Estonia, Greece, Hungary, Latvia, Lithuania, Macedonia, Montenegro, Poland, Romania, Serbia, Slovakia and Slovenia. Eleven of these countries are EU member states and four others are candidates. Taking a page from Russia’s attempt to undermine NATO’s southern flank, in 2017, China stated it was ready to discuss Turkey’s membership in the Shanghai Cooperation Organization (SCO), whose members are China, Russia, India, Pakistan, Kazakhstan, Kyrgyzstan, Tajikstan and Uzebekistan.

As well, Greece and Italy have fallen into the big money-big debt trap of China’s Belt and Road Initiative. Chinese Shipping giant, COSCO, has taken the controlling share of the Greek port of Piraeus and it is said that China wants to build a high-speed rail link between Belgrade and Budapest and then onward to the western part of the continent. The Port of Piraeus is the main sea port of Athens, the largest port in Greece and one of the largest in Europe. In the past decade, Chinese companies have acquired controlling shares in 13 ports in Europe, including in Greece, Spain and Belgium. Together, these facilities handle about 10 per cent of Europe’s shipping-container capacity. In fact, China has gained access to Europe’s three largest ports: respectively Euromax in Rotterdam, of which it owns 35 per cent; Antwerp in Belgium, of which it holds a 20-per-cent stake; and Hamburg, Germany, where it is to build a new terminal. China’s People’s Liberation Army (Navy) warships have already paid a friendly port visit to Piraeus in Greece. Gary Roughead, a former U.S. chief of naval operations, warned that “Chinese port operators will be able to monitor U.S. ship movements closely, be aware of maintenance activities, have access to equipment moving to and from repair sites and interact freely with our crews over protracted periods.”

China is leveraging tensions in the Western alliance over U.S. economic policies, including U.S. sanctions on European countries and Washington’s trade war with China, climate change, multilateralism and the Iran nuclear deal. Beijing also builds networks among European politicians, businesses, media, think-tanks and universities to create layers of active support for Chinese policies and interests as well as a means to shut down and silence commentary from critics and dissidents. China has targeted specific European countries’ vulnerabilities to increase its economic presence, including Greece’s economic crisis and disenchantment among the countries that represent the poor cousins of the EU, those discontented with European Union conditions for investment, such as Serbia, and the United Kingdom post-Brexit. All the while, China is using its investment and new presence to acquire foreign technology through legal and illegal means, with the objective of dominating the innovation industries of the future. The U.S. Department of Defense has warned that China has sought to acquire, legally and illegally, Western technology in order to modernize its economy and build weapons to rival the strength of Western militaries by striking further, harder and faster. Chinese espionage and cyber espionage to gain access to foreign military and industrial secrets is well known. The Chinese government continues its partnership with Russia in Europe, where the two countries have similar strategic objectives and can work together to weaken and degrade U.S. and NATO interests.

#### B—Chinese tech leadership guts the liberal order, risking global wars

Jain, Scowcroft Center analyst & Kroenig, Georgetown professor ’19

[Ash Jain, Senior Fellow, Scowcroft Center for Strategy and Security and Matthew Kroenig, Detuty Director, Strategy, Scowcroft Center for Strategy and Security and Associtae Professor, Government and Foreign Service, Georgetown University, PRESENT AT THE RE-CREATION: A GLOBAL STRATEGY FOR REVITALIZING, ADAPTING, AND DEFENDING A RULES-BASED INTERNATIONAL SYSTEM, Atlantic Council, 2019, p. 50-51]

Develop New Rules for Disruptive Technologies

The system must also be adapted to deal with new issues that were not envisioned when the existing order was designed. Foremost among these issues is emerging and disruptive technology, including AI, additive manufacturing (or 3D printing), quantum computing, genetic engineering, robotics, directed energy, the Internet of things (IOT), 5G, space, cyber, and many others.

Like other disruptive technologies before them, these innovations promise great benefits, but also carry serious downside risks. For example, AI is already resulting in massive efficiencies and cost savings in the private sector. Routine tasks and other more complicated jobs, such as radiology, are already being automated. In the future, autonomous weapons systems may go to war against each other as human soldiers remain out of harm’s way.

Yet, AI is also transforming economies and societies, and generating new security challenges. Automation will lead to widespread unemployment. The final realization of driverless cars, for example, will put out of work millions of taxi, Uber, and long-haul truck drivers. Populist movements in the West have been driven by those disaffected by globalization and technology, and mass unemployment caused by automation will further grow those ranks and provide new fuel to grievance politics. Moreover, some fear that autonomous weapons systems will become “killer robots” that select and engage targets without human input, and could eventually turn on their creators, resulting in human extinction.

The other technologies on this list similarly balance great potential upside with great downside risk. 3D printing, for example, can be used to “make anything anywhere,” reducing costs for a wide range of manufactured goods and encouraging a return of local manufacturing industries.61 At the same time, advanced 3D printers can also be used by revisionist and rogue states to print component parts for advanced weapons systems or even WMD programs, spurring arms races and weapons proliferation.62 Genetic engineering can wipe out entire classes of disease through improved medicine, or wipe out entire classes of people through genetically engineered superbugs. Directed-energy missile defenses may defend against incoming missile attacks, while also undermining global strategic stability.

Perhaps the greatest risk to global strategic stability from new technology, however, comes from the risk that revisionist autocracies may win the new tech arms race. Throughout history, states that have dominated the commanding heights of technological progress have also dominated international relations. The United States has been the world’s innovation leader from Edison’s light bulb to nuclear weapons and the Internet. Accordingly, stability has been maintained in Europe and Asia for decades because the United States and its democratic allies possessed a favorable economic and military balance of power in those key regions. Many believe, however, that China may now have the lead in the new technologies of the twenty-first century, including AI, quantum, 5G, hypersonic missiles, and others. If China succeeds in mastering the technologies of the future before the democratic core, then this could lead to a drastic and rapid shift in the balance of power, upsetting global strategic stability, and the call for a democratic-led, rules-based system outlined in these pages.63

The United States and its democratic allies need to work with other major powers to develop a framework for harnessing emerging technology in a way that maximizes its upside potential, while mitigating against its downside risks, and also contributing to the maintenance of global stability. The existing international order contains a wide range of agreements for harnessing the technologies of the twentieth century, but they need to be updated for the twenty-first century. The world needs an entire new set of arms-control, nonproliferation, export-control, and other agreements to exploit new technology while mitigating downside risk. These agreements should seek to maintain global strategic stability among the major powers, and prevent the proliferation of dangerous weapons systems to hostile and revisionist states.

#### C—Cyber cooperation pivots NATO to address the threat posed by China and enables coordination with the EU

Odgaard, Norwegian Institute for Defense Studies Professor, ‘22

[Liselotte Odgaard, Professor, Norwegian Institute for Defense Studies and Non-Resident Senior Fellow, Hudson Institute, “NATO’s China Role: Defending Cyber and Outer Space,” WASHINGTON QUARTERLY v. 45 n., 1, Spring 2022, p. 175-179]

NATO in Cyber and Outer Space

Cyber and space is a promising arena for NATO to address China challenges by building member state resilience. Like the air and sea domains, as areas that belong to no one state and which provide access to much of the globe, they form part of the global commons. Command of the commons has been the key enabler of the US global position of power for many decades.26 However, China wields a sufficient range of sea, air, cyber, and space capabilities such that the global commons is now a contested zone. In contrast to the sea and air domains, cyber and space are sparsely regulated. This lack of international norms enhances the risk of conflict based on misperception, making NATO cooperation pertinent. Adversarial activities toward the US and Europe in the cyber and space domain threaten transatlantic security. These come not just from China, but also from other adversaries such as Russia and Iran. Mechanisms for addressing these challenges in the military sector are essentially generic and not, at least in their basic design, established with a particular country in mind. Thus, cyber and space provide an avenue for NATO to contribute significantly to deterrence of China without having to combat major internal resistance. NATO would also benefit from long-standing US-EU cooperation on cyber and space issues.27

NATO has vowed to clarify Article Five’s collective defense commitment to encompass threats to satellites in space and coordinated cyberattacks. NATO can design this effort to include adversarial behavior from China. The alliance already has an array of instruments to deal with cyber and space challenges from adversaries. These can be extended to encompass China without pronouncing it a threat.28 This approach allows the US and Europe time to adjust their cooperation to take into account the fact that China poses military threats to them both without explicitly using the language of threat at a time when NATO members do not agree if China should be defined as a challenge that can trigger Article Five responses.

Since the late 1990s, the vulnerability of shared space assets to cyberattacks has been a concern for both the US and Europe. For example, in 1998 a USGerman satellite, used for peering into deep space, was rendered useless after it turned suddenly toward the sun, damaging its High Resolution Imager by exposure. NASA later determined that the accident was linked to a cyber-intrusion at the Goddard Space Flight Center. Coordinated cyberattacks have emerged as a major threat to both the US and Europe since the late 1990s. For example, for about eighteen minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed US and other foreign internet traffic to travel through Chinese servers. Other servers around the world quickly adopted these paths, routing all traffic, including government and military traffic, to about 15 percent of the internet’s destinations through servers located in China.29

In the future, the need to enhance situational awareness in space is likely to lead to further integration of space assets between the US and its allies. Civilian entry points are likely to provide a growing opportunity for infiltration. The weak state of cybersecurity in civilian agencies should also be considered. Chinese military doctrine prioritizes weaponry that targets vulnerabilities in the deployment of US and allied power, such as the use of cyberattacks to disrupt surveillance assets, intelligence networks, and command-and-control systems.30 These threats are significant, since next generation systems, including fighter aircraft, destroyers, and special forces, will not function without access to space communication and space-derived data.

Although European and US allies have indigenous space programs outside the NATO framework, cyber security and outer space would be a useful field for joint explorations of how to divert and manage attacks and identify an agency which can coordinate transatlantic responses to attacks. Allies are embedded in a range of information networks which may be disrupted, giving rise to alliance management concerns emerging from attacks. The lack of red lines regarding behavior in cyber and outer space between the US and its allies on one hand, and adversaries such as China on the other, adds to the risk of misperception and escalation, and hence also highlights the need for allied coordination to avoid starting a war by mistake. An improved NATO dialogue on safeguards and alliance consultation could also assist communication with China on arms control and conflict prevention in cyber and outer space, which is not currently taking place.

Looking to the future, NATO’s success in establishing transatlantic mechanisms for cyber and outer space safeguards and consultation will be crucial to allow NATO a key role in taking on the China challenge in ways that help restore faith in NATO’s credibility as a provider of collective defense in all domains. It will also assist NATO in straddling the chasm between member states prioritizing threats from either China, Russia, the Middle East, or North Africa, since cyber and space threats potentially stem from all of them, and the effectiveness of cyber and space defense mechanisms do not necessarily depend on geographical origin.

Improved communication between NATO and the EU will be essential for NATO to successfully address the military aspects of cyber and space threats. The framework for permanent EU-NATO relations, Berlin Plus, was concluded in March 2003. It allows for the exchange of classified information, the EU’s use of NATO assets and capabilities for EU-led crisis management operations, and the establishment of consultation arrangements.31 Due to disagreements over responsibilities and jurisdiction, however, meaningful coordination did not take place until July 2016. On this occasion, NATO and the EU issued a joint declaration stating their intention to work together on security and defense responses to unprecedented challenges emanating from the South and East of the Euro-Atlantic area.32 During Biden’s visit to Brussels in June 2021, NATO promised to strengthen cooperation with the EU on promoting peace and stability including protecting critical infrastructure, strengthening resilience, maintaining a technological edge, and addressing challenges to a rules-based order.33 The EU-US summit statement from the same visit merely reaffirms support for robust NATO-EU cooperation and promises to strengthen the partnership.34 At the level of policy implementation, it is clear when talking to NATO and EU officials that usually they do not coordinate their strategies and tactics for countering China challenges.35

The EU-US summit statement’s negligible mention of cooperation with NATO indicates that the ball is in NATO’s court if strengthening NATO-EU coordination is to take place. French and German concerns about entrapment are a major barrier to meaningful NATO-EU cooperation. The area of cyber and space security may allow NATO to work around this roadblock. In line with the EU’s practice of supporting the efforts of groups of member states to take the lead on issues where EU institutions cannot trump sovereignty, in the area of cybersecurity the EU has decentralized implementation to work around national resistance. This has allowed the EU to respond collectively and effectively to cyberattacks in Europe, primarily through bolstering capacities and law enforcement cooperation.36 However, the EU is not yet a globally influential and effective cyber-power because differences among member states over issues such as whether to prioritize tech sovereignty or Europe’s global tech competitiveness prevent the EU from acting in unison on the global stage.

The first US-EU TTC meeting held in September 2021 was an important step in strengthening the EU’s global position in cooperation with the United States, and hence called into question whether NATO has a role to play in cyber security.37 The next couple of years will demonstrate whether the EU and the US are able to focus on becoming mutually supportive global cyber security guardians by cooperating on strengthening investment screening, export controls, and rebalance global supply chains in semiconductors. The successful implementation on both sides of the Atlantic of the recommendations of the TTC working groups will determine if transatlantic cooperation positions the US and the EU as global partners in guarding cyber space. In part, this will depend on the EU’s ability to forge common positions that meet the US halfway on issues such as tech sovereignty and data privacy, points of contention through which transatlantic relations have been marred by conflict.

The potential convergence of transatlantic views on cybersecurity leaves room for NATO to play a significant role because the EU is a civilian and economic, rather than military, set of institutions. The NATO summit in Brussels in 2018 carved out a role for NATO which the EU cannot fulfill, allowing NATO members to integrate their sovereign cyber capabilities into NATO operations and missions.38 However, compared to the EU’s major role in cyber, NATO’s role is negligible. As EU civil-military cooperation ramps up in enhancing Europe’s autonomous defense profile while allowing US companies a role in this effort, the union looks set to become an even more dominant actor in transatlantic cyber defense. Because NATO is a military organization, it has the procedures and instruments to position itself in a key role in coordinating and implementing the military aspects of cyber defense between the US and Europe. The multinational cybersecurity effort which is confronting the global threat posed by Chinese state-sponsored cyberattacks involves NATO, the EU, Australia, New Zealand, and Japan, and sets NATO off to a good start in enhancing its profile in countering Chinese challenges to transatlantic cybersecurity.39 However, it remains to be seen if it manages to deliver mechanisms that succeed in integrating allied responses in the military sector in a way that complements US and EU cyber defense initiatives.

In outer space, the EU is also increasingly active, recognizing the need to deepen investments in areas such as satellite navigation, earth observation, space situational awareness, and secure communications, which are all central to enhanced space security. The EU has established the EU Agency for the Space Programme, which has oversight over everything the EU does in orbit as a bloc. Moreover, the EU uses the European Space Agency (ESA) as technical advisor and industrial procurement agent. This setup allows the EU to become more agile, dynamic, and innovative in space as rapid industrialization is taking place with US entrepreneurs and well-funded Chinese space programs in leading roles.40 In the pipeline are a next generation of Europe’s satellite-navigation system, Galileo, and an extension of the scope and capabilities of its Copernicus-Sentinel spacecraft, which monitors the state of the planet. The EU focuses on ensuring that Europe has independent space capabilities, but it does not develop instruments such as space weapons systems.41

In the outer space realm, NATO has tremendous potential for playing a key role in developing instruments in the military sector that involve European and US space capabilities. NATO’s decision to declare outer space an operational domain at the London summit in 2019 is a first step in allowing NATO an active role in addressing growing anti-satellite threats from China and Russia.42 With the US as the leading power in outer space and with the EU developing its space platforms to enhance situational awareness and security, NATO has the tools to work out a common transatlantic definition of the anti-satellite challenges that need to be addressed. The establishment of mechanisms that ensure coordination across military NATO commands regarding intelligence gathering and the interface between cyber and space defense, as well as civilian and military occurrences and initiatives, would potentially strengthen the ability of allies to counter anti-satellite threats considerably. As with cyber, NATO must first integrate the space issue into all its organizational and operational structures, and secondly, develop mechanisms that focus on coordination between US and European capacities on the basis of a common understanding of the challenges to be addressed.

#### D—NATO is critical—action thwarts Chinese efforts to undermine the liberal order, shores up weak links in the alliance

Odgaard, Norwegian Institute for Defense Studies Professor, ‘22

[Liselotte Odgaard, Professor, Norwegian Institute for Defense Studies and Non-Resident Senior Fellow, Hudson Institute, “NATO’s China Role: Defending Cyber and Outer Space,” WASHINGTON QUARTERLY v. 45 n., 1, Spring 2022, p. 169-170]

Washington increasingly looks to the EU rather than NATO for guidance on Europe’s future security policy. One reason is that NATO’s toolbox is lagging in domains such as cyber and outer space, although cyber and outer space operations are key enablers of actions in all domains including air, sea, and land. One indication of this is the US-EU negotiations surrounding a common response to cyber threats which took place during the first US-EU Trade and Technology Council (TTC) meeting in Pittsburgh in September 2021. In addition, during Trump’s presidency, longstanding US dissatisfaction with Europe’s modest defense spending threatened to put NATO on the backburner in transatlantic security debates.5 Since then, Russia’s invasion of Ukraine has elicited a sea change in German defense policy with the announcement in February 2022 that defense spending will increase to more than 2 percent of its gross domestic output annually.6 While this may be a convincing signal that Europe will finally devote the resources required for its own defense and revive NATO’s central role in transatlantic security, there is also a risk that China will be moved to the periphery of the alliance’s agenda.

On February 11, 2022, during the runup to the Russian-Ukrainian war, the Biden administration published its Indo-Pacific strategy as US Secretary of State Anthony Blinken was in the midst of a Pacific trip to Australia, Fiji, and Hawaii.7 This US prioritization signaled that despite Moscow’s war in Europe, Washington remains committed to strengthening its presence in the Indo-Pacific and competing with China. If the US drops the ball on the Indo-Pacific, Washington is concerned that China might use force against Taiwan.8 Consequently, the key question for the US is how many resources can be tied up in Europe without losing sight of the long-term goal: deterrence of China. As US strategic competition with China increases while NATO is sitting on the fence, failure to develop a transatlantic defense policy that addresses China will leave Europe vulnerable to China’s ability to exploit the weak links in European defense arrangements, which are newly fragmented by the Russian invasion of Ukraine.

EU efforts to build an independent regional defense profile and nurture cooperation between Europe’s defense industry and national defense communities reflect a growing recognition that the region needs to become a self-reliant defense actor. However, Europe still needs to demonstrate that self-reliance does not imply merely focusing on Europe’s periphery. Otherwise, the industrial challenges from China may outcompete Europe’s defense industry. Shipbuilding is a case in point. By 2021, China built 50 percent of all existing ships in the world. Through design collaboration agreements, cyber espionage, and acquisitions, China has copied advanced innovative ship designs. Enormous financial resources from the state allow Chinese companies to enjoy economies of scale by building dual-use factories which not only outcompete Western companies in the commercial shipbuilding industry, but also threaten the production of navy vessels. If not taken seriously, Europe and the US may soon have no choice but to buy frigates from China.10 This example demonstrates the centrality of China for global economic and security developments and should encourage Europe to manifest a position of unified strength in defending NATO member states against Chinese security challenges. This realization will help convince the US and its adversaries that Europe continues to be a credible partner in countering common threats against transatlantic security, whether they appear in or beyond the European region.

China’s challenges to US and European security constitute such common threats across a broad range of sectors. These include gradual reinterpretations of principles of international law, the subversion of universal liberal market economic practices, and cyber insurgencies targeting a wide range of civilian and military entities. These Chinese policies all have major military implications because they are related to developments in the operating principles, capabilities, and priorities of China’s armed forces. Only NATO can offer an integrated transatlantic response to the military aspects of Chinese policies that threaten those sectors across the globe, including European actors. NATO’s involvement is essential if the credibility of the alliance’s security guarantees is to be preserved and an effective response to China’s encroachments on a liberal rules-based order is to be established.

The omnipresent character of the China threat demonstrates that it is long overdue for NATO to position itself as a significant player in addressing Beijing’s challenges to transatlantic security. NATO is key to keeping US and European security policies coordinated when applying mechanisms of deterrence and defense against Chinese challenges. If transatlantic unity of purpose is lost, both the US and Europe are far less likely to succeed in addressing China sufficiently.

### China Status Quo: NATO Focus Low Now

#### NATO is not focused on the threat posed by China now—it should be

Odgaard, Norwegian Institute for Defense Studies Professor, ‘22

[Liselotte Odgaard, Professor, Norwegian Institute for Defense Studies and Non-Resident Senior Fellow, Hudson Institute, “NATO’s China Role: Defending Cyber and Outer Space,” WASHINGTON QUARTERLY v. 45 n., 1, Spring 2022, p. 168]

Compared to the United States, Europe took a long time to acknowledge its stake in managing security challenges from China. As Beijing pushed beyond its traditional zones of interest in East and Southeast Asia toward the Indian Ocean in the 2000s, US security policies began to focus more on China as Washington sought a new geopolitical equilibrium in Asia.2 Since 2014, France and the UK have spearheaded Europe’s naval diplomacy to counter the displays of force and increasing tensions in maritime Asia to which China contributes. This engagement has focused on regular exercises with the US and its Asian allies, operations in support of freedom of navigation, and base-sharing agreements.3 In 2021, the EU recognized that these geopolitical dynamics directly impact its security and announced the establishment of supportive mechanisms in its Indo-Pacific strategy.4 However, NATO has been conspicuously absent in these transatlantic endeavors designed to counter challenges to US and European security. Reflecting NATO’s absence from the main arena of US-China strategic competition, the alliance is hardly ever mentioned in off-the-record conversations on Indo-Pacific security between diplomats and think tank personnel.

NATO’s reluctance to take on the China challenge is perhaps not surprising, given its inherent assumption that the European continent is the jewel in the crown of the US alliance system, which is thought to guarantee US assistance in the event of a military threat against Europe. This assumption was challenged during the Trump administration, which openly questioned the US commitment to Article Five’s collective defense obligation. The invasion of Ukraine has given NATO a new lease on life and put it at the frontlines of transatlantic cooperation on deterring Russia from further military action in future. However, NATO’s focus on its eastern frontline carries the risk that the alliance turns into a Russia-focused European institution and ignores that China is a global great power competitor which also constitutes a major challenge to the security of all NATO member states.

### China IL: Tech Dominance

#### China uses cyber/hybrid activity to steal key technologies

Kramer, Atlantic Council fellow, ‘19

[Franklin. D. Kramer, Distinguished Fellow and Board Member, Atlantic Council, “Managed Competition: Meeting China’s Challenge in a Multi-Vector World,” Scowcroft Center for Strategy and Security, Atlantic Council, 12—19, p. 19-20]

C. Security: Hybrid and Conventional Military

China advances its security interests through a combination of hybrid efforts and conventional military capabilities and activities.100

1. Hybrid: Hybrid conflict is not a self-defining term. In the discussion below, hybrid is used to encompass cyber operations, including espionage, economic coercion, and lowlevel use of force. Certain other activities, which could be included under the hybrid rubric, have been previously discussed under the category of influence.101 The key point is that all of these activities are overseen by the CPC and the Chinese government, and, while not necessarily entirely coordinated, are part of a generally common approach.

Cyber: China’s use of cyber as an element of hybrid strategy is well-established. The 2019 Worldwide Threat Assessment by the Director of National Intelligence provided:

“China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems. China remains the most active strategic competitor responsible for cyber espionage against the US Government (USG), corporations, and allies. It is improving its cyber attack capabilities….”102

As noted in the Department of Defense’s (DoD’s) “Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2019”: “China has mobilized vast resources in support of…espionage activities to acquire sensitive, dual-use, or military-grade equipment.”103 Media reports have indicated that DoD contractors and subcontractors have been significantly affected by cyber attacks, and a public report for the secretary of the navy states that the “system has demonstrably failed.”104 Additionally, among many other instances, China engaged in the well-known cyber attack against the Office of Personnel Management (OPM), which resulted in the personal information of 22 million people being compromised,105 as well as attacks against managed service providers and is under indictment for stealing proprietary technology from US-based Micron Technology used to make dynamic random access memory (RAM) chips.106 Numerous groups of Chinese hackers have been identified as “advanced persistent threats” engaging in both commercial and national security espionage.

### China Impact: Liberal Order—2AC

#### An uncontained China threatens the liberal order—it is an existential threat

Bishara, former American University of Paris professor, ‘21

[Marwan Bishara, Senior Political Analyst, Al Jazeera, and former Professor, International Relations, American University of Paris, “China’s Rise and America’s Decline Spell Conflict,” AL JAZEERA, 11—18—21, <https://www.aljazeera.com/opinions/2021/11/18/the-chinese-miracle-and-the-american-debacle>, accessed 6-12-22]

But the similarities are becoming uncanny as a rising China begins to pose a strategic challenge to the global system similar to that of the Soviet Union; as Biden frames the conflict between the US and China in ideological terms (a clash between democracy and autocracy); and as both sides show a willingness to resort to all means necessary to achieve their goals short of a large military confrontation, or a destructive “hot war”.

China has certainly pulled ahead of Russia, which is trying to revive its old glory and influence by any means necessary. President Vladimir Putin may play dirty games with the West, but Xi is adamant about rewriting the rules of the game altogether.

China’s strongman rejects the “international rules-based order” the West dictates and insists on co-authoring the principles of a new world order.

In other words, the US may downplay Moscow’s provocations as the desperate manoeuvres of a “regional power”, but when it comes to Beijing, it has no choice but to pay attention to this bullish and bullying superpower.

China has succeeded where it counts, where the Soviet Union had failed – the economy. China’s economy has expanded at an incredible rate and, all things being equal, is destined to surpass that of the US in this decade.

China is also developing a strategic doctrine and posture worthy of its economic supremacy, and which includes conventional, naval, digital, space and nuclear military power.

There are many ways to quantify the Chinese miracle, no less in comparison with the US. But it suffices for our purpose here to take an overall look at the century since the US emerged as a world power and the Chinese Communist Party was first established, in 1921.

In its first half, China suffered from turmoil, disintegration, foreign occupation and horrific famine that killed tens of millions, while the US became a world superpower, comprising 40 to 50 percent of the world economy.

China began to get its act together during the past 50 years, which coincided with the US’s recognition of the communist government and the late President Richard Nixon’s historical visit in 1972, the first by a US president. But it was not until 10 years later that China began to widely liberalise and industrialise its economy at a breathtaking pace.

Joining the World Trade Organization (WTO), in 2001, has propelled China to global prominence as the “world’s factory”. In the following 20 years, the Chinese economy skyrocketed from the equivalent of 13 percent of the US economy to 73 percent this year; a five-fold increase. In the process, it pulled hundreds of millions of Chinese out of poverty.

Furthermore, Xi’s 2013 multi-trillion-dollar Belt and Road Initiative (BRI), spanning more than 60 countries, has ensured China’s strategic enlargement and geopolitical expansion like never before. Interestingly, renewable energy investments reached a new high of 57 percent of BRI’s total for energy projects in 2020.

The US may have hoped that China’s membership would mean cheap imported goods and the moderation and democratisation of the Chinese government, but eventually, China’s ascension led to a $300bn annual trade deficit and the communist party tightened its grip on power, alas.

As the China miracle unfolded, US power has continued to unravel over the past 20 years, beginning with the debacles of its wars in Afghanistan, Iraq and the greater Middle East and through the 2008 financial crisis and the disastrous Trump presidency, as Washington lost lots of assets, credibility, and influence among friends and foes alike around the world.

In the process, the US’s share of the world economy shrank by almost half to 22 percent.

That is why Biden, who urged Xi not to let their competition veer into conflict, must tread carefully after the summit ends to ensure the US has the necessary geopolitical clout to deter a bellicose China from making any aggressive moves in Asia and beyond.

Likewise, it is incumbent on the Chinese leader, who is feeling super-confident nowadays, to refrain from resorting to unsavoury means or unnecessary threats that could escalate into a large confrontation with dangerous consequences.

The world’s wellbeing, indeed its survival, depends on it.

### China Impact: Liberal Order—Internal

#### Chinese hybrid tactics disrupt the global order—cyber strategies and IP theft are a cornerstone of these efforts

Speranza, Center for European Policy Analysis director, ‘20

[Lauren Speranza, Director, Trans-Atlantic Defense and Security, Center for European Policy Analysis, “A Strategic Concept for Countering Russian and Chinese Hybrid Threats,” Scowcroft Center for Strategy and Security, Atlantic Council, 7—20, p. 5-9]

Similar to Russia, China seeks a world that is less dominated by the US-led international system and gives China more influence over global affairs. However, given its history, governance model, geopolitical position, and relations with the transatlantic community, China has a different worldview and strategic endgame. All Chinese policies are underpinned by the need to keep the Chinese Communist Party (CCP) in power. Beyond that, several long-standing Chinese narratives impact China’s foreign policy. One such narrative relates to the “hundred years of humiliation” China experienced as its once-central global role was diminished by a series of Western incursions in the 1800s.12 The CCP has leveraged this mentality, combined with the filial piety between the Chinese state and its people, to keep China stable and unified against external territorial, economic, political, and cultural threats.13 With another core principle of “history as destiny,” China believes it will regain its stature as a powerful, respected actor in the world and a benevolent overseer of its broader region.14 Described by Chinese President Xi Jinping as the “Chinese Dream,” this notion underpins many of the government’s maneuvers to expand its international influence and reach. At the same time, China has traditionally preserved a culture of peaceful coexistence, indicating it does not seek aggressive expansion or view foreign interference in the same way as other powers. Yet Chinese officials have manipulated this narrative to support China “defending against threats” to its perceived regional and global role, which the Chinese government defines at its discretion.15 Other factors, such as the unique role and leadership style of President Xi Jinping and China’s growing material capabilities, have also created new dynamics suggesting China has shifted toward a much more assertive role, as evidenced by its hostile actions in the South China Sea, for example.16

In light of this, many experts argue that China seeks to displace, or at least gradually adapt, the current international system in order to return to its desired role.17 Yet, such adaptation must be understood with nuance. Indeed, China has benefitted from many of the current order’s features, such as Western capitalism, the Euro-Atlantic trade order, and the US guarantee of free and secure trade routes. Rather than disrupting or entirely displacing those aspects, China wants to manipulate them to fuel its own rise as a great power. Much of China’s strategy to do so involves working with willing nations bilaterally where opportunities for investment and influence exist. This is a necessary in Europe, where shared interests are ample, but where a mismatch of values and political models limits the ceiling for cooperation. Many European democracies desperate for investment from Beijing are only willing to cooperate to a certain extent with communist China. The EU has described it as follows.

“There is a growing appreciation in Europe that the balance of challenges and opportunities presented by China has shifted…China is, simultaneously, in different policy areas, a cooperation partner with whom the EU has closely aligned objectives, a negotiating partner with whom the EU needs to find a balance of interests, an economic competitor in the pursuit of technological leadership, and a systemic rival promoting alternative models of governance.”18

This realization and, subsequently, more restrictive policies toward China are increasingly being adopted by EuroAtlantic countries and institutions. Because China prefers to work through mechanisms in which it has more control, this has driven it to create its own frameworks for engagement in Europe and Eurasia, supported by its growing economic and military might. As a result, China’s moves to gain new political and economic partners have begun to undermine EU, NATO, and transatlantic efforts.19 This has led to the rise of China’s own kind of hybrid activities.

China’s hybrid toolkit in Europe largely focuses on political and economic coercion to advance its objectives. Chinese tools include: leveraging unequal trade relationships with foreign countries to secure favorable terms for China; making large foreign direct investments in strategic sectors, prioritizing investments that give China access to European political elites; and launching massive critical infrastructure projects at cheap rates in foreign countries that connect China to European markets. These projects overtly favor Chinese workers and industry and give China control over operating the infrastructure, posing significant security and geopolitical risks for the receiving country. China has also become known for its use of “debt-trap diplomacy,” which typically involves giving large loans to vulnerable countries to support these big projects, anticipating their inability to fulfill payment obligations. When the country defaults on debt, China subsequently assumes control of the projects, providing significant leverage beyond its borders. Much of this is facilitated through China’s self-promoting political frameworks and initiatives such as 17+1 and the Belt and Road Initiative (BRI).20 By focusing on pragmatic cooperation on shared challenges and interests, such as economic development, China uses these tools to build relationships and further integrate itself with transatlantic countries, despite differences on broader political issues. The Chinese government then uses those relationships to detract from the criticism against its delinquency in other international obligations (e.g., human rights, law of the sea), and to manipulate political decision-making inside institutions such as the EU.

China has also conducted a range of operational and cyber hybrid activities, which have increased as political and trade tensions have escalated between the United States and China. This has included the cyber-enabled theft of US and European intellectual property for China’s commercial and technological advantage. Using coordinated hacking and espionage efforts, China has sponsored numerous operations against defense contractors and producers of civilian and military technologies, such as aerospace, semiconductors, and information technology, which China views as critical to future innovation. China reinforces these efforts by using unfair practices related to industrial policy, such as forced technology transfer, which mandates that US and European companies share their technology to gain access to Chinese markets. Many academics have also been subject to Chinese attempts at appropriating their work or intellectual property.

When it comes to information operations, China has used its Confucius Institutes across Europe and the United States to propagate Chinese language, culture, and influence.21 Beyond this, China uses targeted messengers— whether diplomats in embassies around the world or Chinese students studying abroad in Europe or the United States—to promote misleading Chinese narratives in local, national, and social media. China also uses these organizations and people as vehicles to invest in media companies and partnerships, in hopes that they will favor and share Chinese content, which often oversimplifies complex issues, glorifies China, and misrepresents the truth.

Going forward, China’s hybrid activities will be shaped by a number of factors. First among these will be the aftermath of the coronavirus pandemic. The Chinese government’s management of the outbreak has sparked sharp international criticism ranging from lack of transparency to deliberate manipulation of the crisis for its own geopolitical gain.22 Some argue that China’s actions and geopolitical repositioning around the coronavirus, including its suppression of key outbreak data and propaganda initiatives to boost its authoritarian regime as a model to respond to the crisis, are a prime example of its hybrid activities at work.23 Coupled with massive economic losses, this could limit China’s political and economic ability to expand its influence in Europe and abroad in the short term. In the longer term, however, China’s growth is expected to rebound, fueling renewed political and economic forays into the global arena. Moreover, some experts argue that the shocks from the pandemic crisis will hit democracies and the US-led global system harder than communist China, allowing it to emerge as a more influential world power than before.24

Another major factor that could affect China’s course is the transatlantic community’s response to its hybrid actions. Thus far, China’s hybrid activities have been particularly challenging to counter because some of the actions are currently legitimate or legal, even if undesirable for transatlantic nations. Additionally, as highlighted by the EU’s strategic outlook referenced above, many of these nations, including the United States, rely on China as a critical trading partner, which makes some level of pragmatic cooperation essential. For European nations, especially those struggling financially and in dire need of investments and modernization, few alternatives can compete with China’s infrastructure and loan offers. All of this has constrained a collective response. Nevertheless, as evidenced by new strategic documents released by NATO, the EU, and nations, concerns over China’s hybrid activities are growing, alongside the political will to take action.25 In addition to recent worries about the coronavirus, another major concern involves Chinese-led infrastructure projects in Europe—from 5G telecommunications networks and undersea cables to electric grids, power plants, and nuclear projects—that utilize technology built by Chinese state-run or subsidized companies. There is a growing belief among transatlantic policymakers that the Chinese government could mandate backdoor access to this infrastructure, which it could in turn manipulate for espionage or other political purposes. As unity around this issue grows, China could be forced to change some of its behavior, but only if the transatlantic community can respond effectively.

At the same time, China will seek to utilize its influence in countries like Italy and Hungary to undermine European consensus on these issues. To stay ahead of the curve, the transatlantic community needs a more proactive and comprehensive counter-hybrid approach for China.

Since Russian and Chinese hybrid activities are directly linked to their worldviews and grand strategies, limiting them, let alone causing fundamental behavioral change, is difficult. Because Russian and Chinese hybrid activities come with different motivations, tactics, and effects, developing an overarching counter-hybrid strategy is all the more challenging. Complicating this further is the potential for pragmatic hybrid cooperation between Russia and China against the transatlantic community. Moscow and Beijing have already sought to harmonize their economic and military clout in pursuit of shared interests—for example by using arms sales and joint military exercises to expand their influence in Africa. Something similar could happen in Europe. This difficult threat environment makes a proactive and unified transatlantic approach to hybrid threats increasingly important.

### China Impact: NATO

#### We need to check Chinese influence in Europe to safeguard cohesion and competitiveness

Nietsche et al., CNAS Research Associate, ‘20

[Carisa Nietsche, Research Associate, CNAS Transatlantic Security Program, Jim Townsend, former Deputy Assistant Secretary fo Defense and Adjunct Senior Fellow, CNAS and Andrea Kendall-Taylor, Senior Fellow, CNAS, “Enlisting NATO to Address the China Challenge,” Center for a New American Security, 10—5—20, <https://www.cnas.org/publications/commentary/enlisting-nato-to-address-the-china-challenge>, accessed 4-22-22]

\*\*edited for language

The challenge China poses to NATO has clear implications for U.S. national security. In a worst-case scenario, China could ~~hobble~~ [limit] NATO mobility in a time of crisis. Meanwhile, China could use its increased presence in Europe to undermine NATO cohesion, gather information for Russia, corrupt information and network security, fracture interoperability, and erode U.S. and European competitiveness. To address these challenges, the U.S. Department of Defense should recognize the clear threat that China poses to NATO and work through NATO to address these vulnerabilities. The next National Defense Strategy should pursue a plan of action that enables Europe to bolster its own defense, starting with a few critical European capitals, and that broadens beyond transatlantic allies. Ultimately, the plan should aim to preserve and protect NATO’s military edge vis-à-vis China.

### China Impact: Tech Dominance—Threat Growing

#### China has almost caught up—threatens U.S. leadership

Allison et al., Harvard Government Professor, ‘21

[Graham Allison, Douglas Dillon Professor of Government, Harvard Kennedy School, Kevin Klyman, Research Assistant, Belfer Cetner for Science and International Affairs, Harvard, Karina Barbesino and Hugo Yen, former Research Assistants, Belfer Center for Science and International Affairs, “The Great Tech Rivalry: China vs the U.S.,” Avoiding Great Power War Project, Belfer Center for Science and International Affairs, Harvard Kennedy School, 12—21, p. 40-41]

In sum, although the U.S. has led the past half-century of technological innovation and still retains dominance in several other technological fields, China has emerged as a serious peer competitor in the foundational technologies of the 21st century whose applications promise to be transformative in arenas from intelligence and military power to economic growth and governance.

As the 2020 Report of the American Academy of Arts & Sciences “The Perils of Complacency” concludes: “Given the enormous scale and rate of progress of Asia, particularly China, the United States will find that reversing its own downward slide will be very difficult…If we ignore this issue, declines in the economic well-being of our citizenry and our ability to influence world affairs will be inevitable.”169

#### China is catching up in technology—will surpass the U.S. unless we act

Allison et al., Harvard Government Professor, ‘21

[Graham Allison, Douglas Dillon Professor of Government, Harvard Kennedy School, Kevin Klyman, Research Assistant, Belfer Cetner for Science and International Affairs, Harvard, Karina Barbesino and Hugo Yen, former Research Assistants, Belfer Center for Science and International Affairs, “The Great Tech Rivalry: China vs the U.S.,” Avoiding Great Power War Project, Belfer Center for Science and International Affairs, Harvard Kennedy School, 12—21, p. 2-4]

Today, China’s rapid rise to challenge U.S. dominance of technology’s commanding heights has captured America’s attention. The rivalry in technology is what the Director of the Central Intelligence Agency, Bill Burns, spotlights as the “main arena for competition and rivalry with China.”5 It has displaced the U.S. as the world’s top high-tech manufacturer, producing 250 million computers, 25 million automobiles, and 1.5 billion smartphones in 2020.6 Beyond becoming a manufacturing powerhouse, China has become a serious competitor in the foundational technologies of the 21st century: artificial intelligence (AI), 5G, quantum information science (QIS), semiconductors, biotechnology, and green energy.7 In some races, it has already become No. 1. In others, on current trajectories, it will overtake the U.S. within the next decade.

President Xi Jinping has declared, “Technological innovation has become the main battleground of the global playing field, and competition for tech dominance will grow unprecedentedly fierce.”8 Emphasizing the need to “develop indigenous capabilities, decrease dependence on foreign technology, and advance emerging technologies,” the Chinese government’s most recent Five-Year Plan identifies key performance indicators, sets deadlines for outcomes, and holds provincial and local governments accountable for delivering results.9

One of America’s most respected leaders in advancing and applying technology, Eric Schmidt, who led Google to become one of the world’s leading technology companies, has been candid about his views. Noting that “many Americans still have an outdated vision of China,” he believes “the United States now faces an economic and military competitor in China that is aggressively trying to close our lead in emerging technologies.”10 In his assessment: “Unless these trends change, in the 2030s we will be competing with a country that has a bigger economy, more research and development investments, better research, wider deployment of new technologies, and stronger computing infrastructure.”11

To take stock of the state of the technology race, this report examines the progress made by the U.S. and China in each key technology over the past 20 years.

To begin with our bottom lines up front:

• In the advanced technology likely to have the greatest impact on economics and security in the decade ahead—AI—China is now a “full-spectrum peer competitor” in the words of Eric Schmidt.

• In 5G, according to the Pentagon’s Defense Innovation Board, “China is on a track to repeat in 5G what happened with the United States in 4G.”12 Despite advantages in 5G standards and chip design, America’s 5G infrastructure rollout is years behind China’s, giving China a first-mover advantage in developing the 5G era’s platforms.

• In quantum information science, America has long been viewed as the leader, but China’s national push presents a clear challenge. China has already surpassed the U.S. in quantum communication and has rapidly narrowed America’s lead in quantum computing.

• America retains its position of dominance in the semiconductor industry, which it has held for almost half a century. But China’s decades-long campaign to become a semiconductor powerhouse has made it a serious competitor that may soon catch up in two key arenas: semiconductor fabrication and chip design.

• The U.S. has seven of the ten most-valuable life sciences companies, but China is competing fiercely across the full biotech R&D spectrum. Chinese researchers have narrowed America’s lead in the CRISPR gene editing technique and surpassed it in CAR T-cell therapy.

• Though America has been the primary inventor of new green energy technologies over the past two decades, today China is the world’s leading manufacturer, user, and exporter of those technologies, cementing a monopoly over the green energy supply chain of the future. Consequently, America’s green push relies on deepening its dependence on China.

• China’s whole-of-society approach is challenging America’s traditional advantages in the macro-drivers of the technological competition, including its technology talent pipeline, R&D ecosystem, and national policies. As the National Security Council’s Senior Director for Technology and National Security Tarun Chhabra and the Center for Security and Emerging Technologies have recognized, “The United States is no longer the global science and technology (S&T) hegemon.”

### China Impact: Tech Dominance—Innovation Key

#### Relative innovation is critical to staying ahead of China

Erbas, Beyond the Horizon researcher, ’21

[Yunus Erbas, Resarch Assistant, Beyond the Horizon ISSG, “China-U.S. Tech War: New Hegemony,” Beyond the Horizon, 6—25—21, <https://behorizon.org/china-u-s-tech-war-new-hegemony/>, accessed 6-3-22]

On 14 May 2021, China became the second country to have successfully landed a rover on Mars after its Zhurong spacecraft touched down on the surface of the red planet. Zhurong (祝融), carrying the name of the “god of fire” in ancient Chinese mythology, was the sixth rover to land on Mars, the first five managed by the American NASA Jet Propulsion Laboratory. Although registering as a great success for China, Zhurong received lesser global attention when compared to its American competitor, Perseverance. Yet, it heralds once again that China constantly gains more ground against competing with the U.S. even in cutting-edge technology alongside other sectors.

China is undisputedly becoming a technological superpower and is currently undergoing the fastest expansion in world history despite the recent pandemic crisis. One of the reasons behind the phenomenon is that innovation is at the top of the country’s priority list.

In the year 2017, Chinese President Xi Jinping set out clearly his vision at the 19th CPC National Congress for China to achieve global leadership in science and innovation by 2050. The government has been leading the way for years, and the country’s high-tech sectors are developing at a rapid pace. At the congress, President Xi envisioned China to become one of the world’s most innovative countries by 2020 and a leading global science and technology power by 2049. Surely, how much of those goals China can be achieved in prescribed time is a matter of debate. But in accordance with these objectives, it is evident that China prioritizes innovation in key generic technologies, cutting-edge frontier technologies, modern engineering technologies, and disruptive technologies.

In the terms of Sino-American relationship, the rigorous competition between two major powers has already expanded to numerous fields, from trade to the protection of cutting-edge technologies and the formation of regional strategies. Their development models are supported by different values and norms. The increased intertwining of geopolitics and technology reflects the underlying intensification of competition between China and the United States and exacerbates the direct competition between the two powers for control over the rules, norms, and institutions which will govern international relations of the new world order in the coming decades, including high-technological developments like artificial intelligence and 5G.

The political leaders of both countries are well aware that technological innovation is a strong source of national power. As a result, technology is now largely politicized and has become a more prominent element of great power rivalry.

There is no doubt that the U.S. is the technological superpower in the world. But China is trying hard to seize this title from it. It has grown very rapidly over the development and application of the critical high tech areas such as artificial intelligence, big data, robotics and 5G and likes and there are concerns about whether China would evolve into a new hegemonic superpower based on superiority in high-tech.

### China Impact: Tech Dominance—Hegemony IL

#### Tech innovation is the cornerstone of leadership

Thompson, Lexington Institute researcher ’20

[Loren B. Thompson, Chief Operating Officer, Lexington Institute & PhD, “Why U.S. National Security Requires a Robus, Innovative Technology Sector,” Lexington Institute, 10—20, p. 3-6]

Introduction: America is facing the most serious challenge to its security in a generation.

Every nation strives for security. Although the phrase “national security” in common usage has military overtones, there are other elements as well— economic, demographic, cultural. For instance, energy security was a major concern of U.S. policymakers in recent decades, and environmental

security related to climate change now garners similar interest.

What every facet of national security has in common, though, is that it is shaped by technology. The wide oceans separating North America from the Eurasian land mass were once thought to confer military security on the republic, but long-range weapons altered the significance of distance. The rapid rise of formerly poor East Asian nations has been driven in large part by their mastery of technologies that did not exist two generations ago.

Technology is thus a critical driver of national security, because it is the variable that determines the significance of all the other factors. In the past, the United States was able to sustain a culture of innovation that permitted it to lead the world in advanced technologies. Now that may be changing as other nations pursue investment initiatives aimed at dominating the global information revolution. For example, the Chinese economy today generates as much manufactured output as Germany, Japan and America combined, and that output increasingly consists of advanced information technology.

This report is about the role that America’s own technology sector plays in bolstering national security. It is focused mainly on the defense dimensions of America’s strategic competition with China and other nations, illuminating how a robust and innovative domestic technology sector can contribute directly and indirectly to U.S. military dominance.

The United States has faced major challenges to its military security in every generation since the 20th century began, and in each case new technology was a key factor defining the danger. The threat posed by imperialism at the century’s beginning was closely associated with development of the dreadnaught. The threat posed by fascism a generation later was driven largely by the advent of air power. And the threat posed by communism in the century’s second half arose first and foremost from nuclear weapons.

Unlike those earlier dangers, the technological content of today’s threat from other nations is grounded largely in commercial innovations— innovations readily adapted to new concepts of warfare. If the United States is to emerge from this latest contest with its leadership position intact, as it did in earlier rivalries, it will have to compete successfully in commercial markets through commercial enterprises. This is not an “arms race” in the traditional sense, but its implications for America’s place in the world are every bit as serious as the danger posed by dreadnaughts and bombers in earlier generations.

What is the technology sector, and why will it be central to national security in the years ahead? The domestic technology sector is that part of the national economy devoted to developing and exploiting new information technologies. During the 1960s and 1970s, it was defined by information hardware such as mainframe computers and semiconductors. The definition later expanded to include enterprises focused on the generation of software. More recently, it has come to encompass companies whose business lines are enabled by the internet, such as Google and Facebook.

It is not easy to define the boundaries of the technology sector, because every segment of the economy now relies on digital innovations and the internet to function. Hardware such as the smartphone is central to the emerging information economy, but many tech companies are engaged primarily in delivering services leveraged off of that hardware. For example, Amazon has transformed marketing and logistics using an internet-based business model, but it is mainly a provider of services rather than hardware. It is, nonetheless, a technology-driven change agent that is revolutionizing commerce.

The military’s interest in the technology sector arises from the fungibility of information innovations across all facets of human activity. The same processors and memory chips that enable iPhones can be applied to smart weapons, battlefield communications, and military training devices. The same algorithms that facilitate machine learning in commercial products can be used to operate unmanned attack drones and autonomous fighting vehicles. And the “internet of things” that links disparate appliances is a model for the joint connectivity the military seeks in wartime.

There is a broad consensus among military planners that the industrial model of warfare spawned by 20th century conflicts is giving way to an information-driven model enabled by new digital technologies. Collectively, these technologies allow warfighters to find, fix and defeat threats faster than adversaries can, while minimizing dangers arising from the fog of war such as fratricide. But the process of innovation is unfolding at a furious pace, and America’s military is hard-pressed to keep up. In August of 2020, the chief of staff of the Air Force released a strategy document aptly titled Accelerate Change Or Lose.

The fear among military planners is that a near-peer adversary might use new technologies to leapfrog beyond the warfighting capabilities of America’s joint force, exploiting technologies that barely existed when the current force was conceived. In June of 2020, the Pentagon’s director of research and engineering issued a list of the highest-priority technologies in which the military needed to invest. The top technologies, in descending order of importance, were (1) microelectronics, (2) 5G communications, (3) hypersonics, (4) biotechnology, (5) artificial intelligence, (6) autonomy, and (7) cyber technologies. Only one of these technologies is predominantly military in character; all the others are mainly the products of commercial innovation.

They are also all technologies that China and other nations have disclosed plans to invest in heavily as they strive to overtake the United States. So from a military perspective, the threat posed by new information technologies is twofold. On the one hand, the United States might be overtaken and surpassed in operationalizing the new technologies as tools for gaining military advantage in future conflicts. On the other hand, if America cannot keep up in the race to innovate, it might eventually lack the economic resources needed to sustain a global military posture.

The U.S. government, and the Department of Defense in particular, invests extensively in such technologies. However, it is widely recognized that the private sector is where innovation in advanced technologies occurs more quickly and more imaginatively. Government can help industry to innovate with targeted funding, tax policy and other exertions, but it cannot create a culture of innovation within the public sector. That requires a structure of incentives that exists only in the marketplace.

#### Tech lead key to heg

Thompson, Lexington Institute researcher ’20

[Loren B. Thompson, Chief Operating Officer, Lexington Institute & PhD, “Why U.S. National Security Requires a Robus, Innovative Technology Sector,” Lexington Institute, 10—20, p. 18-19]

Conclusion: The United States will lose its status as the world’s leading economic and military power if its technology sector falters.

This report began by noting that technology shapes every facet of national security. It determines whether the nation possesses sufficient economic resources to compete with other nations; it impacts the quality of military equipment and training; it shapes the ability of popular culture to influence the values of other nations; it even drives socio-economic trends that are the foundation of who Americans are as a people. In short, technology and the economic sector that produces it are the most dynamic force driving the future of our civilization.

Many, perhaps most, Americans understand this. However, for many years the preeminence of American technology in the world has been taken as a given. That preeminence can no longer be assumed. China is working to dethrone America from its status as the sole global superpower, and so far every step it has taken to achieve that end has been successful. If Washington does not rethink its policies, this may be the last generation that can legitimately claim that America leads the world in economic and military power. Protecting the culture of innovation centered in the nation’s technology sector is central to preserving the American future.

### China Impact: Tech Dominance—Liberal Order IL

#### Chinese dominance threatens the global liberal order

Talent, Bipartisan Policy Center and Work, Center for a New American Security ’19

[Jim Talent, Senior Fellow, Bipartisan Policy Center and former U.S. Senator and Robert O. Work, Distinguished Senior Fellow, Center for a New American Security and former Deputy Secretary of Defense, plus 11 other Task Force members, “The Contest for Innovation: Strengthening America’s National Security Innovation Base in an Era of Strategic Competition,” Report of the Task Force on 21st-Century National Securi .ty Technology and Workforce, Ronald Reagan Institute, 2019, p. 9]

Imagine that the Chinese Communist Party, through its control of China’s economy, is allowed to set the global ground rules for the next generation of technology. Imagine phones, tablets, and computers that do not function unless they conform to Chinese standards and censorship requirements or that contain materials that can transmit to Beijing a record of everything that is written, stored, and shared online. Imagine further that authoritarian leaders, armed with class-leading technologies like artificial intelligence, facial recognition, and quantum computing, turn that awesome computing power against people and their data. Imagine finally how autocrats might be able to coerce citizens by leveraging this power.

A real-life example is before us today. Witness the treatment of the million men, women, and children in Xinjiang that Chinese officials identified and targeted with the help of facial recognition technology and data-scraping tools. Innocent people have been rounded up into concentration camps for “reeducation” in Communist Party dogma. That is Beijing’s policy toward its own citizens. How much restraint would China show toward those it deems “outsiders”?

We offer this narrative to explain why the subject of this report is so important. Competition with China need not lead to warfare or even to a policy of containment like the framework that characterized the U.S.–Soviet relationship during the Cold War. Nevertheless, it is a competition, and the side that innovates more effectively over time is likely to win. The result will determine whether nations relate to each other freely, equally, and peacefully, with a recognition of the human rights of their citizens, or if they devolve into a system that legitimizes authoritarianism and rewards power and coercion.

### China Impact: Tech Dominance—War Impact

#### Chinese tech dominance is an existential threat—war

Suchodolski et al., USN General Counsel, ’20

[Jeanne Suchodolski, Attorney, U.S. Navy Office of General Counsel, Suzanne Harrison, Founder, Percipience LLC, Bowman Heiden, Co-Director, Center for Intellectual Property and Visting Professor, University of California, Berkeley, “Innovation Warfare,” NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY v. 22 n. 2, 12—20, p. 176-179]

Innovation, in particular, technology-based innovation, is the key driver for both economic competitiveness and national security. Other nations, with interests adverse to the United States, recognize this fact. In an increasingly interconnected world, nation states seek to accumulate innovation prowess, and hence economic strength, as a key element of their geopolitical power. Especially savvy nation states also pursue such ends as a mechanism to influence or diminish the national security and geopolitical power of the United States. There is no need to inflict upon the world the carnage of war if one’s geopolitical aims can be achieved via alternative competitive means.

Several authors suggest China’s long-term ambitions include unseating the United States as the world’s economic and political leader.1

More compelling than opinions, several United States (“U.S.”) government and private studies document a systematic and coordinated effort by China to achieve technical and economic dominance through misappropriation of U.S. technology.2 These efforts are additionally supported by a companion effort to weaken international economic institutions and norms designed to protect U.S. intellectual property and free trade.3 The Chinese tactics include illegal means, and sophisticated use of legal means, to misappropriate U.S. technology and weaken the U.S. innovation infrastructure including:

a) Leveraging the open university and laboratory ecosystem via direct sponsorship and engagement of Chinese nationals;4

b) Devaluing U.S. positions in patents and technology platforms;5 and

c) Accessing private sector U.S. technology through acquisitions and ownership stakes in existing firms, funding of high-tech start-ups, and forced joint ventures and other contractual agreements as a prerequisite for entering the Chinese market.6

This particular form of competitive strategy targeting the innovation ecosystem in the United States is labeled by the Authors as “Innovation Warfare,”7 and it is defined as an executable competitive strategy:

a) Reflecting an innovation, intellectual property, and technology strategy articulated and executed by the state (e.g. China);

b) Using illegal means, political means, and legal economic activities—of the type previously residing solely in the province of commercial enterprise, to achieve the state’s objectives;

c) Employing these economic and innovation activities to achieve both economic geopolitical power and to enhance military capabilities; and

d) Functioning as a military, national security, and defense doctrine not solely as a reflection of the state’s economic policy goals nor commercial competition in the ordinary course.

Innovation Warfare does not just threaten American jobs and economic prosperity. By simultaneously co-opting and weakening the innovation capabilities of the United States, China seeks to advance its rise to world power. China’s prosecution of Innovation Warfare not only encompasses a rejection of a rules-based international order, but also poses an existential threat. A world where China dominates the technology landscape is not just about who earns the profits or prevails in an abstract geopolitical fight. According to the National Security Strategy of the United States of America (“National Security Strategy”), China pursues a world in which economies are less free, less fair, and less likely to respect human dignity and freedoms.8 China’s Innovation Warfare activities risk the type of economic and geopolitical aggressions that were a root cause of two World Wars.

#### Shifts in relative power cause war—miscalc

Nye ’21 [Joseph S. Nye Jr, Professor, Harvard University, “The Factors that Could Lead to War Between the U.S. and China,” THE STRATEGIST, Asutralian Strategic Policy Institute, 3—3—21, <https://www.aspistrategist.org.au/the-factors-that-could-lead-to-war-between-the-us-and-china/>, accessed 6-3-22]

When China’s foreign minister, Wang Yi, recently called for a reset of bilateral relations with the United States, a White House spokesperson replied that the US saw the relationship as one of strong competition that required a position of strength. It’s clear that President Joe Biden’s administration is not simply reversing Donald Trump’s policies.

Some analysts, citing Thucydides’ attribution of the Peloponnesian War to Sparta’s fear of a rising Athens, believe the US–China relationship is entering a period of conflict pitting an established hegemon against an increasingly powerful challenger.

I am not that pessimistic. In my view, economic and ecological interdependence reduces the probability of a real cold war, much less a hot one, because both countries have an incentive to cooperate in a number of areas. At the same time, miscalculation is always possible and some see the danger of ‘sleepwalking’ into catastrophe, as happened with World War I.

History is replete with cases of misperception about changing power balances. For example, when US President Richard Nixon visited China in 1972, he wanted to balance what he saw as a growing Soviet threat to a declining America. But what Nixon interpreted as decline was really the return to normal of America’s artificially high share of global output after World War II.

Nixon proclaimed multipolarity, but what followed was the end of the Soviet Union and America’s unipolar moment two decades later. Today, some Chinese analysts underestimate America’s resilience and predict Chinese dominance but this, too, could turn out to be a dangerous miscalculation.

It is equally dangerous for Americans to over- or underestimate Chinese power, and the US contains groups with economic and political incentives to do both. Measured in dollars, China’s economy is about two-thirds the size of that of the US, but many economists expect China to surpass the US sometime in the 2030s, depending on what one assumes about Chinese and American growth rates.

Will American leaders acknowledge this change in a way that permits a constructive relationship, or will they succumb to fear? Will Chinese leaders take more risks, or will Chinese and Americans learn to cooperate in producing global public goods under a changing distribution of power?

Recall that Thucydides attributed the war that ripped apart the ancient Greek world to two causes: the rise of a new power and the fear that this created in the established power. The second cause is as important as the first. The US and China must avoid exaggerated fears that could create a new cold or hot war.

Even if China surpasses the US to become the world’s largest economy, national income is not the only measure of geopolitical power. China ranks well behind the US in soft power and US military expenditure is nearly four times that of China. While Chinese military capabilities have been increasing in recent years, analysts who look carefully at the military balance conclude that China will not, say, be able to exclude the US from the Western Pacific.

On the other hand, the US was once the world’s largest trading economy and its largest bilateral lender. Today, nearly 100 countries count China as their largest trading partner, compared to 57 for the US. China plans to lend more than US$1 trillion for infrastructure projects with its Belt and Road Initiative over the next decade, while the US has cut back aid. China will gain economic power from the sheer size of its market as well as its overseas investments and development assistance. China’s overall power relative to the US is likely to increase.

Nonetheless, balances of power are hard to judge. The US will retain some long-term power advantages that contrast with areas of Chinese vulnerability.

One is geography. The US is surrounded by oceans and neighbours that are likely to remain friendly. China has borders with 14 countries, and territorial disputes with India, Japan and Vietnam set limits on its hard and soft power.

Energy is another area where America has an advantage. A decade ago, the US was dependent on imported energy, but the shale revolution transformed North America from energy importer to exporter. At the same time, China became more dependent on energy imports from the Middle East, which it must transport along sea routes that highlight its problematic relations with India and other countries.

The US also has demographic advantages. It is the only major developed country that is projected to hold its global ranking (third) in terms of population. While the rate of US population growth has slowed in recent years, it will not turn negative, as in Russia, Europe, and Japan. China, meanwhile, rightly fears ‘growing old before it grows rich.’ China’s labour force peaked in 2015 and India will soon overtake it as the world’s most populous country.

America also remains at the forefront in key technologies (bio, nano and information) that are central to 21st-century economic growth. China is investing heavily in research and development, and competes well in some fields. But 15 of the world’s top 20 research universities are in the US; none is in China.

Those who proclaim Pax Sinica and American decline fail to take account of the full range of power resources. American hubris is always a danger but so is exaggerated fear, which can lead to overreaction. Equally dangerous is rising Chinese nationalism, which, combined with a belief in American decline, leads China to take greater risks. Both sides must beware of miscalculation. After all, more often than not, the greatest risk we face is our own capacity for error.

### China Impact: War / Revisionist

#### Conflict risks are high—many drivers

Lyons, Belfer Center fellow ‘22

[Marco Lyons, National Security Fellow 2022, Belfer Center, “China’s Rise and U.S. Defense Implications,” POLICY BRIEF, Belfer Center for Science and International Affairs, Harvard Kennedy School, 1—14—22, <https://www.belfercenter.org/publication/chinas-rise-and-us-defense-implications>, accessed 6-12-22]

There may be circumstances and options for major powers to control their ambitions and cooperate for stability and peaceful development, but the drivers for conflict point to even more intense competitive rivalry. Significant drivers for war include: diminishing arms control; weakening international institutions; persistent competition between democracies and autocratic states; increasing nationalism; advancements in long-range strike, and in nontraditional ways of warfare; and a possible explosion in mis- and disinformation.19 U.S. China scholars and policy experts have been starting to refer to decisive turning points in Washington-Beijing relations, such as the March 2021 meeting in Alaska between senior officials, and this may reflect a growing sense that the stakes involved are significantly higher than in any recent period.20 China will continue working for a dominant regional position, as a major power may be expected to do, but it is also maneuvering for global power, and these advances to the global stage may surprise American strategists if Beijing does not follow expected paths.21 While power shifts alone should not spell future armed conflict, the U.S.-China rivalry has multiple dimensions, including technological, security-defense, and ideological, and that suggests that the drivers for conflict will be hard to manage for both sides.

#### China is a revisionist power—any war will escalate

Beckley, Tufts professor and Brands, Johns Hopkins professor, ‘21

[Michael Beckley, Visiting Fellow, American Enterprise Institute and Associate Professor, Tufts University and Hal Brands, Senior Fellow, American Enterpreise Institute and Henry A. Kissinger Distinguished Professor of Global Affairs, School of Advanced International Studies, Johns Hopkins University, “What Will Drive China to War?” THE ATLANTIC, 11—1—21, <https://www.theatlantic.com/ideas/archive/2021/11/us-china-war/620571/>, accessed 6-12-22]

Beijing is a remarkably ambitious revanchist power, one determined to make China whole again by “reuniting” Taiwan with the mainland, turning the East and South China Seas into Chinese lakes, and grabbing regional primacy as a stepping-stone to global power. It is also increasingly encircled, and faces growing resistance on many fronts—just the sort of scenario that has led it to lash out in the past.

The historical record since the founding of the People’s Republic of China in 1949 is clear: When confronted by a mounting threat to its geopolitical interests, Beijing does not wait to be attacked; it shoots first to gain the advantage of surprise.

In conflicts including the Korean War and clashes with Vietnam in 1979, China has often viewed the use of force as an educational exercise. It is willing to pick even a very costly fight with a single enemy to teach it, and others observing from the sidelines, a lesson.

Today, Beijing might be tempted to engage in this sort of aggression in multiple areas. And once the shooting starts, the pressures for escalation are likely to be severe.

### China Solvency: NATO Action

#### NATO coordination enables coalitions of the willing within the alliance to solve the Chinese hybrid threat

Speranza, Cetner for European Policy Analysis researcher, ‘20

]Lauren Speranza, Director, Trans-Atlantic Defense and Security, Center for European Policy Analysis, “China Is NATO’s New Problem,” FOREIGN POLICY, 7—8—20, <https://foreignpolicy.com/2020/07/08/china-nato-hybrid-threats-europe-cyber/>, accessed 5-7-22]

Over the past decade, Chinese companies have invested billions of dollars throughout Europe—buying up critical infrastructure and increasing Beijing’s political clout across the continent. As Chinese firms, often with strong ties to the state and Chinese Communist Party (CCP), acquire parts of sensitive ports, pipelines, and telecommunication networks, China’s incursions into Europe’s security umbrella are drawing serious concern.

But NATO, long worried about Russia, has largely been silent on China. Now, that is changing. NATO Secretary-General Jens Stoltenberg recently called on the alliance to stand up to Beijing’s “bullying and coercion,” underscoring how China’s rise is fundamentally shifting the global balance of power. It’s apparent that NATO can no longer ignore the threat. If the alliance hopes to remain competitive, it will need to develop a new strategy for dealing with Beijing.

First, NATO needs a common assessment of China’s hybrid threats—a mix of diplomatic, economic, security, information, and technological actions designed to quietly undermine democratic states and institutions to Beijing’s benefit while avoiding a traditional conflict. While China’s conventional military threat in the Indo-Pacific is far from NATO’s borders, its hybrid activities are happening in the alliance’s own backyard.

Cyber-espionage, intellectual property theft, infiltration of critical infrastructure, debt manipulation, and disinformation are prime examples. While these threats may seem to fall outside of NATO’s purview, they pose serious security risks for the alliance. For instance, China’s desire to invest in Lithuania’s Klaipeda Port may not look like a problem for NATO on its surface. But its investments have worrying strings attached that give China operating control over the infrastructure. That control could decrease allies’ willingness to move military forces—including sensitive technologies—through the port and its surrounding networks. This could lead to disrupted planning and fewer military exercises, decreasing NATO’s ability to defend the Baltic States during a crisis with Russia. This could also open the door for pragmatic collaboration between China and Russia to undermine trans-Atlantic security.

Allies need to forge a shared understanding of these risks through information-sharing and dialogue—no small feat for countries that do not see eye to eye on China. Some are even willing to ignore such vulnerabilities, due to economic benefits or disenchantment with trans-Atlantic institutions. The United States has a critical role to play in getting allies on the same page and setting common goals for countering China’s hybrid activities.

Second, NATO needs to focus on public diplomacy. NATO has an important role to play in the battle against the CCP’s global narratives, which Beijing promulgates through hybrid activities. To defend the trans-Atlantic values on which the alliance is built—freedom, democracy, rule of law, and human rights—NATO should clearly communicate China’s violations of these principles and its propaganda efforts to cover them up. (These include, among others, human rights abuses against ethnic Uighurs in Xinjiang and violations of the U.N. Convention on the Law of the Sea in the South China Sea.) NATO should also enhance its outreach to key partners in the Indo-Pacific, such as Australia, Japan, New Zealand, and South Korea, which can serve as important counterweights to Chinese influence in the region. Effective public messaging also means getting serious about attributing the blame for attacks, as the European Commission recently did over Chinese disinformation around COVID-19, to raise the pressure on Chinese officials. Trans-Atlantic countries have struggled to shape China’s behavior because they cannot prove malign intent or agree to call out Beijing for its subversive efforts. Allies should develop clearer guidelines—what needs to be proved, by whom, and to what degree—to enable collective attribution. NATO is strongest when it speaks with one voice. It should use that voice to demand transparency and change from China.

Third, the alliance should step up its counteroffensive. China’s hybrid actions intentionally blur the lines between what is legally permissible, politically inappropriate, and downright escalatory.

This makes it difficult for leaders to determine appropriate responses, producing a reactionary approach thus far. But an intensifying geostrategic competition has already begun. To compete in this environment, the trans-Atlantic community needs a more proactive approach. Rather than waiting for China to invest in the next major European port, allies should coordinate legislation to prevent the riskiest Chinese acquisitions. And rather than waiting for more Chinese cyberintrusions, allies should collaborate on responsible, targeted offensive cyberactions. Over time, this would help dissuade China from manipulating investments in critical infrastructure, conducting cyber-espionage, and other hybrid activities. While adopting a more offensive posture remains controversial among certain allies, it is gaining traction across Europe and is strongly supported in Washington. Although NATO, as a defensive alliance, should not implement such a counteroffensive, policymakers should leverage it as the primary forum to coordinate actions among willing nations.

Fourth, NATO needs to deepen its cooperation with other key players, such as the European Union and the private sector. Where NATO lacks the mandate and means, the EU and multinational businesses play critical roles in developing, implementing, and enforcing the legislation and financial incentives necessary to counter Chinese hybrid threats. Complementary to that, NATO and its allies can focus on providing intelligence, defending cyberspace, developing capability targets for new technologies, conducting exercises and contingency planning, informing resilience requirements for secure infrastructure, and bolstering deterrence. Despite the political obstacles that impede more formal NATO-EU cooperation, allies should look to the European Centre of Excellence for Countering Hybrid Threats in Helsinki to bring together NATO and EU staff, national officials, and industry voices in one place to align their counter-hybrid policies for China.

The Chinese government’s manipulative efforts around the coronavirus have thrust China’s hybrid activities to the center of trans-Atlantic debates. Policymakers need to seize the moment and respond by “using NATO more politically,” in Stoltenberg’s words. NATO is first and foremost about its nations. In the fight against China’s hybrid threats, these nations bring much more to the table than military power alone. They have access to a broad range of tools—military, political, economic, technological, and information—which the alliance can use to its collective geopolitical advantage in the competition with China. What NATO needs now is a strategy to leverage those tools in a coordinated manner. That will go a long way in solving NATO’s China problem.

#### Strong NATO enables U.S. to manage China’s rise

Lute & Burns, Harvard researchers, ‘19

[Ambassador Douglas Lute, Senior Fellow, Belfer Center and President, Cambridge Global Advisors and Ambassador Nicholas Burns, Professor, Diplomacy and International Politics, Harvard Kennedy School, “NATO at Seventy: An Alliance in Crisis,” Project on Europe and the Transatlantic Relationship, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2—19, p. 37]

Most important, on the scale of grand strategy, the rising challenge from China underlines the enduring importance of the NATO alliance. The defining geo-strategic contest of the 21st century will be between the U.S. and China, which will play out in political, economic and perhaps military dimensions. Both Europe and America are best postured for this competition inside a strong, cohesive NATO that balances the security burden equitably and enables the U.S. increasingly to focus on China. This looming strategic reality amplifies the recommendations of this report. NATO, the trans-Atlantic bond, will become even more important as China’s power grows. The goal is to live and work with China where possible but to compete to maintain the primacy of the free, democratic countries in both Europe and the Indo-Pacific.

#### A strong NATO better positions the U.S. to address the China challenge

Lute & Burns, Harvard researchers, ‘19

[Ambassador Douglas Lute, Senior Fellow, Belfer Center and President, Cambridge Global Advisors and Ambassador Nicholas Burns, Professor, Diplomacy and International Politics, Harvard Kennedy School, “NATO at Seventy: An Alliance in Crisis,” Project on Europe and the Transatlantic Relationship, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2—19, p. 8]

While China does not pose a direct military threat to most NATO allies, it is emerging as a global competitor politically, economically and in seeking dominance in digital military technologies. Europe, the United States and Canada need to adopt a more cohesive approach to China. Beijing is emerging as the strongest strategic competitor of both North America and Europe in this century. The European allies need to focus more intently on the challenge from Chinese economic and technological power and industrial espionage. NATO allies should thus tighten restrictions on Chinese investments in key technology sectors on both sides of the Atlantic. And NATO should strengthen its military partnerships with Japan, South Korea, Australia, New Zealand and others.

China will be the main geo-strategic competitor of the United States in the decades ahead. It is in the interest of NATO allies to take on the defense burden in the trans-Atlantic region more equitably, to enable the U.S. to focus increasingly on the competition with China. In this strategic sense, NATO’s military strength and unity could be a potentially decisive factor in the long-term competition ahead in the Indo-Pacific. The goal is to live and work with China where possible, but to compete to maintain the primacy of the free, democratic countries in both Europe and the Indo-Pacific.

#### Allies and our tech edge are vital to staying ahead of China

Magnuson, NDM Editor, ‘21

[Stew Magnuson, Editor-in-Chief, “The Quad: Creating a Defense Tech Alliance to Stand Against China,” NATIONAL DEFENSE, 12—7—21, <https://www.nationaldefensemagazine.org/articles/2021/12/7/creating-a-defense-tech-alliance-to-stand-against-china>, accessed 4-23-22]

When it comes to the undeclared Technology War between the United States and China, there is a lot for Americans to be worried about.

Beijing seems to have the advantage in several key areas which is causing a great deal of consternation in Washington.

The U.S. rival has become adept at industrial espionage and is stealing billions of dollars worth of intellectual property.

China has a command economy and long-term vision on where it wants to be in regards to technology development. It doesn’t have to contend with hyper partisanship and delayed budgets.

The nation is cornering the markets on raw materials, particularly strategic minerals needed for advanced technologies.

And it has a seemingly unending pile of money to invest in emerging technologies that may give its military — and economy as a whole — a winning edge.

But there is one thing the United States has in abundance that China is sorely lacking: friends and allies.

U.S. military leaders often say that the United States does not go to war alone — it fights alongside friends and allies.

This special report is devoted to the notion that the military research-and-development community must adopt the same approach. It must form partnerships with allied nations to develop the cutting edge technologies needed to stand against China’s goals of hegemony in the Indo-Pacific.

And while this is a defense magazine, our editorial stance has been that it’s myopic to look at the rivalry with China solely through the lens of military technology. China has clearly stated goals to advance the development of a host of commercial and dual-use technologies that it could employ to dominate both battlefields and commercial sectors, thus making it a global leader and economic powerhouse, potentially leaving the United States and its allies behind.

#### The U.S. needs to lead in threat assessment of China’s hybrid activities—vital to solving

Speranza, Center for European Policy Analysis director, ‘20

[Lauren Speranza, Director, Trans-Atlantic Defense and Security, Center for European Policy Analysis, “China Is NATO’s New Problem,” FOREIGN POLICY, 7—8—20, <https://foreignpolicy.com/2020/07/08/china-nato-hybrid-threats-europe-cyber/>, accessed 5-22-22]

But NATO, long worried about Russia, has largely been silent on China. Now, that is changing. NATO Secretary-General Jens Stoltenberg recently called on the alliance to stand up to Beijing’s “bullying and coercion,” underscoring how China’s rise is fundamentally shifting the global balance of power. It’s apparent that NATO can no longer ignore the threat. If the alliance hopes to remain competitive, it will need to develop a new strategy for dealing with Beijing.

First, NATO needs a common assessment of China’s hybrid threats—a mix of diplomatic, economic, security, information, and technological actions designed to quietly undermine democratic states and institutions to Beijing’s benefit while avoiding a traditional conflict. While China’s conventional military threat in the Indo-Pacific is far from NATO’s borders, its hybrid activities are happening in the alliance’s own backyard. Cyber-espionage, intellectual property theft, infiltration of critical infrastructure, debt manipulation, and disinformation are prime examples. While these threats may seem to fall outside of NATO’s purview, they pose serious security risks for the alliance. For instance, China’s desire to invest in Lithuania’s Klaipeda Port may not look like a problem for NATO on its surface. But its investments have worrying strings attached that give China operating control over the infrastructure. That control could decrease allies’ willingness to move military forces—including sensitive technologies—through the port and its surrounding networks. This could lead to disrupted planning and fewer military exercises, decreasing NATO’s ability to defend the Baltic States during a crisis with Russia. This could also open the door for pragmatic collaboration between China and Russia to undermine trans-Atlantic security.

Allies need to forge a shared understanding of these risks through information-sharing and dialogue—no small feat for countries that do not see eye to eye on China. Some are even willing to ignore such vulnerabilities, due to economic benefits or disenchantment with trans-Atlantic institutions. The United States has a critical role to play in getting allies on the same page and setting common goals for countering China’s hybrid activities.

### China Solvency: Transatlantic Coop

#### US-European unity is vital to checking China

Taussig, Harvard’s Project on Europe and the Transatlantic Relationship Research Director, ‘20

[Torrey Taussig, Research Director in the Project on Europe and the Transatlantic Relationship (PETR) at Harvard Kennedy School and Non-Resident Fellow at the Brookings Institution, STRONGER TOGETHER: A STRATEGY TO REVIALIZE TRANSATLANTIC POWER, Belfer Center for Science and International Affairs, Harvard University and German Council on Foreign Relations (DGAP), 12—20, p. 39]

The U.S. and Europe will be stronger if they work together on a strategy toward China. They should capitalize on their converging assessment of the challenges posed by China to strengthen dialogue and pursue a common path forward. A shared agenda will require the Biden administration to restore trust in the transatlantic relationship. It will also require Europe to unite around tougher policies where it sees China infringing on European values and interests.

Only together can the U.S. and Europe build the leverage necessary in trade, technology and multilateral engagement to hold China to a set of standards that protects democratic societies and contributes to global stability. United they can rally other nations around these objectives.

#### Better relations key to challenging China

Taussig, Harvard’s Project on Europe and the Transatlantic Relationship Research Director, ‘20

[Torrey Taussig, Research Director in the Project on Europe and the Transatlantic Relationship (PETR) at Harvard Kennedy School and Non-Resident Fellow at the Brookings Institution, STRONGER TOGETHER: A STRATEGY TO REVIALIZE TRANSATLANTIC POWER, Belfer Center for Science and International Affairs, Harvard University and German Council on Foreign Relations (DGAP), 12—20, p. 35]

Both sides of the Atlantic are converging in their assessment of the challenges China poses to transatlantic prosperity and democracy. The U.S. and Europe must now build on this convergence to advance a common strategy toward China. Only together can the U.S. and Europe, alongside other democratic nations, maintain the necessary leverage in trade, technology and multilateral engagement to hold China accountable to a set of standards that protects democratic societies and contributes to global stability.

To develop a stronger transatlantic approach toward China, the Biden administration must work to rebuild trust in the transatlantic relationship and recommit to multilateral alliances and institutions abandoned by President Trump. Europe for its part must unite and take action where it sees China exploiting its critical industries and infringing on its values. A common position on China at the EU–level and across several influential EU member states is critical to making transatlantic cooperation on China feasible.

### China Solvency: Resilience—China Espionage

#### Resilience measures help address the China cyber espionage threat

Kramer, Atlantic Council fellow, ‘19

[Franklin. D. Kramer, Distinguished Fellow and Board Member, Atlantic Council, “Managed Competition: Meeting China’s Challenge in a Multi-Vector World,” Scowcroft Center for Strategy and Security, Atlantic Council, 12—19, p. 39-40]

C. Security—Hybrid and Conventional Military

In the security arena, assurance, resilience, and deterrence measures will be necessary to respond to both hybrid and conventional challenges posed by China.

1. Hybrid: China’s hybrid activities include cyber espionage, economic coercion, and low-level use of force. Many of the response options include military activities, but it is worth underscoring that US military leaders uniformly support strong diplomatic efforts.

a. Countering cyber espionage

Chinese cyber espionage has been significant even apart from the issues raised by Huawei in conjunction with the establishment of 5G networks. No complete solution can be expected, but significant benefits can be achieved by enhancing resilience and raising the cost of cyber intrusions. Cybersecurity issues are not limited to China. Russia, North Korea, Iran, and criminal and terrorist organizations likewise are significant threats. Accordingly, a cyber response to China will necessarily be part of a larger cybersecurity effort, though certain parts of an overall approach could be China-directed.

Accomplishing cybersecurity objectives requires a multifaceted approach, including 1) development and deployment of advanced technologies and critical capabilities such as cloud technologies, automation, and AI; 2) public-private “coordinated partnerships” for protection of confidential government and business information as well as key critical infrastructure arenas; 3) significant governmental efforts that include resources; 4) legal remedies and sanctions to ensure that cyber intrusions provide no benefits; 5) appropriate use of the US doctrine of “persistent engagement and defending forward”; and 6) like-minded countries working together via an International Cyber Stability Board. Countries with more significant cyber capabilities will have greater success in dealing with Chinese cyber activities, so Multi-vector international coordination to enhance cybersecurity capacity can have significant value.210 The recently enacted Asia Reassurance Initiative Act of 2018 (ARIA) specifically authorizes $100 million annually for cybersecurity cooperation to “strengthen resilience against cyberattacks, misinformation, and propaganda” and to “strengthen the resilience of critical infrastructure.”211 These arenas are generally understood by each country in the region, but practical cooperation needs to be enhanced.

Overcoming vulnerabilities and enhancing cybersecurity resilience will require multiple steps. In dealing with its own vulnerabilities, the US government is shifting its approach of increasing resilience to greater use of cloud technology provided by expert firms and supported by other advanced capabilities such as AI and automation. Further actions should include providing a standard “resilience architecture” for contractors and subcontractors, and necessary additions of cybersecurity personnel and budgetary funding to the US Department of Homeland Security (DHS) and the DoD.212

A comparable approach is required for the private sector. Most organizations do not have the expertise or resources to provide effective cybersecurity, and will, therefore, benefit greatly from utilizing cloud technology run by experts for data storage and provision of services. Businesses, of course, have to connect to the cloud and protect information at their own sites. This can be done through “software defined networks,” which are one of the developing advanced technologies, as well as the employment of expert firms that can monitor and respond to activities on a business’s networks. To help assure the requisite expertise, the government could create a certification approach, including the frameworks for effective “resilience architectures”—though, since cyber is a highly dynamic arena, it will be important not to create a checklist, but rather adopt a performance-oriented approach.

There are a variety of ways to organize international interactions. A valuable starting point would be organizing around like-minded countries and organizations, including through the establishment of an International Cyber Stability Board.213 Such a board could focus on provision of protection and resilience to key cross-border critical infrastructures, including finance and transportation; undertake a multinational campaign response to malignant cyber actions by a significant nation state and criminal threats; and enhance capabilities to defend against armed attack, including with allies and close partners. It is important to recognize that technology is not the only way to deal with cyber attacks. Legal remedies, including the use of sanctions, freezing of assets, and forfeitures can have a key role. Such actions can have greatest effect when coordinated at a multinational level.

#### Resilience startegies can check Chinese efforts

Kramer, Atlantic Council fellow, ‘19

[Franklin. D. Kramer, Distinguished Fellow and Board Member, Atlantic Council, “Managed Competition: Meeting China’s Challenge in a Multi-Vector World,” Scowcroft Center for Strategy and Security, Atlantic Council, 12—19, p. 3-4]

3. Security

In the security arena, undertaking assurance, resilience, and deterrence measures will be necessary when responding to both hybrid and conventional challenges. The most significant unresolved challenge is in the cyber arena where China has utilized its capabilities to steal advanced technologies and to undertake continuous attacks, including through “advanced persistent threats,” and where the expansion of technology from China’s Huawei Technologies Co., Ltd. into the 5G arena will significantly increase security risks for users of this technology.

a. Hybrid

In the hybrid arena:

■ for cyber, undertake expanded development of resilience capabilities, create an International Cyber Stability Board of like-minded nations to respond to ongoing Chinese cyber campaigns, place limits on the use of Chinese technology as key elements in national information technology infrastructures, and establish additional legal remedies focused on denying benefits to those using illegally obtained information;

■ responses to economic coercion should include a governmental review of technology transfers to reduce pressure on companies, coordinated diplomacy to generate multilateral objections to any such actions against a single country, and evaluation of the creation of backup financial mechanisms to ameliorate economic cutoffs by China;

■ Chinese attempts to limit free speech, particularly outside China or by non-Chinese entities, should be met with diplomatic support, countervailing economic actions including sanctions, and by civil society groups monitoring and making public inappropriate censorship activities; and

■ opposition to low-level use of force will require security activities in the East and South China Seas, including diplomatic support, freedom of navigation activities, and expansion of maritime initiatives to provide intelligence that includes a common maritime picture, and capabilities and training.

### China Solvency: Resilience—Tech Innovation / Cooperation

#### NATO-grounded resilience policies spur technological innovation

Efthymiopoulos, UCLan Cyprus Visiting Fellow ‘19

[Marios Panagiotis Efthymiopoulos, Senior Visiting Fellow, Law School UCLan Cyprus, Pyla-Larnaka, Cyprus, “A Cyber-Security Framework for Development, Defense and Innovation at NATO,” JOURNAL OF INNOVATION AND ENTREPRENEURSHIP v. 8 n. 12, 2019, p. 3-5]

Cyber-security is yet to be globally, legally, operationally, and strategically defined. The scale of a security perspective is more attractive at this time considering the geostrategic challenges and threats. The possibility of innovation and entrepreneurship in the field is also a tangible reality, due to the necessary research and development methods. More so, the possibility of an open market economy sharing of knowledge and technological skills makes security and cyber-security or defense for that matter more attractive. What lacks in the world wide legal and political framework of operations, exchange of information and protectiveness from new sources or methods that can be deemed as elements of infiltration.

The article’s aim is to examine and recommend a global strategic framework for operational capacity and management resilience between allied and cooperative partners in the field of cyber-security. The current article is a follow up of prior scientific publications made in 2014 first and later in 2018, on NATO’s cyber-security strategy, presented through a framework of Cyber-Development, Cyber-Democracy, and Cyber-Defense (Carayannis, Campbell & Efthymiopoulos, 2014; Carayannis, Campbell & Efthymiopoulos, 2018). The aim is to converge diversified information on cyber-security, in a single strategic framework; reflect to the actual practical needs in understanding operations and tactical ability to deliver in multi-complex and dimensional world through management and operational efficiency capabilities. The article requests interoperability of aims and objectives under a global framework of cyber-security; through a strategic framework on cyber-security, global law can be proposed, defined, and adopted by the international community. The strategic framework will define structures that are needed to be put in place on a global scale, when reflecting issues of cyber-security and inclusive for NATO. It will define threats and challenges, as cyber-attacks are real. Cyber-security is not an asymmetrical or hybrid threat, but an existential one. Its destructive capacity can be multi-leveled and can also lead to human casualties. The future of e-safety lays at both a global estimation framework of what constitutes cyber-security and how we react to it; it lays in between cooperation of allies and members of wider alliances, against specified or approximate threats. Yet, its framework of aims and objectives, management, command and control, and operations will be defined and decided by allied parties only such as is the case of NATO.

Operationally, national and cooperative forces need to be continuously agile and technologically advanced. In an asymmetrical world, which is complete with unforeseen challenges and threats, we need forces with flexibility, adaptability, operational and strategic command structure, based on high technologically sophisticated information “coming in,” but also being used while in training or through active operations.

On a theoretical scale, the current article requests a cyber-security strategic framework adoption of resilient adaptability and interoperability policy in the framework of safety and defense. The article considers that understanding the realities of threats is by definition a natural innovation and as we move ahead, we structure and operate a single strategy on cyber-security against a virtual threat from wherever it comes from. Its long-term resilience may be more complex as operational capacity needs to constantly develop and adapt into the convergence of societal structures, and methods; where socio-economic, technological, defense even health, and education issues are affected.

When theory on cyber-security, resilience, and operational capacity will be applied at NATOs level, it will enable allies and members, jointly, to create a true policy and strategy for cyber-security resilience against hybrid virtual threats. The methodology on how to is presented through this current article.

The article’s design is based on cross-disciplinary and interdisciplinary approaches. It combines elements of global security and strategy, national and international law, economic development, and technological research and advancement and most importantly is innovative and entrepreneurial; its understanding will enable us to comprehend global and regional market establishment and convergence, as also economic changes.

The setting of the study required lapse of time to showcase the need and the necessity of the subject. Current output reflects a set of written analyses, rules, and primary experiences. It methodologically acquired sources of information of related necessity and relevance, shaped the understanding, and need to point out for a framework of rules, regulations, management, and operations on cyber-security.

The article and its author frames a specific policy recommendation with regards to the creation of not only a regional alliance (NATO-based scale), Cyber-Security Strategy for the twenty-first century but a global one. The article defines the “dynamism” of cyber-security both as a topic and subject. Cyber-security is a twenty-first century element of policy orientation; a necessity for both collective and individual defense and security resilience.

In specific, a cyber-security strategy for NATO will enhance its innovation and creativity core of operations and methodologies against any kind of virtual threats. It will set standards, policy procedures, and recommendations. NATO’s strategy of cyber-security through its new Cyberspace Operations Centre, in Mons (Belgium) as decided in the Brussels Summit of July 2018 (Cyber-Space Operations Center Mons Belgium, 2018) unfolds options and opportunities, innovation, and entrepreneurship in operations efficiency and capabilities application. Current technological advancements and dynamisms through innovation and sustainable futuristic advancement will soon be evident.

#### NATO tech cooperation—including with partners—is critical to checking China

Nouwens, IISS Senior Fellow, ‘22

[Meia Nouwens, Senior Fellow for Chinese Defence Policy and Military Modernisation, International Institute for Strategic Studies, “NATO and China: Addressing New Challenges,” CSDS Policy Brief, Centre for Security, Diplomacy and Strategy, Brussels School of Governance, 3—9—22, p. 5]

The challenges posed by China to the alliance are not new. Already in the last ten years, allies have been grappling with issues of foreign investment into strategic industries and critical infrastructure, imbalanced trade relationships with China, influence operations and disinformation, and the problem of technology transfer to China.

However, the increasing assertiveness by the PLA and China’s increasingly forceful and at times aggressive diplomatic tactics in the Indo-Pacific, as well as its increasingly authoritarian turn at home, have heightened awareness in the alliance. The war in Ukraine made it clearer that the alliance will need to think carefully about how to balance its focus on maintaining security in the Euro-Atlantic region with any potential role in the Indo-Pacific. However, there is scope for the latter. Members should continue to improve information sharing and assessing Chinese investment in their economies, within the alliance as well as with partners in the Indo-Pacific region. Allies should build a stronger common approach to domestic Chinese challenges, such as in national critical infrastructure, keeping an innovative edge, and resilience needs to be addressed first to enable the alliance to ensure both political and military security. Doing so is not just in NATO’s internal interest but of benefit to its engagement with the Indo-Pacific region and to setting common standards with partners outside of the alliance, particularly in areas of defence-relevant disruptive technologies. There is scope for NATO to be a platform to engage with China, too, on areas of key interest, such as arms control. However, on this last point, expectations should be measured.

#### U.S. should use joint innovation within to check Chinese infilation and influence

Nietsche et al., CNAS Research Associate, ‘20

[Carisa Nietsche, Research Associate, CNAS Transatlantic Security Program, Jim Townsend, former Deputy Assistant Secretary fo Defense and Adjunct Senior Fellow, CNAS and Andrea Kendall-Taylor, Senior Fellow, CNAS, “Enlisting NATO to Address the China Challenge,” Center for a New American Security, 10—5—20, <https://www.cnas.org/publications/commentary/enlisting-nato-to-address-the-china-challenge>, accessed 4-22-22]

Maintain the U.S. and European military and competitive edge. NATO is an important vehicle for spurring joint innovation. The United States should work through NATO’s Defense Planning Process to identify allied military gaps that are vulnerable to being filled by purchases from China. To avoid this, NATO defense planners should develop allied innovation goals that can help alliance members find other ways to fill these gaps. NATO member states should prioritize jointly building at home future technologies that will underpin military capabilities, such as quantum computing, artificial intelligence, and 6G. Allies will need to begin developing AI technology and its regulations in concert to ensure that systems remain interoperable, and that China does not secure the upper hand in this pivotal technology.25

To maintain their competitive edge, allies will need to increase and protect U.S. and European joint innovation. The alliance should prioritize securing supply chains and ensuring procurement processes that prevent Chinese goods from inclusion in mission-critical tools. Further, NATO should participate in export control dialogues with EU member states to ensure that semiconductor manufacturing equipment and other foundational technologies are controlled multilaterally. As part of this effort, NATO should coordinate with the EU to establish baseline risk assessments for the adoption of critical technologies from Chinese providers, such as 5G, to ensure that risk mitigation strategies are developed and implemented with possible military use in mind.

# Resilience Aff: Solvency Extensions

## Solvency: Specific Mechanisms

### Solvency: Resilience—NATO-Industry Cooperation

#### NATO should facilitate cooperation between member states and private sector—key to cyberdefense

Lété and Dege, German Marshall Fund analysts, ‘17

[Bruno Lété, Senior Fellow for Security and Defense Policy, German Marshall Fund and Daiga Dege, Trainee, German Marshall Fund, “NATO Cybersecurity: A Roadmap to Resilience,” POLICY BRIEF n. 23, German Marshall Fund of the United States, 7—17, <https://www.gmfus.org/news/nato-cybersecurity-roadmap-resilience>, accessed 6-8-22]

NATO and Cyber Industry Cooperation

Cybersecurity is largely market-driven. Government intelligence capabilities increasingly find it hard to keep up with the requirements for combating the surge in cyber threats. NATO should play a crucial role in facilitating contacts between those member states that seek stronger links with the private sector and encourage the role that industry can play in cyber threat deterrence and intelligence sharing. Flagship initiatives, such as the NATO Industry Cyber Partnership, are important steps in that direction but there is still a need to build more access and trust between NATO governments and industry. Educating member states and partner nations about the role of the private sector in cybersecurity is key. To make the partnership with the industry more effective NATO could play a more important role in mapping and evaluating what kind of cyber defense technologies and intelligence gathering methods the private sector offers, share lessons learned with the member states and encourage capitals to integrate the best practices into capabilities, policy, and implementation planning. NATO can also play an essential role in improving communications and information sharing between the private and the public sectors. More can be done at the NATO level to identify what kind of information between governments and companies can or cannot be shared, to develop standardized methods and formats for information sharing, and to encourage the use of automated platform capabilities to share this information quickly.

#### NATO should bolster existing partnerships with the private sector to improve cyberdefense

Pernik & Jermalavičius, International Centre for Defence & Security analysts, ‘16

[Piret Pernik and Tomas Jermalavičius, Research Fellows, International Centre for Defense and Security “Resilience as Part of NATO’s Strategy: Deterrence by Denial and Cyber Defense,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. 110]

Cyber threats defy organizational borders, most critical infrastructure is operated by the private sector, and various non-state actors yield significant power, knowledge and expertise in cyberspace.As noted above, bolstering resilience can be achieved only through an integrated approach involving key stakeholders. NATO has engaged industry in its cyber defense activitiesthrough the NATO CyberIndustry Partnership. 26Technical agreements on information sharing and improving situational awareness have been concluded with cybersecurity companiessuch as Symantec, Cisco,Fortinet and others, and industry also participate in NATO exercises and trainings, as well as Smart Defense Projects. 27 The Alliance should continue leveraging its partnership with industry and provide grants to research community in order to conduct projects in target countries to help them to ensure cyber defense.

### Solvency: Resilience—NATO Information Sharing

#### Information sharing is necessary—strong members need to work with weaker ones

Hasanov et al., Azerbaijani War College of the Armed Forces analyst ‘19

[Arif Hasan Hasonov, Khayal Ibrahim Iskandarov and Sadi Saleh Sadiyev, analysts, War College of the Armed Forces, Republic of Azerbaijan, “The Evolution of NATO’s Cyber Security Policy and Future Prospects,” JOURNAL OF DEFENSE RESOURCES MANAGEMENT v. 10 n. 1 (18), 2019, p. 102-103]

Even though the cyber security is a part of NATO’s collective defense, there are some setbacks. According to Salih Bicakci, there are three main reasons of why NATO is still not sufficient on collective cyber security. The first reason is that the capacities of member states on cyber security are different. The second reason is that the threats on cyberspace frequently transform themselves, so adoption process is not easy for everyone. The third reason is that most of the threats come from the private sector, so it is not easy to communicate with the all private sectors in each member state.

According to Piret Pernik, the most important lack of NATO’s cyber security policy is the lack of sharing experiences. He argues that more advanced member states, having heavily invested into national cyber capabilities, hesitate sharing these with others for financial and security reasons [6].

As the cyber security expert, Jarno Limnell, has noted, the central barrier to greater cooperation and overall increased cyber capability for NATO has essentially been a certain lack of trust. More powerful allies don’t yet fully trust less capable ones with information and knowledge about their abilities and weaknesses and prefer to have bilateral or smaller-scale multilateral cooperation in the cyber defense domain [17].

### Solvency: Resilience—NATO Partner Cooperation

#### Resilience is the best framework within which to bolster NATO’s cyber capabilities—partnership actions are vital

Hasanov et al., Azerbaijani War College of the Armed Forces analyst ‘19

[Arif Hasan Hasonov, Khayal Ibrahim Iskandarov and Sadi Saleh Sadiyev, analysts, War College of the Armed Forces, Republic of Azerbaijan, “The Evolution of NATO’s Cyber Security Policy and Future Prospects,” JOURNAL OF DEFENSE RESOURCES MANAGEMENT v. 10 n. 1 (18), 2019, p. 103-104]

Without any doubt, the best avenue is to collectively battle cybercrime and to collaboratively reinforce NATO’s resilience to cyber-attacks. It underscores that, while NATO conducts business in cyber defense area, a continued emphasis on involving other actors (organizations, Allies, partner nations, private sectors) is essential. The cooperation with different actors to learn to work together, share information and fully grasp the rapid dynamics of cyber crises. It is critical for creating bonds between specialists of different countries, improving interoperability and practicing the intricacies of preventing malicious cyber threats. It in turn will build trust and strengthen bonds of NATO partnerships.

Prospective cooperation areas in cyber security are increasing interoperability, sharing strategic and technical information and threat assessments, coordinating responses to cyber crisis and engaging partners into NATO’s education, exercises and training activities. In order to to help develop national expertise NATO is helping member countries by sharing information and best practices, and conducting cyber defense exercises. Cyber defense is as much about people as it is about technology.

#### Working with NATO partners is critical to bolstering NATO’s defenses—collaboration is key

Hasanov et al., Azerbaijani War College of the Armed Forces analyst ‘19

[Arif Hasan Hasonov, Khayal Ibrahim Iskandarov and Sadi Saleh Sadiyev, analysts, War College of the Armed Forces, Republic of Azerbaijan, “The Evolution of NATO’s Cyber Security Policy and Future Prospects,” JOURNAL OF DEFENSE REOURCES MANAGEMENT v. 10 n. 1 (18), 2019, p. 104-105]

The ubiquity of cyber threats highlights the need to work together – a key issue when reviewing NATO’s role. It came to the fore as a result of the cyberattacks plotted against both NATO and partner nations. The cooperation between like-minded states and international organizations is the best way to address many cyber risks. NATO has the capabilities to offer a clear platform for exchanging practice between Allies and partners through a more extensive variety means, including NATO’s Defense Planning Process.

Such mechanisms might include operational and technical support and advice regarding cyberdefense capability development and implementation. It might entail advice on the establishment of a cyber-security strategy or brokering the exchange of lessons learned and situational awareness on cyber domain.

Even though the cyber-attacks are unlikely to be as lethal as strategic bombs for the foreseeable future, NATO has to brace itself for much more complicated predicaments regarding cyber threats emanating from its rivals. It will take a lot of effort and further bold decisions to move closer towards achieving the goal on thwarting cyber threats before they have important physical ramifications.

If virtual space becomes an inherent part of the NATO operations and exercises it will help the Alliance to adapt to emerging technological challenges. It in turn will necessitate to bridge the gap between Allies. Together with its member states NATO has to facilitate partner nations’ cyber defense capability development and participation in the annual trainings and exercises based on reciprocal interests, shared values and common approaches. There is not any obstacle for partners to cooperate at a technical level. NATO might establish individually-tailored projects in accordance with interests and capacities of partners to enhance their cyber security.

Only when the Allies and trusted partners collectively pursue a cyber-policy, they will be able to successfully prepare themselves for cyber threats to their national security. Even though the cyber defense is a part of collective security, NATO still lacks a stringent deterrence against cyberattacks. A stringent deterrence means that a state should have an offensive capability if it is attacked. Thus NATO has to prove that it is not only aware of the gravity of the cyber threat but also ready to defend against it.

#### Cooperation is important to effective cyberdefenses

Hasanov et al., Azerbaijani War College of the Armed Forces analyst ‘19

[Arif Hasan Hasonov, Khayal Ibrahim Iskandarov and Sadi Saleh Sadiyev, analysts, War College of the Armed Forces, Republic of Azerbaijan, “The Evolution of NATO’s Cyber Security Policy and Future Prospects,” JOURNAL OF DEFENSE RESOURCES MANAGEMENT v. 10 n. 1 (18), 2019, p. 102]

In cyber conflict, the terrestrial distance between adversaries can be irrelevant because everyone is a next-door neighbour in cyberspace. And of course it necessitate cooperating internationally. As Jamie Shea, NATO deputy assistant secretary general for emerging security challenges mentioned: NATO has agreed a series of actions that can be taken in the form of assistance to allies, he said, including training, education, exercises, malware intelligence sharing, early warning, and incident response. The third key element of the enhanced NATO cyber defense policy is multi-national cooperation in cyber defense, which includes the concept of “smart defense” through pooling and sharing capabilities. This means that all future NATO military exercises will involve a cyber-component and look at the challenges of running military operations in a degraded cyber operating environment [16].

#### NATO should adopt a forward resilience strategy—partner capabilities are critical to reliance stability

Hamilton, Johns Hopkins Professor, ‘16

[Daniel S. Hamilton, Austrian Marshall Plan Foundation Professor and Executive Director of the Center for Transatlantic Relations at Johns Hopkins University’s School of Advanced International Studies, “Going beyond Static Understandings: Resilience Must Be Shared, and It Must Be Projected Forward,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. 51]

Project Resilience Forward

NATO members share a keen interest in the societal resilience of other countries beyond the EU and NATO, particularly in wider Europe, since strong efforts in one country may mean little if neighboring countries, with which they share considerable interdependencies, are weak. Russia’s hybrid efforts to subvert Ukrainian authority are but the latest examples of this growing security challenge. Allies should be proactive about sharing societal resilience strategies, not only with allies but with selected partners.

Through a strategy of “forward resilience,”NATO allies and EU memberstates would identify—very publicly—their resiliency with that of others beyond the EU and NATO, and share societal resilience approaches and operational procedures with partners to improve societal resilience to corruption, psychological, and information warfare, and intentional or natural disruptions to cyber, financial, and energy networks and other critical infrastructures,with a strong focus on prevention but also response. Forward resilience would also enhance joint capacity to defend against threats to interconnected domestic economies and societies and resist Russian efforts to exploit weaknesses of these societies to disrupt and keep them under its influence.

The EU and its memberstates, and NATO and its allies, should facilitate joint or complementary efforts to project “forward resilience” toE U Eastern Partnership or NATO Partnership countries in areas such as security sector reform, police and gendarmerie training, public health-biosecurity measures, civilian control of the military, or economic reconstruction. In thisregard,the EU and its memberstates, and NATO and its allies,should consider deploying coordinated Forward Resilience Support Teams, at the invitation ofEU Eastern Partnership or NATO Partnership countries, to support building resilient capacity in areas ranging from critical infrastructure protection and strategic communications,to disaster prevention, management, and relief, to civil-military cooperation.

#### NATO should step up its resilience capabilities—can play an important support role

Hamilton, Johns Hopkins Professor, ‘16

[Daniel S. Hamilton, Austrian Marshall Plan Foundation Professor and Executive Director of the Center for Transatlantic Relations at Johns Hopkins University’s School of Advanced International Studies, “Going beyond Static Understandings: Resilience Must Be Shared, and It Must Be Projected Forward,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. 40-41]

NATO’s Role

While resilience requires a broad approach with significant civilian political and economic aspects, it also has major military components. NATO military forces, even in small number, can be effective to back up local border forces or special operations forces to detect and neutralize foreign insurgents. National forces should be primary, in keeping with Article 3 of the Washington Treaty. But NATO allies can assist where requested, for example, for protection of key industrial, commercial, and transportation nodes (especially those intended for use in reception of reinforcements), counter insurgency operations and para-military police functions,responses to civil emergencies and covert operations, and crisis response management.

NATO and its members already possess noteworthy capabilitie sin these areas, but their ability to act as a fully organized, capable alliance is not well-developed. NATO will need improved physical assets, strengthened strategic planning and operating capacities. It will need to coordinate closely with national governments, many of which view control of societal security resources as vital manifestations of their sovereignty, and have diverse constitutional approaches to domestic uses of their military and to civil-military cooperation in crisis situations.

Moreover,NATO engagement in this area will require a fundamentally different relationship with the EU, which has undertaken a range of activities and initiatives aimed at improving its military and civilian capabilities and structures to respond to crises spanning both societal defense and societalsecurity,including cross-border cooperation on consequence management after natural and manmade disasters.

In short, resilience is a job for NATO, but it is not a job for NATO alone. In many instances it may require national or EU authorities to play a lead role. The issue for NATO is not just what it should do, but how it fits within an array of necessary Western efforts to bolster transatlantic resilience. In such instances, NATO may play a support role. Hybrid challenges, for instance, may include but are not limited to military elements and must be addressed in more comprehensive ways. 4

#### Partnership coop effective if it focuses on capabilities and interoperability

Pernik & Jermalavičius, International Centre for Defence & Security analysts, ‘16

[Piret Pernik and Tomas Jermalavičius, Research Fellows, International Centre for Defense and Security “Resilience as Part of NATO’s Strategy: Deterrence by Denial and Cyber Defense,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. 107]

To further enhance its assistance to partner countries NATO should identify, via cooperation with the research community and recipient countries, individual cyber defense needs in the areas of material and nonmaterial resources, knowledge, expertise, and information sharing. The first area where NATO should consolidate more efforts is increasing interoperability of partners’ cyber defense capabilities, communication and information systems and networks, as well asinformation and threat assessment exchange protocols. Allied Command Transformation maintains that interoperability of communication and information systems upon which NATO’s command structure dependsis a key elementin developing forward presence. 17

#### NATO should cooperate with partners on threat assessment capabilities

Pernik & Jermalavičius, International Centre for Defence & Security analysts, ‘16

[Piret Pernik and Tomas Jermalavičius, Research Fellows, International Centre for Defense and Security “Resilience as Part of NATO’s Strategy: Deterrence by Denial and Cyber Defense,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. 108]

Sensitivity related to offensive cyber capabilities and fear of disclosing one’s own vulnerabilities have been obstacles in fostering trust that is fundamental for cooperation, and especially information and intelligence sharing. NATO should work closely with partners to expand mutual information and threat assessment sharing, a critical aspect of defending against hybrid and cyber threats. NATO and EU agreed at the Warsaw Summit to share information and—to the extent possible—intelligence between staffs, cooperate on strategic communication, and expand existing cooperation on cyber security and defense, including operations, exercises and training.The EU has a wide toolbox ofstrategies, policies, procedures and technical measures to support non-military aspects of cyber security in member states and partner countries.

### Solvency: Resilience—NATO Standards

#### NATO needs to create standards and support partner cyber response efforts

Lété and Dege, German Marshall Fund analysts, ‘17

[Bruno Lété, Senior Fellow for Security and Defense Policy, German Marshall Fund and Daiga Dege, Trainee, German Marshall Fund, “NATO Cybersecurity: A Roadmap to Resilience,” POLICY BRIEF n. 23, German Marshall Fund of the United States, 7—17, <https://www.gmfus.org/news/nato-cybersecurity-roadmap-resilience>, accessed 6-8-22]

More Tools to Coordinate National Efforts

The core of NATO cybersecurity efforts lie at the member-state level. NATO is responsible for protecting its own institutional information and communication systems, but it has little say in coordinating how member states develop their national cyber defense capabilities. Despite having signed the Cyber Defense Pledge at the Warsaw NATO Summit, many member states still struggle to implement and evaluate their national cyber-security plans. As a result NATO’s efforts at developing uniform, alliance-wide cybersecurity are undermined by significant inconsistencies across the national level of the member states and NATO’s collective security and deterrence in cyberspace still show serious vulnerabilities against the backdrop of a growing number of attacks.

For NATO to operationalize cyberspace as a domain of NATO defense policy and planning — as was agreed at the NATO Warsaw Summit — the Alliance should have authorizations from member states to do more than just provide advice, expertise, training, or education. Similar to how NATO coordinates Allied military forces in the conventional domain, NATO could also be asked to evaluate how member states can develop, synergize, and complement their mutual national cyber defenses. At a minimum, NATO should develop standards and better indicators that allow a standardized measurement of a nation’s annual progress — and should be tasked with testing and measuring members’ capabilities annually. To achieve this objective, a strong cooperation with the European Union is essential. NATO and the EU could work together to design minimum cybersecurity requirements and benchmarks that would also be adopted by the European Defense Agency.

### Solvency: Resilience—NATO Support

#### NATO can build resilience by engaging with civilian organizations and national governments

Kramp-Karrenbauer, German Defence Minister, ‘20

[Annegret Kramp-Karrenbauer, German Defence Minister, “How to Keep Nato Fit for Purpose in Years to Come,” FINANCIAL TIMES, 5—10—20, <https://www.ft.com/content/bb4b2b34-8faa-11ea-9b25-c36e3584cda8>, accessed 5-17-22]

Third, Nato needs to get better at combating less traditional security challenges. This pandemic is one of many diverse threats to national security, from terrorism and cyber attacks to disinformation campaigns and the effects of climate change.

None can be deterred by tanks and missiles. In fact, the best defence is to strengthen our ability to absorb such blows and continue to tackle their causes. That means we must improve our resilience — for example by strengthening and adjusting our critical infrastructure, be that energy grids, roads and railways, or computer networks and healthcare systems. While this is primarily a task for national governments, Nato should play a strong supporting role, building resilience into its own structures, forces and operations and adding military and organisational expertise to national efforts.

Nato has been working on all this — from the Cyber Defence Centre of Excellence in Estonia, to the management of emergency relief through the Euro-Atlantic Disaster Response Coordination Centre.

“Resilience” should become the alliance’s watchword, high on its list of priorities. To build such resilience, Nato needs to engage more regularly and systematically with civilian organisations, from police forces to disaster relief agencies, to experts in medicine, climate and cyber security.

The alliance has just established a reflection group,chaired by American and German leaders. I am confident that this group will aid Nato’s strategic development, developing fresh ideas on how to achieve greater security for all transatlantic allies.

My country is doing its share — in cash, capabilities, and commitments, with another significant increase in 2020. After all, West Germany joined Nato 65 years ago last week. Accession to the alliance meant the return to western civilisation, a mere 10 years after the end of the second world war. It allowed for German reunification and a united Europe a few decades later.

Today, Nato continues to keep our homeland safe, projects stability and provides immediate relief from unforeseen disasters such as this pandemic. Building on this proud tradition of safeguarding freedom and security for all states, the 30 sovereign members must take the next step in creating a more resilient alliance.

#### Resilience measures can strengthen the alliance—should focus on supporting development of national and partner capabilities

Pernik & Jermalavičius, International Centre for Defence & Security analysts, ‘16

[Piret Pernik and Tomas Jermalavičius, Research Fellows, International Centre for Defense and Security “Resilience as Part of NATO’s Strategy: Deterrence by Denial and Cyber Defense,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. 110-112]

Recommendations

• The Alliance should develop and continuously maintain a comprehensive picture of the vulnerabilities of allies and partners to ‘hybrid warfare’ scenarios and tailor its resilience-building assistance measures to the needs of particular nations. However, it should remain cognisant that national resilience is the responsibility of the national governments.

• The Alliance should establish a comprehensive system of national resilience indicators (ResilienceMonitor/Index), covering all relevant domains,to monitor and assess the overall state of resilience in individual nations.This would provide a basis for more focused and specific measures—at the national and NATO levels—to address the short, medium and long-term needs.

• Although NATO is paying most attention to infrastructure,networks and civil preparedness, it should also include societal resilience into its monitoring, assessment and support measures.This is particularly important from the perspective of maintaining the Alliance’s credibility, cohesion, unity and public support to its mission.

• Much more effort has to be dedicated by NATO and the EU to studying and understanding what deters Moscow, how it assesses vulnerabilities of target countries and how it seeks to exploit those vulnerabilities to its strategic ends. This has to be linked with early warning and strategic anticipation efforts.

• NATO should establish individually-tailored projects and expand existing projects in accordance with interests and capacities of partners to enhance their cyber security and defense. Prospective cooperation areas in cyber defense include increasing interoperability, sharing strategic and technical information and threat assessments, coordinating responses to cyber crisis, and engaging partners into NATO’s education, exercises and training activities.

• NATO should consider establishing special cyber support teams that can be deployed to partner countries with the aim to increase interoperability, improve information sharing and coordinate crisis response.

• To support NATO Allies’ resilience in the cyber security context cyber experts should be included into NATO Force Integration Units (NFIU). This would help assess vulnerabilities, increase preparedness and interoperability in regards with crisis response.

• To support projecting resilience in NATO partner nations NATO and the EU should first assess the levels of the existing maturity of cyber security and defense capacity in the target countries. They should coordinate and synchronize mutual training and assistance projectsin orderto avoid overlapping.Partnership Review and Planning Process (PARP) should include as part of broader resilience also cyber defense elements, and planning should to be aligned with the NATO Defense Planning Process (NDPP).

• Partners would benefit from the development of minimal requirementsforthe protection oftheir critical infrastructure and in regards with cyber defense.

• NATO allies should develop a clear political guidance concerning which activities will be open for different partners, taking into consideration willingness of an individual partner to cooperate with the Alliance, as well as their maturity level. Some partners should be engaged into partnerships with industry and into various NATO’s education and training efforts (cyber defense courses, cyber ranges, cyber hygiene platforms, etc.). Some parters should be engaged in planning phases of crisis management and cyber defense exercises. Engagement in these activities and in the Federated Mission Networking should be widened beyond the current range of seven partners.

• While common funding of partnership activities and the establishment of trust remains challenging along with management difficulties of common endeavors, NATO could facilitate a lead/framework nation approach that would contribute to the setting up of specific trustfunds and tailored training projects .A lead nation could promote specific projects,task and working groups where other nations could plug in.

• In addition to providing technical cyber defense training, consulting partner nations on how to develop their national cyber security and defense programmes, policies and strategies would contribute to the development of common terminology and increase partners’ understanding of cyber threats, as well as promote adherence to fundamental democratic values in cyberspace activities.

#### Resilience is key to the alliance—NATO should step up its support efforts

Hamilton, Johns Hopkins Professor, ‘16

[Daniel S. Hamilton, Austrian Marshall Plan Foundation Professor and Executive Director of the Center for Transatlantic Relations at Johns Hopkins University’s School of Advanced International Studies, “Going beyond Static Understandings: Resilience Must Be Shared, and It Must Be Projected Forward,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. 41-44]

At the July 2016 Warsaw Summit, NATO allies agreed to set resilience standards and each made a pledge to bolster its own national resilience under Article 3 of the North Atlantic Treaty, according to which allies commit to “maintain and develop their individual and collective capacity to resist armed attack.’’ This is an important step. But more will need to be done.

Make resilience an integral element of NATO’s core tasks, or consider making resilience a fourth core task. A key element of Russia’s strategy isthe use ofstrategic surprise and hybrid threatsto take advantage of weak states. Extremist threats from the south also challenge the fabric of Western societies. Greater societal and defense resilience can be an important component of an effective response. Creating a higher degree of resilience in vulnerable societies makes it more difficult for state or non-state actors alike to disrupt and create the instability they need for their success. Societies deemed indefensible in traditional defense terms can be rendered indigestible through resilience. Resilience has become integral to each of NATO’s current core tasks of collective defense, cooperative security, and crisis management.Initial activities could include the following:

• Develop civil-military Resilience Support Teams, small operational unitsthat could offersupport to NATO member national authorities in such areas of emergency preparedness including assessments; intelligence sharing,support and analysis; border control; assistance to police and military in incident management including containing riots and other domestic disturbances; helping effectuate cross-border arrangements with other NATO members; providing protection for key critical infrastructures including energy; and, in the cyber arena,support and enhancement of NATO’s Cyber Response Team. NATO is moving forward with such Advisory Support Teams. It should consider that these NATO teams could work in parallel with similar EU groups using the same playbook. In certain countries, Resilience Support Teams could be collocated with NATO Force Integration Units, and help national responses with NATO military activities including especially special operations activities. 5

• Create “National Resilience Working Groups.” Encourage relevant nations to establish working group-type secretariats to coordinate defense activities with overlapping civil authority and private sector key critical infrastructure functions to enhance national capacity to anticipate, prevent, respond and recover from disruptive scenarios and to provide a key point of contact for outside assistance,including NATO Resilience Support Teams in the east, focused on the development of resilience and response to hybrid threats; in the south, focused on resilience and humanitarian requirements; and throughout the Alliance, focused on cyber and particularly its support to the electric grid and finance. Such a group should also have continuous situational awareness of a state’s hybrid risk assessment. Coordina tion,integration, and exercises at the national level will make outside support from NATO and other organizations most useful.

• Encourage the establishment of regional working groups. In addition to national working groups, concerned nations could establish working groups with overlapping issues—one approach would be to look to the nations in the framework arrangements for the east and for the south—with invitations later for others to join as they deem desirable. This would be somewhat similar to such regional mechanisms as Nordic Defense Cooperation (NORDEFCO) or the Southeast European Defense Ministerial.

• Include resilience events in NATO exercises, training, education and operational planning. Resilience events should be included especially in NATO Crisis ManagementExercises(CMX) and cyber exercises such as the annual cyber coalition exercises.

Bolster coordination with the private sector. Effective resilience requires engagement by the private sector,which owns mostinfrastructures critical to essentialsocietal functions.A good firststep would be to develop mechanisms to coordinate with private institutions and entities on key security issues focused on the development of resilience, with cyber as the initial arena.

Enhance counterterrorism cooperation. Counterterrorism within the NATO region remains primarily the responsibility of national intelligence,interior, and police authorities.NATO’s counterterrorism activities since 2001 have consisted primarily of safeguarding allied airspace and maritime approaches and intelligence sharing,i.e.,guarding the approaches to NATO territory. NATO should consider options for expanding intelligence sharing and its capabilities to support the protection of critical infrastructure, especially infrastructure essential to the performance of NATO core tasks. This should include the development of procedures and plans to ensure the prompt deployment of special operations forces— useful in disrupting some kinds of terrorist attacks—if national authorities ask NATO for this type of assistance. NATO should apply its plans for securing pipelines, offshore oil platforms, and ports to insure energy suppliesin wartime to the challenge of anti-terrorist protection ofsuch critical infrastructure.

Develop a more robust strategic communications strategy to address Russia’sinformation operations, particularly where Moscow seeks to exploit social and political differences in allied states, including those with sizable ethnic Russian or Russian-speaking populations.

### Solvency: Resilience—NATO Tech Development

#### NATO cyber tech development bolsters deterrence

Magula, Army strategist and Alvarez-Couciero, SAIS graduate, ’21

[Justin Magula, Army Strategist, Strategic Landpower and Futures Group, U.S. Army ar College and Paula Alvarez-Couceiro, gradaute, SAIS, Johns Hopkins University, “Maintaining and Improving NATO’s Technological Edge,” Wavell Room, 9—30—21, <https://web.archive.org/web/20210930061529/https://wavellroom.com/2021/09/30/maintaining-improving-natos-technological-edge-technology/>, accessed 4-9-22]

Harnessing and Countering Emerging Disruptive Technologies

While emerging and disruptive technologies (EDTs) touch all aspects of life and present exciting opportunities for the alliance, they also present threats. Many of NATO’s adversaries use EDTs against alliance personnel and infrastructure, such as recent cyberattacks targeting Polish politicians and the Colonial Pipeline. Enhancing its innovation processes will allow NATO to improve its military technology across all domains and boost its deterrence and defense capabilities. NATO could then better deter Russian and Chinese hybrid threats in cyber, space, electronic warfare, and information domains. For instance, NATO can use its forthcoming Cyber Command to take collective action and demonstrate cyberspace thresholds that will result in unified offensive cyber or conventional responses if crossed by its adversaries. By strengthening its cyber abilities and adding new capabilities, NATO can deter adversaries in the information space and take the offensive against them. NATO would then rob Russia and China of success in areas where they currently excel, and better protect the alliance’s people and infrastructure.

### Solvency: Resilience—NATO Threat Assessment

#### NATO should focus on improving risk assessment and response capabilities

Lété and Dege, German Marshall Fund analysts, ‘17

[Bruno Lété, Senior Fellow for Security and Defense Policy, German Marshall Fund and Daiga Dege, Trainee, German Marshall Fund, “NATO Cybersecurity: A Roadmap to Resilience,” POLICY BRIEF n. 23, German Marshall Fund of the United States, 7—17, <https://www.gmfus.org/news/nato-cybersecurity-roadmap-resilience>, accessed 6-8-22]

Rapid Assessment and Decision-Making Tools

The scale, speed, and intensity of today’s cyber-attacks demand a new approach to respond at the political, military, and civilian level. To develop a rapid decision-making process when facing a cyber-attack NATO can take a few effective measures across its organization. First, more resources must be allocated to accurately and quickly detect and define hostile cyber actions. Further work on indications, warnings, and situational awareness is critical. In this context, NATO’s various civil and military intelligence units, inter alia, could have a useful role. In addition, the Supreme Allied Commander Europe (SACEUR) could be granted more powers by the North Atlantic Council in authorizing some of the preparatory procedures. At the same time, NATO headquarters should increase the number of exercises that test rapid decisions-making procedures in complex and demanding cyber crisis-conflict scenarios.

Much can also be done at the member-state level. Allies and willing partners should continue to work on improving and updating threat assessments, and facilitating closer intelligence cooperation. In this light, Allies should identify information sharing as a clear requirement and task.

NATO could also intensify its interaction with national intelligence services and establish supply chain management partnerships with national industries. Cyber threats come in the form of networks and it takes a similarly well-organized network of international and cross-sector cooperation to defeat those threats.

### Solvency: Resilience—NDPP / Consultation

#### [x] There is capital for resilience improvements now—should focus on resilience within the context of deterrence (by denial) through consultative policies

Hall & Sandeman, London School of Economics researchers, ‘22

[Jonny Hall, PhD Candidate, International Relations, London School of Economics and Political Science and Hugh Sandeman, Visiting Senior Fellow, LSE Ideas and Project Head of Global Strategies, “NATO’s Resilience: The First and Last Line of Defence,” Strategic Update, LSE IDEAS, 5—22, London School of Economics p. 11-13]

Policy Recommendations

NATO could resolve the tension between its collective responsibility for resilience and the continuing national responsibility among member states for implementing resilience measures by addressing resilience in the framework of deterrence and defence.

This aligns with the concept of deterrence used in the 2019 NATO Military Strategy and the 2020 Concept for the Deterrence and Defence of the Euro-Atlantic Area, which focuses less on crisis response and more on how deterrence can be used in persistent competition.33 The growing use of hostile measures short of war—which prompted the search for more sustained and wider resilience after 2014—has increased the importance of deterrence by denial.

Considering resilience within the context of deterrence will establish the overarching logic of NATO’s engagement with resilience issues and encourage the practicalities of moving towards “collective resilience”. As a form of deterrence, resilience policies will need to meet the three key criteria of all forms of deterrence: commitment, capability and communication.34

Commitment to strengthening resilience, already significantly enhanced among member states after the Russian invasion of Crimea, will be greatly strengthened by the war in Ukraine. It will be important for NATO and its members to take advantage of the political capital created by these developments and the COVID-19 pandemic in enacting costly resilience measures. NATO should therefore focus on four aspects of resilience rather than the broader seven baseline requirements. These are: continuity in energy and essential supplies; the security of the digital realm to ensure key socioeconomic functions; maintaining the independence of critical technologies beyond the control of adversaries; and the ability to detect and dispel disinformation.

In terms of capability, NATO should adopt a practical approach to helping the process of strengthening alliancewide resilience. Rather than trying to “establish, assess, review and monitor broad resilience objectives to guide nationally-developed resilience goals”, NATO should start the other way round. A similar approach to the NDPP, which consults with allies about their military plans, could be taken to encourage the harmonisation of member state and NATO objectives concerning resilience.

The NDPP identifies shortfalls in NATO capabilities before setting, assisting and reviewing the efforts of individual members to achieve country-specific targets aimed at resolving weaknesses and strengthening NATO’s defensive posture.35 As a process tailored for each member, “capability targets” are produced for each member according to the “political principles of fair burden-sharing”.36 Though this expectedly produces political tensions surrounding the issue of what is “fair”, it represents a more nuanced and realistic approach than the adoption of organisation-wide requirements. As argued above, it would still be advisable for NATO to set relatively few, clearly understandable goals that allow for the positive effects of peer competition, much like the success of the Defence Investment Pledge of 2014 in which members committed to spend at least 2 percent of Gross Domestic Product on defence and 20 percent of defence spending on major new equipment within a decade.37 Resisting the temptation to set numerous goals also helps bring clarity and focus to avoid potential gaps between rhetorical commitments and policy fulfilment.

Lastly, communication with both internal and external audiences will be essential to fostering resilience within NATO. The ability to demonstrate resilience to external audiences can serve as an effective deterrent against aggressive action. As with NATO’s annual military deterrence exercise,38 comprehensive preparation and regular exercises can play an important role in resilience measures by enhancing deterrence by denial. Exercises can get messages across to allies and domestic audiences.39 Societal and psychological resilience is also an essential complement to developing physical resilience capabilities. This was exemplified in 2018 by NATO partner Sweden’s delivery of a brochure to every household titled “If War or Crisis Comes”, which offered advice on what to do in events of power shortages or loss of internet access.40 The leaflet stated that “everyone who lives in Sweden shares a collective responsibility for our country’s security and safety”.41

One avenue for building societal resilience that could be explored by NATO members is working with creative industries to put across the need—and help create a narrative—for preparation for crisis events. Following precedents from the Cold War, in 2019 the French military employed science fiction writers to assist in conceptualising potential threats to national security.42 The same logic could be applied to getting the public to think about unfamiliar scenarios that may emerge in the contemporary and future security environment.

#### Best way to improve resilience is to house it in deterrence logics and work through NDPP-style consultative processes

Hall & Sandeman, London School of Economics researchers, ‘22

[Jonny Hall, PhD Candidate, International Relations, London School of Economics and Political Science and Hugh Sandeman, Visiting Senior Fellow, LSE Ideas and Project Head of Global Strategies, “NATO’s Resilience: The First and Last Line of Defence,” Strategic Update, LSE IDEAS, 5—22, London School of Economics p. 6-7]

This Strategic Update makes two proposals towards ensuring that attempts to strengthen resilience within NATO deliver practical results.

First, locating the effort to improve resilience firmly in the context of NATO’s new approach to deterrence can resolve the tension between long-established requirements for resilience in meeting armed attack and the newer, broader requirements for resilience against hostile acts below the threshold of war. This should help to maintain the focus on reducing vulnerabilities and threats to security, ensuring that NATO’s forces can operate effectively in varying states of peace, crisis and conflict.

Second, by adopting and improving a consultative approach to resilience that is similar to the NATO Defence Planning Process (NDPP), NATO can avoid applying a bureaucratic and probably unproductive checklist for evaluating progress in the national resilience of member states. This would involve agreeing what each state individually should set as its resilience priorities, with the collective resilience of the whole alliance as a parallel objective.

These recommendations are reached in three steps: answering the question of what resilience is; analysing NATO’s evolving role in issues of national resilience among its members; and outlining the political challenge of setting and meeting resilience objectives.

### Solvency: Resilience—Strategic Concept Incorporation

#### Resilience needs to be a focus of the new Strategic Concept

Binnendijk, Atlantic Council & Hamilton, Woodrow Wilson Center, ‘20

[Hans Binnendijk, Distinguished Fellow, Atlantic Council and Daniel S. Hamilton, Director, Global Europe Program, Woodrow Wilson Center, “Four Factors to Consider in Keeping NATO Relevant,” DEFENSE NEWS, 11—24—20, <https://www.defensenews.com/opinion/commentary/2020/11/24/four-factors-to-consider-in-keeping-nato-relevant/>, accessed 5-22-22]

Second, the alliance needs to continue its efforts to strengthen its capabilities in two distinct areas: conventional military might and resilience against so-called hybrid or non-kinetic attacks.

Since the Russian annexation of Crimea in 2014, NATO nations have begun to focus again on a major power competitor. Four NATO battlegroups are forward-deployed to the Baltic states and Poland. A small, very high-readiness force and a larger readiness initiative were undertaken to back up those battalions. A mobilization initiative was designed to make sure ready forces can forward-deploy quickly. But European defense budgets constrained by COVID-19 will put those initiatives in jeopardy. The Strategic Concept will need to prioritize those programs.

The alliance must also more methodically address unconventional challenges to human security from Russia such as media disinformation, corrosive cyber operations, supply chain disruptions and energy intimidation. The Strategic Concept needs to design resilience programs so that alliance members can better protect the critical functions of our societies to such disruptive dangers.

### Solvency: Resilience—U.S. Support / Push

#### The U.S. should push resilience measures—can do so through NDPP standards and other means

Kramer et al., Scowcroft Center Distinguished Fellow, ‘20

[Franklin D. Kramer, Distinguished Fellow, Scowcroft Center for Strategy and Security and Board Director, the Atlantic Council, Lauren Speranza, Director, Transatlantic Defense and Security, Center for European Policy Analysis, and Conor Rodihan, Assistant Director, Transatlantic Security Initiative, Scowcroft Center for Strategy and Security, “NATO Needs Continuous Responses in Cyberspace,” NEW ATLANTICIST, The Atlantic Council, 12—9—20, <https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/>, accessed 5-23-22]

President-elect Biden and his team have pledged to renew US leadership in cooperation with Allies and partners. That agenda should start at NATO, and a key focus should be on cybersecurity. In early NATO meetings, the Biden administration should champion a cybersecurity continuous-response campaign, built around three key actions.

First, NATO should require the development and implementation of resilient cybersecurity architectures for itself, its members’ forces, and its key critical infrastructures. A resilient cybersecurity architecture involves an integrated set of capabilities that work as a system to reduce the disruptive effects of cyber adversaries. Key elements of a resilient architecture should include use of private sector cloud technology; zero-trust architecture for effective access management; development of secure hardware capabilities; and machine-learning and artificial-intelligence-augmented cyber defenses. This architecture also needs to be flexible to incorporate emerging technologies as they are developed.

NATO itself cannot develop such architectures. It can, however, underscore their necessity and require its members to do so, using the NATO Defense Planning Process (NDPP), acquisition procedures, standards and targets, and innovation from Allied Command Transformation to support a comprehensive research and development effort. In establishing requirements for these resilient architectures, NATO must recognize that one size will not fit all. Not only will requirements differ among military, government, and critical infrastructures operators, but, as has been shown in the development of autonomous vehicles and space capabilities, there are a variety of different approaches that may prove effective. In fact, having diversity within these capabilities will increase resilience by complicating adversaries’ abilities to infiltrate and attack them.

### Solvency: Resilience—S: A2 “Attribution”

#### Attribution is getting easier and anonymous attacks are ineffective

Davis, STC General Rapporteur, ‘19

[Susan Davis, General Rapporteur, STC, “NATO in the Cyber Age: Strengthening Secuirty & Defence, Stabilising Deterrence,” Science and Technology Committee (STC), NATO Parlilamentary Assembly, 8—13—19, p. 3]

15. However, in recent years, governments, private companies, and research organisations have increased their ability to attribute attacks at higher levels of confidence. Forensic tools have improved, and private and state analysts have built up databases and characteristic patterns for known intruders. On a technical level, truly harmful cyber attacks are very complicated and involve many moving pieces. Thus, the more complicated the cyber attack, the more likely that the attacker will commit mistakes along the way, enabling a forensics expert to trace the origin of the attack (Lindsay, 2015). Indeed, governments within the Alliance and beyond are increasingly attributing malicious cyber incidents to states and their proxies. Such transparency on cyber incidents is increasingly collective, coordinated in policy and time, and independent of the scale, nature, or impact of the incident (Giles and Hartmann, 2019). The Rapporteur supports this emerging policy of naming and shaming perpetrators and encourages further conversations at the NATO level.

16. Even if states and their proxies could be confident they will remain anonymous, truly convincing strategic rationales for large-scale surprise attacks are lacking. Anonymous cyber attacks are not well-suited for coercion, for example. Coercion only works if the attacked knows whom to yield or make concessions to. As one analyst points out succinctly, “[p]urely anonymous coercion is almost impossible because communicating and understanding the power to hurt implies that there is someone doing the hurting and a target concerned about avoiding getting hurt” (Lindsay, 2015). As a result, if an opponent wishes to coerce through cyber attacks, he cannot hide himself. This would defeat the purpose. How can the victim give in to demands if he does not know who the attacker is? (In contrast, cyber criminals want to stay anonymous when they, for example, attempt to extort money from victims.)

#### Cooperation bolsters attribution abilities

Alatalu, NATO Cooperative Cyber Defense Centre of Excellence staff, ‘18

[Siim Alatalu, Cyber Strategy and Policy Research and Traning lead, NATO Cooperative Cyber Defence Centre of Excellence, “NATO’s Responses to Cyberattacks,” HACKS, LEAKS AND DISRUPTIONS: RUSSIAN CYBER STRATEGIES, Chaillot Papers, ed. N.Popescu & S.Secrieru, 10—18, p. 102]

Thirdly, NATO’s particular advantage in cyber defence could stem from cooperation with its partner countries and with other international organisations, especially the European Union. Neither the Alliance nor the Union is an island on its own when it comes to cyber threats and vulnerabilities. The EU can do a lot in areas that are relevant for NATO, such as cybersecurity certification of devices imported into and used in European markets. Dependence on non-EU and non-NATO software could become a critical national security concern, as illustrated by for instance the Kaspersky case in the US.24 As highlighted by the recent attributions, there could be a global will for cooperation between NATO and non-NATO countries as any of them could become a target, as well as a bridgehead for further spreads of malicious cyber activities, as demonstrated by the WannaCry and NotPetya attacks.

## Solvency: Multi-Prong / Author Proposals

### Solvency: Resilience—Blessing Recommendations

#### [x] NATO needs to incorporate a resilience (safe-to-fail) strategy—necessary to check cyber threats, address limits of retaliation and protection strategies

Blessing, American Enterprise Institute fellow, ‘22

[Jason Blessing, Visting Research Fellow, American Enterprise Institute and PhD, Political Science, Syracuse University, “Fail-Deadly, Fail-Safe, and Safe-to-Fail: The Strategic Necessity of Resilience in the Cyber Domain,” NATO 2030: TOWARDS A NEW STRATEGIC CONCEPT AND BEYOND, Ed. J.Blessing, K.KjellstromElgin, N.M.Ewers-Peters, School of Advanced International Studies, Johns Hopkins University, 2022, p. 261-264]

The last several years have seen calls for NATO to embrace strategic resilience, and the COVID-19 pandemic has both amplified and accelerated debates surrounding resilience. One recommendation that has emerged is that NATO should adopt “comprehensive resilience” as a fourth core task alongside the three existing tasks of collective defense, crisis management, and cooperative security laid out in the 2010 Strategic Concept. Resilience has generally referred to the ability to “anticipate, prevent, and…protect against and bounce forward from disruptions to restore critical functions.”1 Comprehensive resilience is thus meant to address a range of challenges facing the Alliance and is necessarily a shared endeavor that can be projected forward outside the membership bounds of NATO.2 This chapter addresses one dimension of comprehensive resilience by highlighting the Alliance’s cybersecurity challenges and the strategic necessity of resilience in the cyber domain.

The COVID-19 pandemic has highlighted that cybersecurity encompasses more than “cyber war”3 by underscoring the reliance of nations and their economies on cyberspace and digital infrastructures. Massive migrations to online services have occurred with the transition to remote telework and education, among other vital societal activities. NATO itself has been no exception, as the Alliance worked to facilitate remote work by shipping critical communication and information systems items to NATO Communications and Information Agency (NCIA) support teams across various countries. This effort included simultaneously shipping laptops from its Headquarters in Belgium to Allied Command Transformation (ACT) in Virginia, United States and shuttling devices across European borders to Mons, Belgium to ensure business continuity for Allied Command Operations (ACO).4 Pandemic-induced shifts into business and operational continuity plans have thus brought to the forefront security issues like threats to digital supply chains, which have become even more salient in the wake of the SolarWinds hack.5 Recent high-profile ransomware attacks against US companies Colonial Pipeline and JBS Foods have only intensified the need to secure supply chains from digital threats.6

Concomitantly, broader questions have arisen about NATO’s strategic approach to cyberspace. The most recent Strategic Concept, released in the wake of the 2010 Lisbon Summit, provides few clues as to how collective defense, crisis management, and cooperative security relate to cyberspace. In fact, the document only mentions the word “cyber” five times.7 An urgency to reconsider NATO’s efforts in the cyber domain has been evidenced by recommendations from the NATO 2030 Reflection Group, which devoted an entire sub-section of its report to hybrid and cyber threats. In particular, the Reflection Group highlighted the need to develop both greater collective defense capacity in cyberspace and a more robust consultation framework to facilitate collective defense, crisis management, and cooperative security in the domain.8 These concerns were largely echoed by Allies in the recent 2021 Brussels Summit Communiqué.9

This chapter argues that for NATO to effectively address the broad range of security challenges emanating from the cyber domain, the Alliance must complement its current collective defense efforts by incorporating resilience and “safe-to-fail” principles into a new Strategic Concept. The unique dynamics of cyberspace mean that resilience must be a shared effort among members, and it must be projected outside the Alliance’s borders. This chapter therefore recommends that NATO adopt a fourth core task of comprehensive resilience that includes shared and forward cyber resilience as a major component. While NATO has thus far prioritized the operationalization of collective defense in cyberspace, the strategic logics that underpin collective defense will not apply to the full spectrum of threats presented by the domain. Part of the challenge, then, is to reframe the Alliance’s cyber security conversations to acknowledge the limits of collective defense.

NATO’s ongoing efforts to operationalize collective defense have relied primarily on ‘fail-deadly’ and ‘fail-safe’ logics. On the one hand, the Alliance has drawn on deterrence principles in attempts to discourage and prevent adversarial actions in and through cyberspace through the imposition of costs that would outweigh potential gains.10 While denial strategies are vital to cost imposition, deterrence-by-punishment has been the strategic bedrock of NATO’s recent initiatives. The threat of retaliatory punishment is traditionally a ‘fail-deadly’ strategy: should an adversary undertake an undesired action, i.e., deterrence fails, the Alliance responds with the use of deadly force. On the other hand, NATO has also focused on implementing defensive measures to minimize the damage and fallout from an attack in or through cyberspace. Such a ‘fail-safe’ strategy seeks to ensure that, should deterrence fail, the Alliance and its members retain the ability (albeit degraded) to operate safely and securely in the cyber domain.

Combined, fail-deadly and fail-safe strategies look to prevent and mitigate of the costs of adversarial actions in the cyber domain. In contrast, resilience in cyberspace—the ability to anticipate, withstand, recover from, and adapt to strategic shocks or surprises occurring in or through the cyber domain11—emphasizes passive protection, risk-minimization, and forward-looking continuity-of-operations efforts.12 Unlike NATO’s current approach to collective defense, resilience rests on ‘safe-to-fail’ principles. As a ‘safe-to-fail strategy,’ resilience is built on the assumption that, despite deterrent and defensive measures, the Alliance may fail to foresee adverse strategic disruptions that remove the ability to operate and coordinate in the cyber domain. To withstand and bounce forward from such disruptions, NATO must ensure that military cyber functions and capabilities fail safely—that is, to fail in ways that do not remove the ability to recover at or above original operating capacity. Resilience thus offers a way for the Alliance to account for a variety of threats and scenarios to which fail-deadly and fail-safe strategies prove ineffective. At the same time, resilience serves to enhance collective defense in the cyber domain: collective defense is more credible if the Alliance is more resilient.

This chapter proceeds in the following sections. The first describes the cyber threats facing the Alliance. The second section outlines NATO’s policy and organizational developments related to cyberspace. The third section discusses the limitations of collective defense; in short, collective defense efforts are best suited for countering the small subset of cyber incidents that reach damage levels analogous to conventional uses of force. The fifth section explores what cyber resilience looks like for NATO and why it must be a shared phenomenon that is projected forward outside the Alliance. The chapter concludes with several recommendations for the Alliance as it looks ahead to 2030 and beyond.

### Solvency: Resilience—Hamilton ’16 Recommendations

#### NATO needs to improve resilience to address cyber threats—including a NCOCC, enabling SACEUR to support member cyber capabilities, mutural cyber pledges, enhancing NCIRC, expanding training, and increasing support for CCDCE

Hamilton, Johns Hopkins Professor, ‘16

[Daniel S. Hamilton, Austrian Marshall Plan Foundation Professor and Executive Director of the Center for Transatlantic Relations at Johns Hopkins University’s School of Advanced International Studies, “Going beyond Static Understandings: Resilience Must Be Shared, and It Must Be Projected Forward,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. 44-46]

The Cyber Dimension

The responsibility to deter, detect, defend against, and defeat a cyber attack rests primarily with nations and their private sectors. But the severe impact a cyber attack can have on a nation’s critical information infrastructure, and its use in recent military operations and intimidation campaigns, has implications for Alliance security.

NATO and the defense establishments of its members are under constant attack from cyber hackers seeking to penetrate their information systems, extract data, and plant viruses that could be eventually be used against allies. NATO officials have deemed these attacks to be a tier 1 threat. Attacks are aimed against NATO systems used to develop defense policies and plans, but also more dangerously against operational cyber networks needed to execute military missions.

NATO has taken the threat of cyber attacks very seriously.It has created a high level Cyber Defense Committee that reports directly to the NAC, a working level NATO Cyber Defense Management Board, a NATO ComputerIncident Response Capability (NCIRC), a Cyber Defense Center of Excellence in Tallinn, and more recently a NATO Industry Cyber Partnership. The Wales Summit endorsed an Enhanced Cyber Defense Policy which further strengthened NATO’s efforts in this area. Yet more must be done.

Recognize cyber as an operational domain and launch a voluntary NATO Cyber Operations Coordination Center (NCOCC). The NCOCC would report to Allied Command Operations and would be funded and manned by participating members. Ideally the United States should take the lead. Participating members should be those countries with cyber operationsforces.The primary purposes ofthe NCOCC would be to share information among the cyber operational forces of members, conducttraining and education in conjunction with the Cooperative Cyber Defense Center of Excellence (CCD COE), helpAllied Command Operations and Allied Command Transformation plan cyber exercise events, and ensure deployable cyber elements are forces listed with the Enhanced NRF and VJTF.

In due course,if the NCOCC proves a success,it should transition into a permanent NATO Cyber Operations Headquarters similar to the NATO SOF HQ. Such a headquarters should generate the necessary arrangements and readiness to allow nations to pool their capabilities and produce cyber effects should there be a collective decision to do so. It should also act to achieve consensus on issues of cyber deterrence, particularly whetherindividualAlliance cyber defense capabilities alone are adequate, or whether capabilities are needed to effectively deter major strikes against NATO networks, the networks of individual nations, or against the critical infrastructures of Allied nations—especially the infrastructure identified as essential to NATO’s core tasks. While NATO’s ability to acquire capabilities to respond to such attacks is not a practical near-term consideration, individual Allies are already taking on this mission and could do the same for the Alliance in certain scenarios.

• Establish the means to allow SACEUR to plan for, integrate and employ the contributions of members’ cyber forces for defensive, offensive and exploitative cyber operations.While NATO is unlikely to agree to establishing offensive cyber capabilities for the Alliance itself, individual Allies do possess these capabilities and those capabilities may need to be coordinated in time of crisis or conflict.

• Consider Mutual Cyber Standards Pledges. National networks that connect to the NATO network can be weak, creating potential vulnerabilities for the entire system. The Alliance might address this problem via a “mutual cyber pledge,’’ grounded in an Alliance-wide certification system, in which an individual Ally pledges to meet agreed cyber defense standards and NATO itself pledges assistance to those lacking capability to meet those standards, which is then followed with a concrete work plan to achieve certification. NATO at Warsaw took some important steps in this direction.

• Enhance NATO’s Computer Incident Response Capability (NCIRC) by rationalizing and normalizing common funding, strengthening its Rapid Response Teams in order to better assist members under attack who ask for help, and generating greater protection and resilience planning for critical mobile networks,including capabilities development of national cyber cells earmarked for NRF and VJTF.

• Task ACT to develop a Cyber OperationsTransformation Initiative to explore opportunities for multinational training, networking, information sharing and interoperability among the growing number of NATO members fielding operational commands. The model for this initiative should be the successful special operations transformation initiative of the Riga summit.

• Increase support to NATO’s Cooperative Cyber Defense Center of Excellence in Estonia, which should lead NATO to draft a clear policy on responding to cyber attacks

#### NATO should expand support for internal cyber resilience initiativesand integrate resilience into partner programs

Hamilton, Johns Hopkins Professor, ‘16

[Daniel S. Hamilton, Austrian Marshall Plan Foundation Professor and Executive Director of the Center for Transatlantic Relations at Johns Hopkins University’s School of Advanced International Studies, “Executive Summary and Policy Recommendations,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. ix-xiii]

NATO

Make resilience an integral element of NATO’s core tasks, or consider making resilience a fourth core task. A key element of Russia’s strategy is the use of strategic surprise and hybrid threats to take advantage of vulnerable societies.Extremist threats from the south also challenge the fabric of Western societies. Greater societal and defense resilience can be an important component of an effective response.Creating a higher degree ofresilience in vulnerable societies makesit more difficult forstate or nonstate actors alike to disrupt and create the instability they need for their success. Societies deemed indefensible in traditional defense terms can be rendered indigestible through resilience. Resilience has become integral to each of NATo’s core tasks of collective defense, cooperative security, and crisis management, and forward resilience can be an important element of NATo partnerships. Initial activities could include the following: • Conduct a survey of resilience requirements. NATo’s newly adopted resilience guidelines provide an opportunity to survey NATo members and partners to identify how countries believe they measure up against these guidelines. The results can be used to guide further support efforts.

• Set priorities. NATo analysts might create a matrix using country vulnerability profiles and functional requirements suggested in this book along with survey results to establish a list of priority activities. For example, the matrix might show that border control is the top priority in the Baltic states but would be something differentin other nations. NATo might then use the results of this matrix to identify immediate- and longer-term resilience requirements. This effort could complement the recommended survey.

• Identify those who can strengthen forward resilience. NATo’s Civil Emergency Planning Committee has compiled a list of civilian experts who could be called upon to support the enhancement of resilience. But given the magnitude of the task, much greater efforts will be needed to identify others who can strengthen and project resilience. No single organization or country has the breadth and capability to deliver on all of these requirements for enhancing resilience. This effort would include identifying those international institutions, non-governmental organizations, nations, and individuals that have a particular expertise in some element of resilience. For example,NATo’s Cyber Center ofExcellence and its Computer Incident Response Capability are already helping countries with their network security resilience, while oSCE and institutions such as the U.S. National Endowment for Democracy or the European Endowment for Democracy might be well suited to support societal resilience.

• Expand the functions of NATO’s Civil Emergency Planning Committee (CEPC). NATo’s CEPC currently has a mandate to plan for contingencies that involve civilian casualties and to provide civilian expertise in the field of terrorism preparedness, consequence management, disaster response, and protection of critical infrastructure. If the expanded scope of resilience requirements we suggest is accepted, CEPC’s responsibilities need to be expanded and more resources will be required. There would be a corresponding shift in its emphasis towards enhancement of national resilience.

• Create Forward Resilience Advisory Support Teams. NATo has periodically used Advisory Support Teams for civilian emergency planning purposes.The resilience commitments made attheWarsaw Summit willrequire a revitalization and expansion of theseAdvisory Support Teams in such areas of emergency preparedness including assessments; intelligence sharing, support and analysis; border control; assistance to police and military in incident managementincluding containing riots and other domestic disturbances; helping effectuate cross-border arrangements with other NATo members; providing protection for key critical infrastructuresincluding energy; and, in the cyber arena, support to and enhancement of NATo’s Cyber Response Team.Efforts to build these teams should be accelerated. In certain countries, such Teams could be collocated with NATo Force Integration Units, and help national responses with NATo military activities including especially special operations activities.

• Host nations could be encouraged to establish working grouptype secretariats to coordinate defense activities with overlapping civil authority and private sector key critical infrastructure func tions to enhance national capacity to anticipate, prevent, respond and recover from disruptive scenarios and to provide a key point of contact for Forward Resilience Advisory Support Teams.

• Create “Partnership Programs” for Resilience. This concept would be modeled on the current U.S. National Guard State Partnership Program which now operates in 22 European countries and five Middle Eastern countries. In the first instance, these U.S. National Guard programs might be expanded to focus more on resilience issues.But more ambitiously, national partnerships might be created on a framework nation basisto connect NATo members and NATo partners. For example, Italy might serve as a framework nation to develop a resilience partnership with a country in NorthAfrica.Sweden might serve as a framework nation to develop a resilience partnership with a country in eastern Europe. This concept could help to decentralize the resilience-building effort and significantly expand its scope, while also contributing to establishment of specific trust funds and tailored training projects.

• Develop clear political guidance concerning which activities will be open for different partners, taking into consideration willingness of an individual partner to cooperate with the Alliance, as well as their maturity level. Some partners should be engaged into partnerships with industry and into various NATo’s education and training efforts (cyber defense courses, cyber ranges, cyber hygiene platforms, etc.). Some partners should be engaged in planning phases of crisis management and cyber defense exercises.Engagement in these activities and in the Federated Mission Networking should be widened beyond the current range of seven partners.

• Establish specialcyber support teamsthat can be deployed to partner countries to increase interoperability, improve information-sharing and coordinate responses to cyber crisis. Establish individually-tailored projects and expand existing projectsin accordance with interests and capacities of partners to enhance their cyber security and defense. Prospective cooperation areas in cyber defense include increasing interoperability,sharing strategic and technical information and threat assessments, coordinating responses to cyber crisis, and engaging partnersinto NATo’s education, exercises and training activities.

• To support NATo allies’ resilience in the cyber security context, cyber expertsshould be included within NATo Force Integration Units(NFIU).This would help assess vulnerabilities,increase preparedness and interoperability in regards with crisis response.

• Assess the levels of the existing maturity of cyber security and defense capacity in partner countries.Coordinate and synchronize mutual training and assistance projects with the EU in order to avoid overlapping.The Partnership Review and Planning Process (PARP) should include cyber defense elements as part of broader resilience efforts, and planning should to be aligned with the NATo Defense Planning Process (NDPP).

• Partners would benefit from the development of minimalrequirements for the protection of their critical infrastructure and in regards with cyber defense.

• Include resilience and forward resilience components in NATO exercises,training, education, and operational planning. Resilience events should be included especially in NATo Crisis Management Exercises (CMX) and cyber exercises such as the annual cyber coalition exercises. NATo/Partner exercises should incorporate forward resilience efforts.

• Pay attention to societal resilience. Although NATo is paying most attention to infrastructure,networks and civil preparedness,itshould also include into its monitoring, assessment and support measures considerations of societal resilience, i.e., the ability of society to maintain rule of law,respect for human rights, and democratic principles in the face of disruptive challenges.This is particularly important from the perspective of maintaining the Alliance’s credibility, cohesion, unity and public support to its mission.

• Place renewed emphasis on oversight of implementation, including novel compliance mechanisms. Peer-review groups (3-5 members making site visits to other member governments to report on resilience) has worked in otherinternational organizations – NATo should consider such mechanisms of naming and shaming as well.

• Develop a more robust strategiccommunications strategy to address Russia’s information operations, particularly where Moscow draws on social media and hidden messages that seek to exploit social and political differences in allied and partnerstates.The StratCom Center of Excellence in Riga could be used to plan how the EU, NATo, and partners could connect in order to ensure efficient strategic communication to counter hybrid threats. This would include suggestions for both vertical and horizontal organisation and points o contact in individual countries, as well as NATo and the EU, and should cover the full spectrum of endeavors, from proactive efforts to crisis management.

Include Finland and Sweden as full partners in these efforts. Both countries have significant traditions of total defense and societal security, and would bring significant added value and experience to these efforts. Finnish experience with territorial defense, border guards, and whole-ofgovernment approaches to societal security, for example, or Swedish expertise with addressing asymmetrical dependencies on externalresource flows, may mean that these countries could be leaders in cooperative efforts as neighbors seek to enhance their efforts in such areas.

• Forward resilience should be integrated as a high-priority element of each country’s Enhanced Opportunities Partnership (EOP).

• NATO should also intensify work in the 28+2 format connected to Civil Emergency Planning, which has not advanced as far as the 28+2 in the military and political arenas.

### Solvency: Resilience—Lute & Burns Recommendations

#### Resilience measures are necessary to deter hybrid attacks—NATO should lead in developing common standards, leading exercises, and developing new deterrence strategies

Lute & Burns, Harvard researchers, ‘19

[Ambassador Douglas Lute, Senior Fellow, Belfer Center and President, Cambridge Global Advisors and Ambassador Nicholas Burns, Professor, Diplomacy and International Politics, Harvard Kennedy School, “NATO at Seventy: An Alliance in Crisis,” Project on Europe and the Transatlantic Relationship, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2—19, p. 25-26]

Deterrence of hybrid, or sub-conventional, attack demands urgent attention. NATO is vulnerable to means short of Article 5’s “armed attack” including by cyber attacks, intimidation by threatening energy cut-offs, political subversion by covert agents and funding, disinformation campaigns and election interference.58 Russia has already attacked NATO members in this realm. Examples include the 2007 cyber attack on Estonia, and interference in 2016 elections in France, the United States and the United Kingdom’s Brexit referendum.59 NATO allies must invest in building national resilience—the ability to resist such measures and to respond effectively if an attack occurs. The idea of resilience is not new: Article 3 of the Treaty commits allies to “…develop their individual and collective capacity to resist armed attack.”60 Today this mandate must extend below the classic Article 5 threshold where Russia is most likely to attack.

Deterrence of hybrid attack, however, is vastly more complex than traditional deterrence. Deterrence can be achieved by denying an attacker’s ability to attain objectives and by increasing the risk of unacceptable punishment for an attack.61 Hybrid tactics challenge both forms of deterrence. National capabilities required to deny hybrid objectives extend well beyond traditional defense and are dispersed among other elements of the government at multiple levels and even the private sector, complicating integration and coordination. Cybersecurity and election security illustrate this point. Further, while the first responsibility for resilience lies with states, both NATO and the EU have a responsibility to back up member states, yet lines of authority between these multilateral institutions and member states may not be clear, common standards are not established and sharing classified information remains a persistent challenge.62 Deterring by promising punishment requires clarity on the origin of the attack. Hybrid attacks, however, are designed to be ambiguous, complicate attribution and shield the attacker from punishment. As we have seen in Ukraine, ambiguity and difficulty of attribution stressed Alliance decision-making and risked paralysis while Russia established facts on the ground that are hard to reverse. Finally, deterring hybrid attacks is connected to the drift from NATO’s core values discussed in this report. Moving away from common democratic values opens vulnerabilities for Russian attacks that aim to erode the cohesion of the Alliance by exploiting political divisions within and among allies.63

As a start, NATO should define standards for national resilience and clarify shared responsibilities for deterring hybrid attacks.64 The Alliance should be a leader in the global effort to adapt traditional deterrence principles to the cyber realm. Exercises that focus on hybrid attacks, including at the level of ministers, can illustrate the deterrence challenge and lead to refined policies. NATO could bring together ministers of defense, ministers of interior and national intelligence officials to increase the value of such exercises. NATO and the EU should coordinate common standards in member states, with priority on cybersecurity, election security and countering disinformation. A priority should be placed on publicly disclosing the nature and source of hybrid attacks. Russia must be held to account, not allowed to deny, obfuscate and hide in the shadows. In the longer term, diversifying energy sources and fully assimilating Russian-speaking minority populations should be addressed as vulnerabilities that Russia could exploit.65

### Solvency: Resilience—Maigre ’22 Recommendations

#### NATO resiliency solvency – capacity building, including info sharing, consultation, training and assistance key

Maigre, 2022

[Merle, senior cybersecurity expert at e-Governance Academy in Estonia. In 2017–2018, she served as director of the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE), “NATO IN A NEW ERA: GLOBAL SHIFTS, GLOBAL CHALLENGES NATO’s Role in Global Cyber Security” German Marshal Fund APRIL 06, 2022 [https://www.gmfus.org/news/natos-role-global-cyber-security accessed jcp-TM 6/8](https://www.gmfus.org/news/natos-role-global-cyber-security%20accessed%20jcp-TM%206/8)]

The third action focuses on building resilience of domestic critical infrastructures. Doors are locked to keep homes safe. Likewise, all NATO member states should address their digital insecurity by locking digital doors as individuals, companies, and countries. The strategic vulnerability to disruption and sabotage lies not so much in the military space but in the hospital booking system, logistics schedule, power grid, and thousands of other mainstream, civilian, mostly privately owned networks. Based on the 2016 Cyber Defence Pledge, in which member states committed to improving their ability to protect their cyber networks, the alliance could formulate a NATO cyber-security baseline with concrete resilience goals to achieve or maintain the baseline. These resilience goals could then be apportioned among member states in the same way as the defense-planning capability targets. This should come with obvious financial and investment implications. Public debates on burden sharing within NATO for too long have focused on how much member states spend on defense in isola- tion, without adequate prioritizing where those funds are going. Member states should be rethink defense spending relative to emerging threats and collec- tive security challenges. To ensure funding for cyber security is appropriately prioritized, NATO should strengthen a commitment to digital defense spending, building on the strong base it has developed in terms of doctrine, standards, and requirements. This also includes strengthening the political resilience of member states by broadening NATO consultations to include more areas of government. Regular North Atlantic Council-format meetings among member state directors of cyber authorities at the political and military levels would help build consensus on cyber policy issues.

Another course of action for NATO in cyber security is to increase its cyber capacity-building efforts for partner countries of strategic impor- tance, reinforcing NATO’s commitment to partners and projecting stability in NATO’s neighborhood. This kind of cyber capacity-building could include various types of support, ranging from strategic advice and cyber institution-building in defense sectors to education and training or advice and assis- tance in cyber defense. The objective should to be to enable capacity-building activities for military actors, along with the provision of training, equip- ment, and infrastructure for security purposes. This would allow NATO to improve the capacities of part- ners to address crises, prevent conflicts, and cater for their own security and stability by themselves, to the benefit of their population.

As one example, NATO could fill a gap in capacity- building for partner countries by bringing together military Computer Emergency Response Teams (CERTs) to share information on incident manage- ment dynamics, a key factor in modern cyber defense. While partner countries can receive support from donors in establishing mechanisms and processes to exchange information between civilian CERTs, such cooperation and communication channels are much less developed in the military domain due in large part to the high sensitivity of the information. There is a need to extend the information-sharing practices used in civilian circles to partner countries’ military CERTs. Building cyber-security capacity should focus on partners’ ability to respond to and recover from cyber incidents.

In sum, most future conflicts will have cyber components that require a technical, political, and diplomatic response. Whether the adversary is a state’s elite unit or a criminal group rendering ransomware as a service, cyber security is about risk management and solid, pragmatic defense and response measures to improve the security of the digital environment. There is a technical aspect to hardening defenses and building redundancy in data and services, but the core of resilience lies in leadership that does not ignore the problem. How our national cyber-security strategies are translated into policies and procedures needs to be understood by all stakeholders. It is now up to the alliance’s member states to provide clarity and coherence to successfully draft a new Strategic Concept that includes defense and deterrence. But this is not a job for NATO alone—it requires close coordination across national governments and the private sector, and NATO and the European Union must therefore continue to work very closely on this vital issue.

#### Solvency - expand cooperation and mil to mil exercises like Baltic Ghost

Maigre, 2022

[Merle, senior cybersecurity expert at e-Governance Academy in Estonia. In 2017–2018, she served as director of the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE), “NATO IN A NEW ERA: GLOBAL SHIFTS, GLOBAL CHALLENGES NATO’s Role in Global Cyber Security” German Marshal Fund APRIL 06, 2022 <https://www.gmfus.org/news/natos-role-global-cyber-security> accessed jcp-TM 6/8]

Action Plan for the Next Five Years

To make NATO future-proof, it must be cyber-secure and operational. But is it doing enough to address the complex and evolving challenges of cyberspace? NATO’s strategic challenge is to blend its successful conventional deterrence functions with a new strategy for cyber action. NATO’s ability to send a collective message of resistance and to establish a credible threat response is its most valuable asset on the cyber-security front.

Four sets of actions for NATO are proposed. First, denying covertness by attribution: NATO should persuade opponents that they cannot be clandestine in their cyber actions. NATO and its members need to demonstrate that it is difficult or impossible to act covertly and be clear about attributing responsibility for cyberattacks.

Until recently, governments did not publicly release details on cyber incidents. But since 2018, public disclosures of cyberattacks by several Western powers indicate a new multinational policy of state transpar- ency. The growing relevance of attribution is partially due to states becoming better at attributing cyber operations.1 Greater public knowledge of cyberattacks heightens awareness of cyber conflicts and leads to greater public acceptance of cyber countermeasures.

Ultimately, what matters is that states engaging in unlawful actions using cyber means will face conse- quences. With attribution, policymakers show that they know what is happening in these networks and can investigate incidents. It also clearly spells out unacceptable behavior and can help create state prac- tice. The best way to implement the international norms is by calling out behavior and having conse- quences when these norms are breached. Attribu- tion will make clear to the malicious actor that their actions will be seen and addressed. It is the basis, under international law, for countermeasures and self-defense.

When should states publicly attribute cyberat- tacks? Effective public attribution requires a clear understanding of the attributed cyber operation and the cyber-threat actor, but also the broader geopo- litical environment, allied positions and activities, and the legal context. The public attribution frame- work put forward by Max Smeets and Florian Egloff in March 202127 distinguishes four factors that act as enablers or constraints in public attribution. These factors are intelligence, incident severity, geopolitical context, and post-attribution actions. The combina- tion of these four components enables consistent deci- sion-making about whether to publicly disseminate information about an adversary’s actions, privately tell the adversary, or restrict knowledge of the intrusion to the government and potentially other partners.

Collecting and processing intelligence—infor- mation about foreign countries and their agents— provides a technical basis for attribution. How could allies improve intelligence sharing to conduct more rapid attribution and enable a response to adver- sary cyber activity? During the Nordic-Baltic foreign ministers meeting in Tallinn in September 2020, a 90-minute tabletop exercise was organized28 to test the ministers’ ability to respond to and attribute an esca- lating cyberattack. They answered multiple-choice questions on communication of and possible diplo- matic countermeasures to the attack. The minis- ters learned through first-hand experience that a timely exchange of technical intelligence can be key in attributing any cyberattack. “The shared view [of the countries involved]—especially when it comes to complicated issues—is crucial,” said Urmas Reinsalu, Foreign Minister of Estonia.29

Attribution is only as good as the information that allies are willing to share. NATO’s value can be in becoming the preferred platform for sharing cyber information. General Paul Nakasone, who heads US Cyber Command, told the House Armed Services subcommittee on intelligence that “in 35 years” he has never seen a better sharing of accu- rate, timely, and actionable intelligence than what has transpired with Ukraine.30 Sharing information and intelligence with allies “builds coalitions” and can “shine a light on disinformation” campaigns, like the one Russia used to lay the groundwork for their invasion of Ukraine.

As the second course of action, NATO should use the current crisis to accelerate the progress with setting up NATO’s own cyber command and sharpen allied responses to malicious cyber actions. Overall, this would give more credibility to its cyber defense. In February 2019, allies endorsed a set of tools to respond to cumulative cyber activities, but not much has happened to take it forward. It is now time to build upon this set and develop concrete steps at the political, military, and technical levels to model alli- ance behavior according to the threat landscape. This means a sharper focus on future responses to high- and low-end cyberattacks along with concrete deter- rence actions and tools for individual sectors and target types. Much of this is based on the high-end cyber capabilities of select individual allies called “volunteer sovereign cyber effects,” where cyber- capable nations deliver voluntarily offensive cyber effects on a target designated by an operational-levelcommander. The NATO Cyber Command would be responsible for matching military needs with the willingness and capabilities of the nations potentially able to deliver such effects.31 The alliance should clarify which allies are responsible for offensive cyber operations against certain targets and the informa- tion-sharing and notification requirements.

A good plan requires practice. The scenarios of cyber responses that are under the Article 5 threshold should be regularly practiced, and the NATO Cooper- ative Cyber Defense Centre of Excellence (CCDCOE) Locked Shields exercise is a good way to do so. Orga- nized since 2010, it enables cyber-security experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. The focus should be on realistic scenarios simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects. Locked Shields is a unique opportunity to encourage experimentation, training, and cooperation among allies in an authentic but safe training environment.

NATO should also make more use of its Cyber Range, a platform for NATO exercises and training in Estonia operated by the Estonian Ministry of Defense. The Cyber Range already facilitates NATO’s flagship annual cyber defense exercise Cyber Coalition, and NATO CCDCOE has based Locked Shields on Cyber Range for over a decade. The versatility and computing power of the platform allows a different, complex scenario to be simulated every year for an increasing number of participants. The technical, red-teaming exercise CrossedSwords, organized by NATO CCDCOE, tests the capabilities and skills needed when executing a full-spectrum cyber operation in real life, focusing on experimentation with integrating kinetics and offensive cyber operations in the context of a modern battlefield. More operational- and technical-level joint activ- ities should be practiced among allies and with like- minded partners in order to contribute to imposing costs to malicious actors in cyberspace. Given that NATO’s cyber response teams are stretched thin due to protecting NATO’s own networks, bi- and multilateral collaboration enables countries to share best practices and, in the event of an emergency, provide mutual rapid assistance in crisis response.

The cyber exercise Baltic Ghost originated from a series of cyber defense workshops in 2013 and should be expanded to include all NATO battlegroups in the Baltics and Poland. Currently it is facilitated by the United States European Command with the objective to develop and sustain cyber partnerships between Estonia, Latvia, Lithuania on one end, and the Mary- land, Michigan, and Pennsylvania Army National Guards on the other end. Building on the success of Baltic Ghost, regular cyber exercises should take place in multinational NATO battlegroups, led by the United Kingdom, Canada, Germany, and the United States, in Estonia, Latvia, Lithuania, and Poland. Future exercises should regularly support NATO enhanced forward presence forces and train participants to respond to aggression in a contested, degraded, and denied cyberspace environment.

# Resilience Aff: EU CP / NB Answers

### EU Link: Cooperation Turn

#### The plan spills over to increase trilateral cooperation

Ilves et al., Estonian Counselor at EU, ‘16

[Luukas K. Ilves, Counselor for Digital Affairs, Permanent Represnetation of Estonia to the EU, Timothy J. Evans, Senior Advisor, Cyber Strategy and Policy, Johns Hopkins University Applied Physics Laboratory, Frank J. Cilluffo, Director, Center for Cyber and Homeland Security, George Washington Univesity, and Alec A. Nadeau, Presidential Administrative Fellow, Center for Cyber and Homeland Security, George Washington University, “European Union and NATO Global Cybersecurity Challenges: A Way Forward,” PRISM v. 6 n. 2, 2016, p. 136-137]

EU-NATO cooperation has always presented a challenge due to the differences in the makeup of each organization’s membership. There are signs that the relationship could be warming up: the EU and NATO signed a technical arrangement in February 2016 to increase information sharing between the NCIRC and CERT-EU.65 The agreement authorizes technical information sharing to improve incident prevention, detection, and response, and is s i m i l a r t o U . S . i n f o r m a t i o n - s h a r i n g requirements between government agencies. While information sharing within the American federal government has been ongoing since 2004, it is now becoming more effective than ever due to improvements in information-sharing software, hardware, and procedures, and the adoption of standard technical specifications. Furthermore, two nonNATO EU countries are members of the CCD COE, and the EU and non-NATO members participate in or observe various NATO-related cyber exercises.

Ultimately, the United States and Europe would benefit from an EU-NATO-U.S. triangle, where the Allies could work together within NATO to further develop joint cyber defense capabilities and approaches. The EU and the United States could simultaneously work bilaterally to achieve shared objectives on other cybersecurity matters. A joint policy agenda between these two powers could include convergence between EU and U.S. security standards for cyber products and services, including joint procurements in less sensitive areas; collaborative exercises; more structured information sharing; continued development and elevation of international cyber crime law enforcement regimes; and consistent and practical data protection regulations.

The United States has much to contribute to the cyber operations of NATO and the EU, and can serve as a force to bring these two organizations closer together. American law enforcement and the deep cybersecurity talent reserves of its private sector have already proven to be invaluable partners in Europol’s cyber crime investigations. The trend toward globalized impacts from cyber threats makes it likely that partnerships on matters of law enforcement and cybersecurity in general will continue to grow. A few areas in which the United States, NATO, and the EU could further cooperate on cybersecurity policy include combined cyber forensics training to improve attribution, more widespread support for resilience and remediation practices, and greater coordination between the U.S. and EU judicial regimes when it comes to bringing cybercriminals to justice.

### EU Link: No Tradeoff

#### The parties are increasily willing to work together

Ilves et al., Estonian Counselor at EU, ‘16

[Luukas K. Ilves, Counselor for Digital Affairs, Permanent Represnetation of Estonia to the EU, Timothy J. Evans, Senior Advisor, Cyber Strategy and Policy, Johns Hopkins University Applied Physics Laboratory, Frank J. Cilluffo, Director, Center for Cyber and Homeland Security, George Washington Univesity, and Alec A. Nadeau, Presidential Administrative Fellow, Center for Cyber and Homeland Security, George Washington University, “European Union and NATO Global Cybersecurity Challenges: A Way Forward,” PRISM v. 6 n. 2, 2016, p. 137-138]

The EU and NATO have respectively made tremendous progress in building their capacity to coordinate cybersecurity and defense activities among their members. The increasing willingness on the part of these organizations to work more closely with one another and international partners is also a promising, if recent, development. Europol’s multilateral law enforcement operations against cybercriminal groups and forums represent one of the best emerging models for international resource pooling and operational coordination. In fact, the crucial role that international law enforcement must play in combatting the global cyber threat qualifies entities such as Europol for a more elevated role in international diplomacy. However, cyber crime is only one piece of the larger puzzle of cybersecurity and cyber defense. The recent successes of coordinated law enforcement operations will reach their full potential for positive impact only if NATO and the EU apply lessons learned from that realm to broader cyber policy issues.

Overall, the cyber threat landscape is pushing national governments and international organizations toward greater transatlantic security cooperation. With a growing cyber threat from nation-state actors, including a resurgent Russia, and a new norm of conflict that ensures kinetic operations will be paired with cyber aggression for the foreseeable future, security cooperation in Europe and around the world is increasingly necessary. The strides that NATO and the EU have made thus far to address cyber threats are promising but ultimately only foundational. These organizations must build on this foundation by continuing to make progress toward cross-border integration of information, capabilities, and defensive strategies if the advantage in cybersecurity is ever to be wrested from the attacker

### EU Competition: Perm Solves

#### Joint action is most likely to solve—resource constraints

Nuland et al., Slbright Stonebridge Group senior Counselor, ‘20

[Victoria Nuland, Senior Counselor, Albright Stonebridge Group, Non-Resident Senior Fellow, Brookings Institution, Christian Mölling, Director of Research of the German Council on Foreign Relations, and Sophia Becker, Research Fellow for U.S. Security and Defense Policy at the German Council on Foreign Relations, STRONGER TOGETHER: A STRATEGY TO REVIALIZE TRANSATLANTIC POWER, Belfer Center for Science and International Affairs, Harvard University and German Council on Foreign Relations (DGAP), 12—20, p. 23]

While advances have been made in NATO mobility and readiness in recent years, arms control with Russia is collapsing, and the transatlantic community has largely failed to address new threats collectively, including cyber and digital security, health security and the challenges of a more assertive China. The COVID-induced global economic recession will stress NATO nations’ defense spending and the ambitious defense capabilities goals of NATO and the EU. While some on both sides of the Atlantic are hoping for a return to “normal” with the Biden administration, the old approaches to security and defense will not be enough to meet today’s challenges.

Within NATO, and in U.S.–EU and NATO–EU relations, considerable effort will have to go into: rebuilding trust; strengthening democratic governance and shared values; aligning threat perceptions; breaking down barriers to collaboration; maximizing defense value for money; and tackling new and emerging challenges collectively. No problem can be solved successfully by the U.S. alone, by NATO alone, or just in the U.S.–EU context. The most effective approaches will combine the institutional strengths of both NATO and the EU and all 36 of their respective member states.

#### Increased cooperation over hybrid threats proves the permutation is possible and necessary

Zandee et al. 21 (Dick Zandee is Head of the Security Unit and Senior Research Fellow at the Clingendael Institute. Sico van der Meer is a Research Fellow at the Clingendael Institute. Adája Stoetman is Junior Researcher at the Security Unit of the Clingendael Institute, October 2021, Countering hybrid threats: Steps for improving EU-NATO cooperation, https://www.clingendael.org/pub/2021/countering-hybrid-threats/5-conclusions-and-recommendations/)

**Cooperation between the EU and NATO in countering hybrid threats is not only desirable, but even necessary. Considering the broad and dynamic area of threats, both organisations cannot deal with them alone and their toolboxes are complementary.** This is also realised within both organisations and their member states, as can be **seen in the intensified cooperation of the past few years**. **There is no internationally agreed definition of hybrid threats. However, the common ground between all available definitions is that hybrid threats consist of a combined use of military and non-military means to undermine societies**. Less clear is which activities should be included in the toolbox for countering hybrid threats, although undoubtedly they have to consist of a mix of military and non-military measures. **The absence of an agreed definition – also in the EU-NATO context – leaves room for flexibility in expanding cooperation between the two organisations in countering hybrid threats.**

#### Cooperation is possible – specifically in cyber – the plan creates momentum

Ilves et al. 16 (Luukas Ilves is Counselor for Digital Affairs at the Permanent Representation of Estonia to the EU. Timothy Evans is Senior Advisor, Cyber Strategy and Policy, at Johns Hopkins University Applied Physics Laboratory in Arlington, Virginia. Frank Cilluffo is the Director of the George Washington University’s Center for Cyber and Homeland Security. Alec Nadeau is a Presidential Administrative Fellow at the George Washington University’s Center for Cyber and Homeland Security, 7-28-2016, "European Union and NATO Global Cybersecurity Challenges: A Way Forward," PRISM | National Defense University, https://cco.ndu.edu/News/Article/840755/european-union-and-nato-global-cybersecurity-challenges-a-way-forward/)

**Ultimately, the United States and Europe would benefit from an EU-NATO-U.S. triangle, where the Allies could work together within NATO to further develop joint cyber defense capabilities and approaches**. **The EU and the United States could simultaneously work bilaterally to achieve shared objectives on other cybersecurity matters.** **A joint policy agenda between these two powers could include convergence between EU and U.S. security standards for cyber products and services, including joint procurements in less sensitive areas; collaborative exercises; more structured information sharing;** continued development and elevation of international cyber crime law enforcement regimes; and consistent and practical data protection regulations.

**The United States has much to contribute to the cyber operations of NATO and the EU, and can serve as a force to bring these two organizations closer togethe**r. American law enforcement and the deep cybersecurity talent reserves of its private sector have already proven to be invaluable partners in Europol’s cyber crime investigations. **The trend toward globalized impacts from cyber threats makes it likely that partnerships on matters of law enforcement and cybersecurity in general will continue to grow. A few areas in which the United States, NATO, and the EU could further cooperate on cybersecurity policy include combined cyber forensics training to improve attribution, more widespread support for resilience and remediation practices, and greater coordination between the U.S. and EU judicial regimes** when it comes to bringing cybercriminals to justice.

### EU Solvency: Division of Labor Fails

#### Division of labor fails—only joint action can address threat posed by Russia and China

Odgaard, Norwegian Institute for Defense Studies Professor, ‘22

[Liselotte Odgaard, Professor, Norwegian Institute for Defense Studies and Non-Resident Senior Fellow, Hudson Institute, “NATO’s China Role: Defending Cyber and Outer Space,” WASHINGTON QUARTERLY v. 45 n., 1, Spring 2022, p. 172-174]

And yet, in the event of US involvement in using force in a conflict with China, it is likely that Washington would redeploy forces stationed in and near Europe to the Indo-Pacific. In the absence of a European commitment to participate in countering China challenges, and if forced to choose, the IndoPacific is likely to trump Europe on the US list of security priorities. This scenario has given rise to the argument that to restore the credibility of NATO’s collective defense commitment, a division of labor between the United States and Europe would be desirable. Such an arrangement would allow the US and its Asian allies to focus on countering China threats in the Indo-Pacific, while Europe concentrates on countering Russian threats, providing more effective defenses collaboratively against threats from China and Russia.17

Rather than highlighting the need for a division of labor within NATO, the 2022 invasion has highlighted that Russia’s appetite for threatening Europe with military action is closely entwined with its long-standing strategic cooperation with China. Intelligence reports that China told Russia in February 2022 not to invade Ukraine before the end of the Winter Olympics in Beijing testify to the closely orchestrated Chinese-Russian approach to the West.18 Moscow and Beijing are both strategic opponents of the US, a shared status that has spurred them to coordinate their separate geostrategic priorities in Europe and the Indo-Pacific, forging unison pushback against what they consider Western encroachments on their spheres of interest.19 The poorer than expected performance of the Russian armed forces in its 2022 war with Ukraine has pushed China to try to appear neutral. Nevertheless, China has joined Russia in opposing further enlargement of NATO, and in the Indo-Pacific, Russia has joined China in opposing Taiwanese independence.20 It would be wise for Europe and the US to plan for Sino-Russian geostrategic coordination to continue unless more clear evidence that China will abandon Russia is presented. One thing is certain: China will work with the partners that help it advance a Sinocentric international order based on authoritarian regimes. And to counter this development, Europe and the United States need to devise effective mechanisms for joint responses to Beijing as well as to Moscow.

A US-European division of labor is not likely to help NATO develop tools to defend itself against threats from China and Russia. The lack of electronic warfare in Russia’s war with Ukraine has revealed gaps between its concept of operations and the tactics of the Ukrainian military. As demonstrated in prior operations in Syria and the Donbas, Russia will adapt and learn in the short and long term. For example, Russia can be expected to improve its electromagnetic spectrum management in order to enhance its planning and management of forces on the battlefield. Meanwhile, China is watching the performance of the parties involved in the war with a view to update its cyber and space capabilities as well as strategic concepts. As a consequence, both Russian and Chinese threats will continue to increasingly emerge in the cyber and space domains. This calls for global and functional defenses rather than an exclusive geographical focus. It is more important than ever to design NATO for a future where threats toward transatlantic security are global and requires a unified response.

### EU Solvency: NATO Key

#### NATO needs to act on the military side—necessary to solve our China impacts

Odgaard, Norwegian Institute for Defense Studies Professor, ‘22

[Liselotte Odgaard, Professor, Norwegian Institute for Defense Studies and Non-Resident Senior Fellow, Hudson Institute, “NATO’s China Role: Defending Cyber and Outer Space,” WASHINGTON QUARTERLY v. 45 n., 1, Spring 2022, p. 179-180]

NATO’s Role in the Global Commons

NATO can only be as effective as its member states allow it to be. NATO reflects the state of transatlantic relations: are US and European security outlooks sufficiently compatible such that the alliance is able to address threats from China collectively? This question is reflected in how well they manage to define common challenges and establish mechanisms that allow them to address these challenges together. NATO was a natural center of security focus for Washington when Europe was the main arena for US-Soviet deterrence. Today, the IndoPacific competes for US attention and resources as competition with China has moved to the center stage of US security and defense priorities.

The strategic shift in US priorities does not mean that Europe cannot continue to remain a significant influence on global security dynamics. The EU has demonstrated its continued relevance in the security realm, not merely by relying on its role as a major trade bloc, but also by reforming the interplay between member states and EU institutions to avoid being paralyzed by consensus requirements, which apply in most areas outside the trade sector. This is done by providing platforms for member states to start initiatives. If successful in attracting support within the union, the initiatives are consolidated by supportive mechanisms and programs.43

NATO is not the EU and hence should not duplicate its methods. The EU is driven by the urge to secure the continued influence of its member states on major global issues. NATO’s raison d’être is to facilitate transatlantic cooperation in the military sector to counter common threats and challenges. Coordination is complex at a time when US and European security outlooks are drifting apart in terms of threat perceptions and priorities. At the same time, fears of entrapment stifle NATO’s efforts to update its relevance, principally because key members such as France and Germany are not interested in NATO taking on China as a threat.

Nevertheless, NATO’s agreement to define China as a challenge promises opportunities for positioning the alliance in a key role in transatlantic relations. Because cyber and space encompass threats from other adversaries such as Russia and Iran, these domains are a good place to start taking on China as they do not require that China be singled out as a threat. By taking on the responsibility for coordinating US and European definitions of cyber and outer space threats in the military sector, integrating these domains in all organizational and operational NATO structures, devising mechanisms for the member states to address cyber and outer space threats, and by facilitating intelligence exchange and management of the vulnerabilities produced by civil-military interaction and overlapping interfaces between the cyber and space sectors, NATO can demonstrate its continued relevance for transatlantic security in an era where threats are increasingly global and transcend geographical boundaries. There’s no time like the present.

#### NATO is the best actor to solve our hybrid war internal links

Prior, Center for Security Studies researcher ‘18

[Tim Prior, Head, Risk and Resilience Research Team, Center for Security Studies (CSS) and PhD, Social and Environmental Psychology, University of Tasmania, “Resilience: The ‘Fifth Wave’ in the Evolution of Deterrence,” STRATEGIC TRENDS 2018: KEY DEVELOPMENTS IN GLOBAL AFFAIRS, Ed. O.Thränert & M/ Zapfe, Center for Security Studies, 2018, p. 64-65]

Naturally, any deterrence debate in Europe focuses first and foremost on NATO and its deteriorated relationship with Russia. Indeed, it is NATO that is primarily responsible for defending its member states and deterring existential threats – both as a nuclear alliance and as the still most effective framework for collective military action. And the alliance faces new challenges: As Russia appears to be leaning towards a broader and deeper understanding of deterrence in the form of “cross-domain coercion”, emphasizing non-military means, subversion, and information warfare besides an aggressive and ambiguous communication of its nuclear might, NATO has to adapt. In the mix of necessary answers, resilience will play an important role.

### EU NB: NATO Key to EU Leadership

#### Turn – the EU needs NATO for security – it’s a prerequisite to leadership.

Bugajski 16 (Janusz Bugajski is a senior fellow at the Jamestown Foundation, 2016, “Only NATO can defend Europe,” *European View*, 1(15), <https://journals.sagepub.com/doi/full/10.1007/s12290-016-0383-9>)

Twenty-five years after the end of the Cold War, there is no viable alternative on the horizon to NATO’s security umbrella over an expanded Europe. The idea floated a quarter of a century ago that Europe could scale down its defences and even dismantle the North Atlantic Alliance exposed a flawed fixation on an ‘end of history’ scenario that has never materialised. In practice, the forces of state nationalism and imperialist revisionism in Russia have proved stronger than those of liberalism and international cooperation with the West. In many respects, a ‘return of history’ scenario has become more evident in and around Europe, with Russia re-emerging as a revanchist power and threatening Europe’s entire eastern flank. In addition, the EU itself faces existential problems, from the financial and institutional to the demographic and political. In a potentially unstable and fracturing continent, NATO is the sole remaining institution that upholds international security. And it may become the sole multinational organisation that can provide Europe with a measure of coherence. Moreover, NATO is the binding glue of the transatlantic link with Washington. NATO without alternatives Several Western European states have hosted US bases since the creation of NATO in April 1949. Since the end of the Cold War and the dismantling of the Soviet bloc in the early 1990s, numerous voices among the new NATO members have called for permanent bases that would include US troops in the eastern part of the continent. Such voices have grown louder as Russia under President Vladimir Putin has become increasingly assertive and is now threatening the independence of numerous states, from the Baltic region to the Black and Caspian Seas. A NATO alliance that encompasses all of Europe with a permanent multinational military presence in Europe’s east is essential for four fundamental reasons. First, there is no viable alternative to NATO’s political and military structure. The EU does not provide security or generate confidence among states facing potential aggression. The EU’s Common Foreign and Security Policy is primarily a diplomatic mechanism, which openly acknowledges that NATO remains responsible for the territorial defence of Europe. Although the EU has engaged in several peacekeeping, policing and humanitarian missions, NATO possesses the main combat force not only of its European members, but most importantly of the US, which contributes a disproportionate share of Alliance troops, equipment and other resources. A strong NATO alliance is the backbone of European security. Proposals for a European Army simply dilute and distract attention from the only capable multinational Western security organisation. A European Army would not only siphon off NATO’s already limited assets and diminish its capabilities, but would also trigger rivalries between Europe and North America over the deployment of military forces. Additionally, it could split Europe between countries committed to upholding close security relations with the US and states at a safer distance from Russia that see a lesser need for American security guarantees. Such an outcome would in effect grant Moscow a strategic victory over NATO. The second reason an effective NATO is needed is that it contributes to ensuring the institutional integrity of members, together with promoting regional stability between them. Its entry stipulations include functional statehood, minority rights, civilian control over the military and settled borders with all neighbours. All new members have had to fulfil these criteria. Such conditionality also generates confidence for foreign investors and sets the stage for the integration of member states into the EU.

The third rationale for an expanded NATO concerns the sovereign choice of every independent state to determine its alliances and security links and not remain vulnerable to pressure from predatory neighbours such as Russia. In this context, it is important to distinguish between Russia’s national interests and Moscow’s state ambitions. If Russia’s neighbours join NATO, this poses no threat to Russia’s security—contrary to the Kremlin’s claims. However, it does thwart Russia’s ability to control these countries’ security postures and foreign policy.

Russia’s ambitions revolve around expanding the ‘Eurasian’ zone in which Russia is the dominant political player. ‘Eurasianism’ involves two interconnected strategies: transforming Europe into an appendage of the Russian sphere of influence and debilitating Atlanticism by undermining Europe’s connections with the US.

The EU occupies a pivotal position in Russia’s strategy as it can either strengthen or weaken the Kremlin’s approach. Moscow views a unified EU foreign policy that is synchronised with Washington’s and undermines Russia’s aspirations as a threat that needs to be neutralised. The EU’s democratisation agenda is also perceived as a pernicious ploy to undermine Russia’s agenda of supporting pliable governments in neighbouring post-Soviet states. Furthermore, EU standards for government accountability, business transparency and market competition endanger Russia’s economic penetration, which is primarily based on opaque and corrupt business practices.

An accommodationist Western approach that concedes some special ‘national interests’ to Russia not only is unacceptable to all the independent states that emerged from the Soviet Union and the Soviet bloc, but also whets Moscow’s appetite for further imperial aggrandisement. Paradoxically, consenting to Russia’s asymmetrical ‘national interests’, through which it claims a privileged role in influencing its neighbours’ affairs, is more likely to result in a collision with NATO than a more dynamic approach. If the Kremlin operates with the conviction that it has a free hand to methodically undermine countries along its borders, this could result in serious miscalculations when it overreaches by sparking conflicts with Alliance members.

Emerging threats from Moscow

The fourth and most important reason why a substantial NATO military presence in Eastern Europe is vital is that it forms the most effective deterrent and responder to major new threats. Two core challenges emanate from Russia: expansion and implosion. Moscow’s primary objective is to restore Russia as a major pole of power in a multi-polar world. The overarching goal with regard to the West is to reverse US influences in Europe and Eurasia. Russia’s neo-imperial project seeks predominant influence over the foreign and security policies of immediate neighbours so that they will either remain neutral or support Russia’s agenda. In effect, Russia seeks dependent protectorates along its borders, tied into institutions controlled from Moscow (Bugajski and Doran 2016).

While its goals are imperial, the Kremlin’s strategies and tactics are flexible, and this can make them more effective than if they were rigid. Moscow engages in enticements, threats, incentives and pressures, while claiming it is pragmatically pursuing its national interests. It pursues asymmetrical offensives by interjecting itself in its neighbours’ affairs, capturing important sectors of local economies, subverting vulnerable political systems, corrupting national leaders, penetrating key security institutions, challenging territorial integrity and undermining international unity.

Moscow is also not averse to using direct military force, as exemplified by the war against Georgia in August 2008, followed by the forced partitioning of Abkhazia and South Ossetia, and the attack on Ukraine in March 2014 with the annexation of Crimea. According to a recent report by RAND Corporation, given current force deployments, Russia could steamroll across the Baltic states of Estonia, Latvia and Lithuania with ground forces reaching the three capitals in a matter of hours. Without a more intensive regional presence, NATO forces would not have the ability to defend its most exposed states (Shlapak and Johnson 2016). Hence, the factor of deterrence may have limited value if Moscow decides to test NATO’s response.

The RAND report mirrors the concerns of Chairman of the NATO Military Committee General Petr Pavel, who has warned that Moscow could conquer the three Baltic states within two days despite their NATO membership. This is possible because of Russia’s ongoing military expansion, NATO’s relatively slow-moving command structure, and the decline in Alliance capabilities because of lowered defence spending and the withdrawal of US forces, including two heavily armoured US divisions from Germany, with only two now remaining in Europe.

Russia’s potential implosion could present an even more unpredictable future in which NATO would need to manage the multi-regional repercussions. A huge failed state on Europe’s doorstep would have various destabilising consequences for the continent—whether refugee outflows, the spillover of violence, civil wars or the emergence of new aspiring states. Paradoxically, Putin’s attempts to construct a new Russia-centred dominion are likely to accelerate the country’s decline.

An economically and militarily overstretched Russia may witness escalating economic, social, political and sub-regional turmoil and present even more menacing challenges for Western policy. NATO needs to assess the possible consequences of the chaotic downfall of the Putinist system and prepare contingencies for the conflicts that this may generate. In particular, Russia’s neighbours must be shielded from the most destabilising scenarios of civil conflict and Russia’s violent fragmentation, which could spill into NATO territory. By positioning permanent NATO bases in the countries bordering Russia, the Alliance would be better prepared for the negative consequences.

NATO realism

NATO’s European flank remains dependent on the US for its security, as its defence expenditures have been seriously depleted since the end of the Cold War. Without American involvement Europe would be unable to deter an increasingly belligerent Russia. Europe’s demilitarisation over the last decade has coincided with Russia’s military build-up (Michta 2015). The US provides 70 % of all NATO defence spending, while Europe’s contribution to NATO’s military capability is less than 25 %, and the figure is steadily falling. Several countries have decimated their equipment to such an extent that they may be incapable of deploying more than a few thousand troops in the event of outright war. Meanwhile, Russia is re-arming to the tune of $700 billion over the next decade and plans to introduce the next generation of armour, aircraft and missiles, and to modernise its nuclear forces.

Since the end of the Cold War, US officials have been prodding their European counterparts to increase defence spending in line with NATO guidelines of 2 % of GDP. Several US defence secretaries have challenged their allies to stop cutting financial support for NATO in the face of emerging and escalating security threats. They have argued that this could result in Europe’s ‘demilitarisation’, particularly in Western Europe, where political leaders and publics are becoming increasingly averse to the deployment of military force. Shortfalls in funding and capabilities will make it difficult for the Alliance to handle several simultaneous security dangers. Over the past decade only a handful of NATO members have consistently spent 2 % of their GDP on defence. During 2015 the defence budgets of several members, including the UK and Germany, actually shrank, despite pledges issued at NATO’s Wales Summit in September 2014 to increase financing of the military. In stark contrast, several front-line NATO states have decided to steadily increase their defence budgets in the face of growing threats from Russia. These include Poland, Romania and the three Baltic states.

In addition to increased funding, the European allies must also pursue military modernisation and become capable of defending all of NATO’s borders rather than operating under the traditional formula of simply being able to retaliate and allowing the extended deterrent to be provided primarily by Washington. There are legitimate concerns that most European states could not realistically meet the goals of optimal capability without significant reforms to their military structure and the elimination of waste, duplication and mismanagement in their defence bureaucracies. If the current feebleness in defence spending and capabilities continues, the next US president will come under increasing domestic pressure to curtail the American commitment to Europe’s security. This will certainly suit a revisionist Kremlin that continues to test NATO’s defences along Russia’s western flank.

In response to conventional military threats from Russia, it is essential to have an effective tripwire by ensuring the permanent presence of soldiers from various NATO states in Estonia, Latvia, Lithuania and Poland, the most exposed members bordering Russia. Moves in this direction, through the use of air policing units, regular military exercises and the creation of small bases to accommodate the planned NATO Rapid Reaction Force, were taken as the war in Ukraine unfolded during 2014 and 2015. Nonetheless, fears remained that without a more permanent stationing of substantial multinational NATO forces in the front-line states, these countries could be quickly overrun by a Russian assault.

At a mini-NATO summit in Bucharest on 4 November 2015, nine countries—Bulgaria, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania and Slovakia—signed a declaration calling on NATO to maintain a permanent presence in the region to deter Russian aggression. Since Moscow’s assault on Ukraine, NATO has taken initial steps to bolster the defence of vulnerable members by adding combat aircraft support to NATO’s Baltic air policing mission: dispatching a dozen F-16 fighters to Poland, and deploying Airborne Warning and Control System reconnaissance aircraft in Poland and Romania to help patrol NATO’s eastern borders. NATO has also drawn up defence plans for Poland and the Baltic states, including guarantees of NATO’s military response to outside attacks.

Deliberations have also intensified over the potential hosting of NATO military infrastructure. However, at the NATO Summit on 4–5 September 2014, Alliance leaders did not endorse the positioning of permanent bases in Eastern Central Europe despite the urging from Warsaw and the three Baltic governments. Instead, they agreed to create a spearhead contingent within the existing NATO Response Force—a Very High Readiness Joint Task Force (VJTF). Once formed, it would be capable of deploying at short notice along NATO’s periphery and would consist of land, air, maritime and Special Operations Force components.

It is intended that the VJTF will include 4,000 troops trained to move on 48 hours’ notice to hotspots in any NATO member state. Nonetheless, this contingent would be too small to counter the massive military might Russia has deployed along its western frontier. The spearhead force is to be part of a wider NATO response force of 13,000–30,000 troops that could take weeks to deploy in a crisis. It will benefit from equipment and logistics facilities pre-positioned in Eastern Central European countries, but the troops will not be permanently stationed in the region (NATO 2015). The force could be used as a mobile tripwire when dispatched to a threatened state. However, at this stage in its deployment, it is difficult to estimate the effectiveness of a relatively small VJTF contingent in deterring Russia’s outright invasion of a NATO member.

In February 2015, NATO decided to establish six command centres in Estonia, Latvia, Lithuania, Poland, Romania and Bulgaria to connect national forces with NATO reinforcements. They will be used for logistics, reconnaissance and planning missions with a multinational headquarters in Szczecin, on Poland’s Baltic coast. This will enable the rapid influx of thousands of NATO troops in the event of a crisis. The positioning of military hardware without the presence of US and other Allied troops is premised on the assumption that the local armed forces would be capable of defending the country for a sufficient time to allow for the timely arrival of more substantial NATO units.

Chairman of the US Joint Chiefs of Staff General Martin Dempsey has stated that America’s military is ready to ensure the deployment of high alert forces within 48 hours to NATO countries bordering Russia (Joinfo 2015). If this is insufficient to stem a Russian attack, then Washington will be ready to use additional force to protect its allies. General Philip Breedlove, NATO’s Supreme Allied Commander for Europe, has called Moscow’s conquest of Crimea a ‘paradigm shift’ that requires a fundamental rethinking of where American forces are located. In February 2016, Secretary of State John Kerry announced that the US will significantly upgrade its commitment to the security of Europe’s eastern flank, with a planned four-fold increase in spending on the European Reassurance Initiative, from $790 million to $3.4 billion.

To maintain NATO as an effective deterrent, Washington needs to adopt a more forward presence on the ‘eastern front’. NATO must also update its security posture to deal with new threats. For example, the Washington Treaty should be updated, especially Article 5 and the definition of an attack on a NATO member. This must reflect the challenges associated with contemporary warfare, including externally generated insurgencies, cyber-attacks, information warfare, and other forms of subversion aimed at undermining state independence or truncating its territory.

The Alliance needs to prepare for a wide assortment of unconventional threats and ensure that its capabilities match its commitments, including stronger national capabilities that increase the costs of a Russian attack (Grygiel and Mitchell 2014). Local forces must possess the ability to protect their own borders and increase the cost of aggression even if they cannot win a conflict unaided. In particular, NATO needs to place greater emphasis on ensuring the ability of front-line states to defend themselves during the critical, early phases of a limited war.

Each NATO state bordering Russia requires three fundamental elements: adequate infrastructure and pre-positioned equipment to allow for the speedy deployment of other NATO forces, early warning of a Russian covert attack and capable forces that can respond quickly to an assault on its territorial integrity. Each country also needs US and Western European forces positioned in them on a permanent basis to act as a tripwire against a potential Russian attack. Front-line states also require an offensive component that can threaten Russia’s aggressive operations by targeting its staging areas, airports, radar installations, sea and river ports, and logistical nodes (Grygiel 2015). Defensive capabilities alone are unlikely to be sufficient to deter a military assault.

Conclusion

For the US an unstable and insecure Europe that is fractured internally and whose borders are challenged by a belligerent Russia would constitute the greatest foreign policy disaster since the Second World War. To prevent such developments, NATO must revive its core mandate of defending the European homeland and focus less on out-of-area operations. By shifting bases and equipment eastward to confront the newest threats, NATO can help ensure that it has sufficient manpower and firepower to dissuade a Russian offensive against the most exposed Alliance members. An effective NATO remains the key institution for protecting Europe’s security. It may also become the sole multinational organisation that can provide the continent with a measure of policy coherence and maintain the transatlantic link with Washington.

### EU NB: No Security Impact

#### EU won’t replace NATO for defense – military capabilities too weak

Borzillo, 2022

[Laurent, “The Resurrection of Lazarus, or the Second Youth of NATO: The Consequences of the Russian Invasion on NATO” Policy Report Network for Strategic Analysis April 2022 - Issue 17 google Scholar – UT accessed 6.16.2022 GDI-TM]

However, given the situation and the context, it is likely that the EU's military capabilities will remain relatively weak, with NATO remaining the preferred forum for most European states. The early adoption of the strategic compass has prevented it from truly taking into account the ongoing and future consequences of the war in Ukraine. The latest version of the project for a new European rapid reaction force is indicative of this gap. Based on the existing European Union battle groups, it provides for only a limited number of troops (around 5,000), far from reaching the initial CSDP objectives set in Helsinki (around 50,000). Moreover, everything seems to indicate that its field of action would remain outside the national territory of the EU member states. It is true that the CSDP is part of the Common Foreign and Security Policy (CFSP), not the internal one. However, refusing to change the possible theatres of operation of the rapid reaction force amounts to condemning it, as the Eastern European states give priority to their territorial defence over external operations in Africa or the Middle East. This position of the Eastern Europeans, which existed before the Russian invasion, can only be strengthened following it. By extension, it is likely that this will also affect the development of the EU's military headquarters, a headquarters developed from the current Military Planning and Conduct Capability. Better coordination and understanding with NATO could avoid this scenario, but would require Paris to propose closer collaboration between the two institutions.

# Resilience Aff: Unilateral CP Answers

### Unilat Solvency: China Deficit

#### U.S. unilateralism pushes European allies towards China

Casarini, IAI Senior Research Fellow, ‘21

[Nicola Casarini, Senior Research Fellow, Instituto Affari Internazionali, “Transatlantic Cooperation on China Can and Should Not Be Taken for Granted,” Wilson Center, 12—16—21, <https://www.wilsoncenter.org/article/transatlantic-cooperation-china-can-and-should-not-be-taken-granted>, accessed 4-24-22]

U.S. unilateralism has traditionally pushed the Europeans towards advancing the so-called ‘strategic autonomy’, including the promotion of ties with Beijing. It is no coincidence that the EU-China strategic partnership and Sino-European space cooperation were established during the early 2000s when the Europeans were in deep disagreement over the Iraq War.

An issue that could trigger the next transatlantic rift over China is the Comprehensive Agreement on Investment (CAI), an accord that if ratified would boost trade and investment relations between the EU and China as well as have profound implications for the United States.

### Unilat Solvency: Hybrid Deficit

#### Multilateral action is the only way to deal with hybrid threats

Kersanskas, Hybrid CoE researcher, ‘20

[Vytautas Kersankas, Deputy Director, Community of Interest on Hybrid Influence, Hybrid CoE, “Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats,” HYBRID COE PAPER 2, Hybrid Centre of Excellence, 3—20, p. 8]

Although the primary responsibility for dealing with hybrid threats is at the national level (recognized by both EU and NATO), hybrid threats transcend national borders, making multilateral cooperation essential. The nature of the threat means that states need to work together with allies and partners. Most importantly, the EU, NATO and other multilateral organisations have numerous means at their disposal which can either support denial of hostile activities or impose costs on hostile actors. Collective action in political, diplomatic or economic domains, multinational attribution, or strategic messaging will often be more effective than national effort.

### Unilat Solvency: Interconnectness Defiict

#### Unilateral action fails--interconnecteness

Hamilton, Johns Hopkins Professor, ‘16

[Daniel S. Hamilton, Austrian Marshall Plan Foundation Professor and Executive Director of the Center for Transatlantic Relations at Johns Hopkins University’s School of Advanced International Studies, “Executive Summary and Policy Recommendations,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. viii]

Nonetheless, no nation is home alone in an age of potentially catastrophic terrorism, networked threats and disruptive hybrid attacks,. Few critical infrastructures that sustain the societal functions of an individual country are limited today to the national borders of that country. Social cohesion within a given country can be affected by flows of goods,services, money, data, energy, or simply people—whether refugees or radical elements who cooperate and operate across borders.

This means that traditional notions of territorial security must be supplemented with actions to address flow security—protecting critical links that bind societiesto one another.Governments accustomed to protecting their territories must also focus on protecting their connectedness. This requires greater attention to shared resilience. None of NATo’s seven baseline requirements for resilience, for instance, can be met without attention to shared resilience.

# Resilience Aff: Midterms DA Answers

## AFF UNIQ

### Too soon

#### Too early to predict midterm results

Mark Brewer May 19, 2022, “The 2022 Midterm Elections,” UNIVERSITY OF MAINE, https://umaine.edu/polisci/the-2022-midterm-elections/

But in politics few things are certain, and sweeping losses for the Democrats in the 2022 midterms are no exception. While their current situation looks grim, there are some reasons to believe that Democrats could avoid the worst, if not even (admittedly, in a best case scenario for Dems) maintain control of at least one chamber of Congress. The underlying economy remains strong, and if economic growth continues and perhaps even accelerates this will likely work to the Democrats’ advantage.

While President Biden’s overall approval rating is low, his approval rating on his handling of the crisis in Ukraine is quite high. If Americans continue to view the president favorably here, this will almost certainly boost Democratic congressional candidates as well. A summer relatively free of COVID restrictions would also likely boost Dems, and this increasingly looks like a real possibility. Democrats have also figured out to gerrymander themselves, which has resulted in a number of states with improved electoral maps for the party. Also, it is possible that Republicans will nominate at least some highly polarizing candidates who might struggle in November. And speaking of candidates, former President Donald Trump is not on the ballot this November, but he is still very much at the front and center of the Republican Party and of American politics. Democrats have had success running against Trump in the past, and they could do so again.

So which way will it turn out? It is too early to say. But we can say with almost absolute certainty that it will be an exciting election season.

#### Too early – GOP is taking shape and Dems are winning redistricting battles

Been Hoffschneider June 2022, “Looking Towards the Midterms: What do Recent Primary Results Mean for November?” BLUE STAR STRATEGIES, https://www.bluestarstrategies.com/news/insight-and-analysis/610-us-primaries-update

On June 7th, primaries took place in California, Iowa, Mississippi, Montana, New Jersey, New Mexico, and South Dakota. While it is still too soon to forecast what the House and Senate will look like come January, primary results so far have shown us that strong fundraising by GOP candidates has helped establishment Republicans hold their ground against MAGA-oriented challengers, while Democrats continued their efforts to capture long-time Republican seats made more favorable to them by redistricting.

#### Too soon to predict the midterms

Laura Santhanam April 29, 2022. “Independents favor the GOP right now, poll finds. Here's why it matters,” PBS NEWSHOUR, https://www.pbs.org/newshour/politics/republicans-have-the-advantage-right-now-on-key-issues-and-midterm-elections

The Republican Party rarely polls ahead of Democrats on the generic ballot, according to political scientist Lara Brown, who directs the Graduate School of Political Management at George Washington University. For Democrats to come back and win elections, they need to make significant gains in public support. But, she added, it’s too early, and political churn is too volatile, to know which party will emerge victorious from the midterms.

“Twelve hours is an eternity in politics,” Brown said.

### UQ – Dems YES

#### Dems can win due to abortion and gun control

Alison Durkee June 14, 2022, “Democrats’ Midterm Nightmare: Polls Suggest Party Could Face Historic Loss,” FORBES, https://www.forbes.com/sites/alisondurkee/2022/06/14/democrats-midterm-nightmare-polls-suggest-party-could-face-historic-loss/?sh=36b8783f5193

How things could change before November for Democrats. The Supreme Court is poised to likely overturn Roe v. Wade and let states ban abortion in the coming weeks, for instance, which recent polling has suggested may help galvanize Democrats and get more to the polls. Gun control could also come into play in the wake of a string of mass shootings, Gallup notes, as polling shows most Americans favor stricter gun measures and thus could be motivated to vote against Republicans who oppose them.

#### Several factors can help the Dems win

Mark Brewer May 19, 2022, “The 2022 Midterm Elections,” UNIVERSITY OF MAINE, https://umaine.edu/polisci/the-2022-midterm-elections/

But in politics few things are certain, and sweeping losses for the Democrats in the 2022 midterms are no exception. While their current situation looks grim, there are some reasons to believe that Democrats could avoid the worst, if not even (admittedly, in a best case scenario for Dems) maintain control of at least one chamber of Congress. The underlying economy remains strong, and if economic growth continues and perhaps even accelerates this will likely work to the Democrats’ advantage.

While President Biden’s overall approval rating is low, his approval rating on his handling of the crisis in Ukraine is quite high. If Americans continue to view the president favorably here, this will almost certainly boost Democratic congressional candidates as well. A summer relatively free of COVID restrictions would also likely boost Dems, and this increasingly looks like a real possibility. Democrats have also figured out to gerrymander themselves, which has resulted in a number of states with improved electoral maps for the party. Also, it is possible that Republicans will nominate at least some highly polarizing candidates who might struggle in November. And speaking of candidates, former President Donald Trump is not on the ballot this November, but he is still very much at the front and center of the Republican Party and of American politics. Democrats have had success running against Trump in the past, and they could do so again.

#### Dems have a strong chance to maintain control post-midterms – their ev is hype

Dean Obeidallah March 8, 2022, “Democrats' chances in the 2022 midterm elections are better than doomsayers predict,” MSNBC, https://www.msnbc.com/opinion/msnbc-opinion/democrats-chances-2022-midterm-elections-are-better-doomsayers-predict-n1290695

Anyone else sick and tired of hearing so-called political experts predict that Democrats are going to lose badly in this year's midterms? Apparently it doesn’t matter that in President Joe Biden’s first year, 6.6 million new jobs were reported, the strongest first year of job gains of any president since our government began collecting such data in 1939. Nor does it appear to matter that unemployment is down from 6.7 percent in former President Donald Trump’s last full month in office to 3.8 percent and that wages are up 5 percent over the past year.

Pundits tell us it’s an “ironclad” rule — as Fivethirtyeight.com put it — that the president’s party loses congressional seats in midterm elections. Hence, headlines that predict Democrats will lose this November in a “wipeout” and a “bloodbath.” If you listen to these people, you might be tempted to cancel the 2022 election and simply crown the GOP the winners of the House and the Senate.

Democrats should be concerned going into November. They hold only a nine-seat margin in the House, and the Senate is divided 50-50, with Vice President Kamala Harris serving as a tie-breaking vote. However, there are multiple signs that tell us Democrats could not only hold on to the House but even pick up a few Senate seats given that there is an open Senate seat in Pennsylvania and a vulnerable GOP incumbent in Wisconsin, both states Biden won in 2020.

For starters, while Biden won the White House in 2020, Democrats lost 13 seats in the House. That wasn’t good for the party, obviously, but for 2022 purposes, it means the most vulnerable Democrats are already gone. On the flip side, not a single Republican incumbent in the House lost in 2018. Good luck with GOP pulling that trick twice and not losing even one of the 213 House seats they currently hold in 2022. For example, in New York, the recently finalized congressional map that reflects the 2020 census data is expected to result in Democrats picking up three current Republican seats in November.

Plus, history tells us that there have been two times in the modern era that a president’s party gained seats during midterm elections —and the circumstances that led to those victories apply to 2022 in varying degrees. In 1998, with Bill Clinton in the White House, Democrats gained five House seats. How did Democrats buck history? GOP arrogance and overreach. The House GOP, led by then-Speaker Newt Gingrich, impeached Clinton for lying about his affair with an intern, Monica Lewinsky. But as midterm exit polls found, two thirds of voters didn’t think Clinton — who was leading a strong economy — should have been impeached, and they cast their votes accordingly.

Today’s GOP is even more arrogant and heavy-handed than Gingrich’s GOP was. Consider the Texas law that bans abortion after six weeks and forces a woman who is raped to carry her rapist’s fetus to term. That abomination of a law is being copied by numerous Republican-controlled states despite the fact that 65 percent of Americans believe the Supreme Court should uphold its landmark Roe v. Wade decision and only 29 percent support the Supreme Court striking down the constitutional right to abortion access. The Republicans don’t care what a majority of Americans think; they only care about imposing their extreme religious beliefs upon the rest of us.

Ditto for the party’s overreach by banning books and what they wrongly call critical race theory (CRT). Americans are becoming increasingly aware that so-called CRT bans are racist laws designed to prevent teachers from sharing the history of Black achievement and Black suffering at the hands of white bigots. Look at Virginia where Republican Glenn Youngkin won the governor’s race in 2021 based in part on his attacks on CRT. A recent poll found that 57 percent of Virginians oppose banning CRT and only 37 percent support it. That finding helps explain why Youngkin, who won in November with 51 percent of the vote, is already underwater with a 41 percent approval rating.

With only a few exceptions, these extreme abortion bans, bans on books and CRT, and voter suppression efforts in 19 states are embraced by Republicans nationwide. To animate their own voters, Democrats can and should use the GOP’s tyranny against them in 2022.

The second time in recent history that a president’s party picked up seats during a midterm election was 2002, the year after the 9/11 terrorist attacks, when President George W. Bush was in the White House with a sky-high approval rating and Republicans gained eight House seats and two in the Senate.

While Jan. 6, 2021, and 9/11 are not nearly the same, the 2022 election will be the first after the “domestic terrorism” waged on the U.S. Capitol by Trump supporters trying to prevent the peaceful transfer of power. The big difference, of course, is that after 9/11, Americans united against those who attacked us. In contrast, the GOP overwhelmingly supports and celebrates former President Donald Trump, who radicalized his supporters with lies about the election and called them to Washington to “stop the steal.” Since then, Trump has defended the attackers and suggested he would pardon them if he were elected president again.

Republicans want 2022 to be a referendum on Biden’s performance given that his approval ratings are in the low 40s, but Democrats should turn the tables and frame the election as a referendum on Republican extremism: from the oppressive laws mentioned above to their embrace of the man who gave us Jan. 6. That could spike Democratic turnout.

### UQ – GOP overwhelms the link – it’s a lock

#### The strength of their uniqueness cards proves the election can’t be reversed – whatever is “baked in” now will only strengthen with time

Henry Olsen June 1, 2022, senior fellow at the Ethics and Public Policy Center, “The GOP midterm wave is set — and Democrats can’t do anything about it” WASHINGTON POST, https://www.washingtonpost.com/opinions/2022/06/01/gop-midterm-wave-is-set-democrats-cant-do-anything-about-it/

Recent political history shows that the course of a fall election is almost always set by Memorial Day. RealClearPolitics Senior Elections Analyst Sean Trende recently noted that “election outcomes are more-or-less baked in” by the end of the second quarter of an election year. Not even the financial crash of 2008 made a significant dent in that year’s outcome, which Trende says was largely expected in May of that year. One probably needs to go back to the Cuban missile crisis of 1962 to find an event that might have significantly helped the party in power on the eve of a midterm vote.

Political waves also take predictable courses, and the final outcome is almost always worse for the losing party than analysts predicted six months out. In May 2010, the Rothenberg Political Report (now Inside Elections with Nathan L. Gonzales) projected a big Republican year, with GOP House gains of two to three dozen seats. Their final pre-election forecast predicted gains between 55 and 65 seats. The GOP ultimately picked up 63 from Democrats.

#### \*\*\*1AR uq o/w the link\*\*\*

#### Dems can make it closer but cannot win

Alan Greenblatt May 27, 2022, “You Don't Need to Be a Fortune Teller: Signs Point to GOP Sweep This Year,” GOVERNING, <https://www.governing.com/now/you-dont-need-to-be-a-fortune-teller-signs-point-to-gop-sweep-this-year>

For Democrats this year, the only real question is whether the elections will be only moderately bad or completely terrible.

If you think like a weather forecaster, all kinds of data point to a major storm. By basically every metric you can think of — fundraising, candidate recruitment, voter enthusiasm, demographic shifts — a big wave is forming that will sweep hundreds of Democrats out of office, up and down the ticket.

#### Dems will overwhelmingly lose – the plan can’t reverse the outcome

Alison Durkee June 14, 2022, “Democrats’ Midterm Nightmare: Polls Suggest Party Could Face Historic Loss,” FORBES, https://www.forbes.com/sites/alisondurkee/2022/06/14/democrats-midterm-nightmare-polls-suggest-party-could-face-historic-loss/?sh=36b8783f5193

Democrats could experience a “greater-than-average” loss in the midterm elections this November, new Gallup polling suggests, finding that voters’ satisfaction with the country and federal government are largely at record lows compared with other midterm years.

The Gallup poll, conducted May 2-22 among 1,007 U.S. adults, found only 41% approve of President Joe Biden’s job performance, 18% approve of Congress’ performance and 16% are “satisfied with the way things are going in the U.S.”

Only 14% have a positive view of economic conditions right now and 46% rate the economy negatively, meaning Americans have a 32-point net negative view of the economy.

All of those metrics are at least 10 points below the average for midterm years, based on Gallup’s polling going back to 1974.

Americans have a 51% approval rating for the president on average during midterm election years, a 30% congressional approval rating, 35% satisfaction with the state of the U.S. and a nine-point net positive rating of the economy.

Other than presidential approval rating—where Biden’s 41% approval is tied with former President Donald Trump’s in 2018 and higher than President George W. Bush’s 38% in 2006—every metric recorded this year marks a historic low.

Gallup suggests the low ratings mean Democrats will likely lose seats in the election this year—as a president’s party typically does during the midterms—and their losses would likely be even larger than usual if these low ratings hold.

#### Dems cannot win – history, logic, Biden’s limitations

Ed Kilgore March 10, 2022. “Biden’s War Bounce Isn’t Big Enough to Save the Midterms,” INTELLIGENCER, https://nymag.com/intelligencer/2022/03/bidens-war-bounce-isnt-big-enough-to-save-the-midterms.html

The question we really can’t answer now is whether future developments in Ukraine will help or hurt Biden’s popularity. Short of an outright Russian defeat or the deployment of U.S. troops, it’s not easy to envision a trajectory of events that will greatly affect Biden’s standing. The short-term economic fallout is likely to be negative; if it’s very negative, and Biden fails to make a Churchillian appeal for sacrifice, it could make it very hard for him to recover popular support for the most important “real life” indicator, particularly among independents.

What we do know is the party controlling the White House almost always loses ground in the midterms except for rare occasions where the president was unusually popular. And even if Biden’s job-approval rating stabilizes or modestly improves, he’s a long way from what he’d need for his party to triumph in November. As Vox’s Andrew Prokop recently put it:

The historical pattern is clear, and ominous for Joe Biden and Democrats this year: The president’s party usually does poorly in midterm elections.

“It’s not quite a law of physics, but it’s probably as close as you’re going to get in the social sciences,” says Carlos Algara, a professor of political science at Claremont Graduate University.

On the two occasions since 1934 when that near law of physics has been broken, the president in office had job-approval ratings above 60 percent. In 1962, John F. Kennedy had an approval rating of 61 percent, and Democrats still lost four House seats, which happens to be exactly the maximum number of seats Democrats can afford to lose in November without losing the House and their governing trifecta.

So even with the modest good news Democrats have been given in the redistricting process, they will need a lot more than a “bump” in Biden’s approval ratings to overcome history and logic. Yes, stabilizing and marginally improving Biden’s popularity can place a floor on Democratic losses and perhaps (with some luck and a lot of Trump-fueled Republican stumbling) even save the Senate. But the blunt truth is that barring a dazzlingly successful Biden presidency — one that extends his popularity beyond his party deep into the ranks of independents and even Republicans — Democrats have already lost. They sealed their fate in November 2020 when they carried the House by such a surprisingly small margin. Nothing Biden has done right or wrong since then has changed that fundamental reality.

## AFF LINK

### No link – Ukraine/NATO not a winner

#### Biden isn’t winning on Ukraine – voters don’t think diplomatic maneuvers like NATO cooperation are realistic

John T. Bennett April 11, 2022, “America is the Ghostbusters of Western affairs. Voters know it and want more from Biden,” ROLL CALL, https://rollcall.com/2022/04/12/america-is-the-ghostbusters-of-western-affairs-voters-know-it-and-want-more-from-biden/

President Joe Biden is hitting the road this week — and facing a challenge to convince voters why they should keep Democrats in control of Congress.

Speaker Nancy Pelosi of California has predicted Democrats will not only keep their narrow House majority but expand it. Some Senate Democrats and outside strategists have suggested they see reasons why the party might maintain its paper-thin Senate edge.

But those forecasts break with the projections of most political analysts, who are projecting Republicans will likely take control of the House and possibly the Senate come January. That means congressional Democrats have a steep uphill climb between Easter and November’s midterm elections.

First-term presidents typically lose seats in their first congressional elections — and, sometimes, as then-President Barack Obama put it in 2010, their party suffers a “shellacking.” The RealClearPolitics polling average for the “generic ballot” question of whom voters prefer gives the GOP an edge.

A major problem for Democrats is Biden, partly due to his own missteps and partly due to factors beyond his control, lacks any real coattails. Some Democratic incumbents and candidates are campaigning with more than a little daylight between themselves and POTUS.

Biden’s approval rating in the regular CBS News-YouGov survey hit the lowest mark for that survey since he started his job: 42 percent. That’s down from 50 percent in August and 62 percent in March 2021, according to the same survey.

But that overall approval number fails to paint the whole picture, and it’s not a pretty one for Biden and his fellow Democrats.

Consider the president’s disapproval ratings on kitchen table issues like his handling of the economy, rising consumer prices and increased gas prices. The number of Americans dissatisfied with his performance on things that impact their wallets every single day typically clocks in no lower than 55 percent in the CBS-YouGov poll — and on many issues, the figure hovers around a whopping 70 percent.

Biden will stop in Iowa and North Carolina this week to deliver remarks on how his administration is implementing the bipartisan infrastructure law, addressing record inflation and trying to pare high gasoline prices. Former President Donald Trump easily won Iowa and narrowly took North Carolina in the 2020 presidential election.

White House officials and Biden confidants say the president will be active on the midterm campaign trail and express confidence Democrats have accomplishments to tout this year, but it is unclear if that will move voters to their column.

’Just got to tell it‘

Barack Obama, visiting the White House last week for the first time since leaving office in January 2017, told reporters that Democratic candidates should do this during the heart of the midterm campaign season: “You’ve got a story to tell — just got to tell it.”

But do voters want to hear it?

Sixty-three percent of those surveyed in that latest CBS-YouGov poll said they disapprove of Biden’s handling of the economy. On inflation, 69 percent are dissatisfied. And more than 60 percent of those polled expressed disapproval with Biden’s handling of immigration and crime.

Biden also is underwater on his handling of Russia’s military invasion of Ukraine, though his 55 percent disapproval level against 45 percent approval more closely reflects a country split into two political camps.

Much of this era of Biden-Democratic control, following a strong start combating the COVID-19 pandemic, has come with a damned-if-they-do-damned-if-they-don’t feel.

For instance, conservative media outlets both describe Biden as a doddering, feckless 79-year-old figurehead who cannot speak coherently — and the mastermind of a liberal attempt to throw open the country’s borders while creating a socialist megastate.

Voters get in on the act, too. Biden’s scrapped “Build Back Better” domestic spending plan, as a whole, was unpopular with voters — but individual parts, when brought up separately by pollsters, got relatively good marks.

There also is a mounting feel of a snakebitten president. On several days when Biden was slated to deliver remarks on his administration’s agenda or perceived accomplishments, tragedies have overshadowed his message. It happened again on Tuesday: Before his Iowa remarks on his team’s economic efforts, a man launched an attack in Brooklyn in New York City that left at least 16 shot or injured in the subway system.

Troublingly for him and other Democrats, voters are not just siding with Republican arguments on domestic matters. New polling shows voters are siding with Republicans on how to handle the Russia-Ukraine war.

Administration officials say they have slapped sanctions, trade and other economic penalties on the Russian government, companies and individuals in an “unprecedented” way. They also tout hundreds of millions of dollars in military weaponry and other aid Washington has sent to Ukrainians.

But pollsters are being told by GOP and Democratic voters one clear thing: Biden has not done enough, nor quickly enough.

Like GOP senators and House members, the new CBS-YouGov poll shows 75 percent of Americans want to get Ukrainians more weapons — and much faster.

The same is true about sanctions. Seventy-four percent said U.S. sanctions on Russia should be increased.

‘We should ship it’

Like on domestic issues, with a deadly and sometimes-barbaric war raging in Europe, Republicans have an edge. They are, in short, winning the messaging battle.

“We know who the Ukrainians are. They’re freedom fighters. We know who Putin is. He bombs women and children,” Senate Intelligence Committee member Ben Sasse, R-Neb., said last week, before turning to pleas from Ukraine’s president: “We’re a superpower and [Volodymyr] Zelenskyy challenged us to act like it. Zelensky needs more.”

Sasse then spoke for nearly three-quarters of Americans, adding this about various missile systems and remotely piloted aircraft: “If it shoots, we should ship it. More S-300s, more Javelins, more drones, more Stingers, more everything.”

After four years of a Trump administration that was chock full of officials with little or no government experience, Biden has made good on his campaign trail promise to fill his with experienced technocrats. They respect policy-making in a way the Trump disrupters and dismantlers admitted they didn’t. Team Biden is methodical, measured and all about inter-agency task forces, whole-of-government approaches and cumbersome processes to produce policy options to Biden.

Voters, however, are hungry for action. On inflation, on gas prices, on COVID-19 and on Russia’s brutal war.

“This administration is constantly giving process answers,” a frustrated Sasse told reporters. “The administration talks about this (Ukraine) like it’s somehow some nerd lawyer discussion, not like it’s a moral battle between good guys and bad guys, and we need the good guys to win.”

Biden administration officials also curiously describe some diplomatic process that seem detached from reality. An example came Sunday, when national security adviser Jake Sullivan was asked about European allies giving Ukraine Soviet-era fighter jets on which their pilots are trained.

### No link – Dems won’t run on it

#### Dems won’t run on the plan – the strategy is to focus on domestic issues

Kevin Liptak and Phil Mattingly April 9, 2022. “Biden turns his focus from Ukraine war to kitchen table issues at home as midterms loom,” CNN, https://www.cnn.com/2022/04/09/politics/biden-domestic-issues-ukraine-war/index.html

Since Biden returned from a last-minute diplomatic outing to Europe last month, he's held no scheduled events about Russia's invasion -- a stark contrast to the previous weeks, when the President emerged regularly to update Americans on new sanctions, intelligence and Western military assistance.

Even as the atrocities of Bucha played out on television screens across the world this week — including in the West Wing, where an outraged Biden and his team watched with horror — there were no specific events to address the grim footage.

Instead, Biden's focus has been squarely at home. From the cost of health care to supply chain bottlenecks to prices at the pump and a robust economic recovery — one that officials believe simply hasn't broken through — Biden's public focus has lately been guided entirely by domestic issues.

The shift comes as Biden and his team assess a concerning political landscape complicated by the ripple effect of severe economic sanctions imposed on Moscow. Other recent developments -- including a decision to lift pandemic-era restrictions on the border -- have contributed to growing unease among Democrats about November's elections. And a recent surge of Covid-19 cases among Biden's circle has acted as a reminder of the virus' continued presence.

Biden's response to Russia's invasion of Ukraine has done little to boost his sagging political standing, despite generating unprecedented unity among Western allies. As the White House settles in for what officials believe will be a prolonged conflict, there has been a clear effort to try and break through wall-to-wall war coverage with Biden's domestic priorities.

"We can do more than one thing at a time," a senior administration official told CNN. "We have a story to tell at home and it's only natural that we would focus on that as much as possible."

### No link – Other issues thump

#### COVID, inflation, and SCOTUS thump---no one runs on or votes for the plan.

Dan Balz and Marianna Sotomayor May 16, 2022. Dan Balz is chief correspondent at The Washington Post, former paper’s deputy national editor, political editor, White House correspondent and Southwest correspondent. Marianna Sotomayor covers the House of Representatives, primarily focusing on Democratic and Republican leadership, “The forces steering the 2022 midterm elections, WASHINGTON POST, https://www.washingtonpost.com/politics/interactive/2022/big-picture-2022-midterms/

Every election has a story.

In 2010, the story was an angry tea party movement and a rebellion against President Barack Obama’s newly enacted Affordable Care Act. In 2018, it was a backlash, fueled by the energy and fury of suburban women, against the chaotic governing style and misogynistic belligerence of President Donald Trump.

The stories of some elections are often clearer in retrospect than they are in the moment, but there were blinking lights throughout 2010 and 2018 that the party in control of the White House was heading for trouble. The same can be said for 2022. President Biden’s approval ratings are in the danger zone, putting the Democrats’ slender majorities in the House and Senate in jeopardy. Many Democratic leaders are already braced, at a minimum, to lose control of the House.

Political volatility has become commonplace in a nation as deeply and closely divided as America today. Seven of the last eight elections qualify as change elections — a shift in the balance in some important way. And, if Republicans were to capture the House and Senate in November, Biden would become the fifth consecutive president to see his party lose both chambers of Congress on his watch.

But other than Democratic nervousness, what is the story of this year? What is motivating voters? What forces are steering the election, other than the tides of history?

Analysts point to a nation weary at a time in which there seems no escape from disorder, whether it be the long bout with the coronavirus or soaring prices or rising crime rates in cities or surging crossings of undocumented immigrants at the southern border. Added to all of that is the brutal war of aggression in Ukraine launched without provocation by Russian President Vladimir Putin, a conflict that is redrawing the international order.

“This is a country that is exhausted from politics,” said Democratic strategist Doug Sosnik, who served in the Clinton administration. “It’s exhausted from covid. It’s exhausted from uncertainty. It’s exhausted from inflation. It’s exhausted from the world unraveling. That’s not great when you’re in charge. But the second factor is disappointment. There was a notion that with Biden taking office we were going to come back to a sense of normalcy in the world.”

“Independent voters decide elections," said Richard Czuba, a Michigan-based analyst. "Right now [in Michigan] they are really worried about inflation — and it’s not just gas prices. You talk to people in focus groups and they will talk about milk and bread and cereal. They understand that gas prices have soared because of the war in Ukraine, but that’s not the case for food.”

#### COVID and the economy control the election – not foreign policy

Long Island University 21. "What Issues Matter Most To Voters in 2022 U.S. Mid-Term Elections: Long Island University Hornstein Center National Poll". No Publication. 9-16-2021. https://www.prnewswire.com/news-releases/what-issues-matter-most-to-voters-in-2022-us-mid-term-elections-long-island-university-hornstein-center-national-poll-301378814.html

BROOKVILLE, N.Y., Sept. 16, 2021 /PRNewswire/ -- Results of a newly released Long Island University Steven S. Hornstein Center for Policy, Polling and Analysis national poll reveal the early issues that matter most to voters in the 2022 U.S. Mid-Term Elections. The two issues that mattered most on deciding how to vote among respondents were the economy (27%) and coronavirus (17%).

TOP ISSUES FOR AMERICAN VOTERS IN 2022 U.S. MID-TERM ELECTIONS: #1 ECONOMY AND #2 CORONAVIRUS

Respondents were asked what one issue matters most in deciding how they will vote in the United States mid-term elections in 2022. While a variety of reasons were mentioned, the two issues that mattered most on deciding how to vote among respondents were the economy (27%) and coronavirus (17%). Following behind were health care (13%), national security (11%), climate change (10%), immigration (7%), racial/gender equality (6%), supreme court (4%), education (3%), and foreign policy (3%).

### No link – FoPo not a winner

#### International issues won’t swing the election

Christina Pazzanese and Gerald Seib May 18, 2022. Harvard Staff Writer. Former executive Washington editor of The Wall Street Journal, author of its “Capital Journal” column, and part of the reporting staff that won a Pulitzer Prize for its coverage of 9/11. “Will rare U.S. unity on Ukraine lift Democrats?” THE HARVARD GAZETTE, https://news.harvard.edu/gazette/story/2022/05/will-rare-u-s-unity-on-ukraine-lift-democrats/

Russia’s invasion of Ukraine has managed to unite a deeply riven America around a rare common cause. A majority in both parties say they approve of U.S. help for Ukraine. This week, Congress is expected to approve a bipartisan $40 billion aid package for the war-torn country. But will the current political consensus on the issue make a measurable difference in this fall’s midterm elections?

Gerald Seib is skeptical. Seib was executive Washington editor of The Wall Street Journal, author of its “Capital Journal” column, and part of the reporting staff that won a Pulitzer Prize for its coverage of 9/11. He retired last week. A current Institute of Politics Fellow, Seib spoke to the Gazette about how the conflict may figure in the upcoming races.

GAZETTE: Foreign policy matters are not known to motivate voters unless American casualties are involved, but the U.S. support for Ukraine is widely popular. Could Ukraine be an important issue in the midterms?

SEIB: It’s, at the moment, a secondary not a primary issue, and that’s because traditionally Americans think about economics and domestic issues first, international issues second, unless they’re forced to do otherwise, and that’s what prevails right now.

#### History of foreign policy shows international issues don’t move voters

James Traub ‘21, nonresident fellow at New York University’s Center on International Cooperation, "Biden’s ‘Foreign Policy for the Middle Class’ Is a Revolution," FOREIGN POLICY, https://foreignpolicy.com/2021/03/17/bidens-foreign-policy-middle-class-revolution/

The truth is that polls mean very little on subjects where most people do not feel personally engaged and thus have weak preferences. The United Nations has generally polled well in the United States, but politicians can make a lot more hay running against it than for it. The reason why “foreign-policy elites” have had so much leeway to fashion policy is that, unlike with domestic affairs, most Americans don’t care that much about issues where the stakes fall below life and death. Policymakers operate with implicit consent—until they can’t.

### Link turn – NATO rallies GOP

#### Plan gives midterm candidates something to campaign against – Trump turned the GOP against NATO

Lisa Mascaro May 16, 2022, AP Congressional Correspondent, “With echoes of Trump, GOP splinters over $40B for Ukraine,” KILLEEN DAILY HERALD, https://kdhnews.com/news/politics/with-echoes-of-trump-gop-splinters-over-40b-for-ukraine/article\_799d457f-8c29-528f-a39c-3ba6b54f8d61.html

Signs of Republican resistance are mounting over a $40 billion aid package to Ukraine, a reemergence of the Trump-led isolationist wing of the GOP that's coming at a crucial moment as the war against the Russian invasion deepens.

The Senate voted late Monday to advance the Ukraine aid bill 81-11, pushing it toward President Joe Biden's desk by week's end to become law. But more vocal objections from Republicans in Congress are sending warning signs after what has been rare and united support for Ukraine as it desperately battles hostile Russia. All 11 no votes came from Republican senators.

It comes as Senate Republican leader Mitch McConnell led a delegation of GOP senators to visit the region over the weekend in a show of support, vowing to push past detractors, finish up the aid package and vote this summer on expanding NATO to welcome Sweden and Finland. The leader finds himself holding down the GOP's more traditional foreign policy approach, in direct confrontation with the GOP's "America First" flank, including Donald Trump, the former president.

“There’s always been isolationist voices in the Republican Party,” McConnell told reporters on a conference call over the weekend from Stockholm. “It won’t create a problem, we’ll get the job done."

The shift in Congress opens a new political phase in Ukraine’s fight for its survival against the Russian invasion, offering a wake-up call for the Biden administration about its strategy as it resists direct U.S. military troop involvement and depends on votes in the House and Senate to fund the military and humanitarian relief effort.

While a strong bipartisan majority is poised to approve the latest round of Ukraine aid, bringing the U.S. total to $53 billion since the start of Russia’s invasion, it’s clear that Republicans, and some Democrats, are wary of a prolonged intervention and demanding a more fulsome accounting of the U.S. role overseas. While the House overwhelmingly approved the $40 billion package last week, 57 Republicans voted against it.

The most vocal lawmakers are insisting Congress will not become a blank check for overseas action amid domestic needs as they move away from the U.S.'s longstanding role of championing democracy abroad.

“We have got to take care of things here at home first,” said Republican Sen. Bill Hagerty of Tennessee, the former Trump administration’s ambassador to Japan, on Fox's “Sunday Morning Futures.”

Republican Sen. Josh Hawley of Missouri tweeted of his no vote: “That’s not isolationism. That’s nationalism.”

It’s stronger pushback than just a few months ago, at the start of war in February, when Congress made a rare show of bipartisan unity against Russian President Vladimir Putin’s invasion and rushed to Ukraine’s aid.

And it comes as the midterm election season is underway in the U.S., with Trump’s influence looming large, particularly with Republican lawmakers desperate for his campaign endorsements and support and afraid to go against him.

“We have a moral obligation to pass this aid as soon as we can,” Senate Majority Leader Chuck Schumer, D-N.Y., said Monday ahead of the procedural vote.

Trump weighed in, breaking the civic norm in the U.S. that former presidents traditionally step aside to allow one president at a time to lead, particularly on foreign policy.

The former president, whose “America First” strategy sought to pull back from U.S. commitments around the world and criticized the NATO military alliance confronting Russia, complained that Democrats are “sending another $40 billion to Ukraine, yet America’s parents are struggling to even feed their children.”

Trump had been impeached by the House in 2019 after he withheld military aid to Ukraine and pressured President Volodymyr Zelenskyy for a favor digging up dirt on Biden ahead of the U.S. presidential election, though he was later acquitted by the Senate.

On the campaign trail in Ohio, the U.S. Senate candidates, Democrat Tim Ryan and Trump-backed Republican JD Vance, have been brawling over the Ukraine assistance.

#### GOP will rally against NATO to maintain perception of hardline

Ashley Parker, Marianna Sotomayor and Isaac Stanley-Becker April 29, 2022, “Inside the Republican drift away from supporting the NATO alliance,” THE WASHINGTON POST, https://www.washingtonpost.com/politics/2022/04/29/nato-republicans-trump/

In early 2019, several months after President Donald Trump threatened to upend the North Atlantic Treaty Organization during a trip to Brussels for the alliance’s annual summit, House lawmakers passed the NATO Support Act amid overwhelming bipartisan support, with only 22 Republicans voting against the measure.

But this month, when a similar bill in support of NATO during the Russian invasion of Ukraine again faced a vote in the House, the support was far more polarized, with 63 Republicans — 30 percent of the party’s conference — voting against it.

The vote underscores the Republican Party’s remarkable drift away from NATO in recent years, as positions once considered part of a libertarian fringe have become doctrine for a growing portion of the party.

The isolationist posture of some Republicans is in line with the “America First” ethos of Trump, the GOP’s de facto leader, who has long railed against NATO. Last week, speaking at a Heritage Foundation event in Florida, Trump implied that as president he had threatened not to defend NATO allies from Russian attacks as a negotiating tactic to pressure them to contribute more money toward the organization’s shared defense.

The vote also comes against the backdrop of Russia’s invasion of Ukraine, which has catapulted NATO to its most prominent role in decades. And it comes as some hawkish Republicans seek to cast themselves as stronger opponents of Russia than Democrats.

#### GOP is swayed by Trump’s anti-NATO sentiment

Zachary B. Wolf February 24, 2022, “Analysis: Will the GOP follow Trump on Russia?” THE PRESS-ENTERPRISE, https://www.pe.com/2022/02/23/analysis-will-the-gop-follow-trump-on-russia/

The GOP, already changed by Trump, may be molting again.

The old party. Republicans used to stand up to Russia. During the Cold War, President Ronald Reagan demanded that Soviet General Secretary Mikhail Gorbachev “tear down this wall” in Berlin.

They used to oppose unwarranted invasions. In 1990, George H.W. Bush said to Iraqi leader Saddam Hussein that his aggression against Kuwait “will not stand.”

They used to recognize that even modern Russia is a threat to the US. Mitt Romney — who became the Republican presidential nominee in the 2012 race against President Barack Obama — said that year that Russia was the United States’ main geopolitical foe.

A new tone. The party today is under the influence of Trump, who heaped admiration on Putin for invading another country with a democratically elected leader.

“I went in yesterday and there was a television screen, and I said, ‘This is genius.’ Putin declares a big portion of the Ukraine, of Ukraine, Putin declares it as independent. Oh, that’s wonderful,” Trump said on Tuesday in an interview on “The Clay Travis & Buck Sexton Show,” a conservative radio show.

He then suggested it would be nice to have a “peace force” like the Russian military to be stationed on the US border with Mexico — a supremely flawed comparison since Trump wants to secure the border, whereas Putin appears to be set on claiming new territory. Putin has misleadingly referred to Russian forces he ordered to enter eastern Ukraine as “peacekeepers.”

Holdouts. It was Republicans like Reps. Liz Cheney of Wyoming and Adam Kinzinger of Illinois, the few seeking accountability for the Capitol Hill insurrection, who openly criticized Trump’s praise of Putin.

Others’ praise for Putin. Before the Ukraine invasion, there were already echoes of Trump’s high regard for Putin among Republicans.

Trump’s secretary of state, Mike Pompeo, called Putin “a very talented statesman” who has “lots of gifts” in a Fox interview. The Kansas City Star wrote in detail about Pompeo’s comments regarding Putin and Ukraine over the years.

Disinterest in other democracies. After the invasion of Ukraine began, there was a lot of disinterest from conservative voices.

“As an American, what’s in this for me and my neighbors and the rest of us? And all I’m getting is that we can feel morally satisfied because we hate Putin,” Tucker Carlson said on Fox on Tuesday.

J.D. Vance, an author and Trump acolyte running for Senate in Ohio, has pushed an almost isolationist view of foreign policy, arguing the US has no real interest in Russia’s incursion into Ukraine and should instead be focused solely on the Southern border.

“‘America First’ means not listening to the same people who have blundered us into disaster after disaster on the world stage,” Vance said on Twitter on Wednesday.

Coincidental alignment. Even Republicans who talk about the need to support Ukraine have suggested the US might reject out of hand, as Putin desires, admitting Ukraine into NATO.

Sen. Josh Hawley, the fist-pumping Missourian who helped question the US presidential election results, recently wrote a letter to Secretary of State Antony Blinken questioning the wisdom of even entertaining the idea of adding Ukraine to NATO.

It just so happens that Putin’s main goal of halting the expansion of NATO is exactly in line with Hawley’s letter.

An authoritarian and a wannabe authoritarian. Trump’s reverence of Putin is well documented, as are Putin’s efforts to meddle in recent US presidential elections with an eye toward helping Trump’s chances.

Putin has won elections with unbelievable support. Trump is still won’t believe he lost the 2020 election. Both men may be running again in 2024.

In fact, their interests have often dovetailed.

Putin wants to beat NATO back to its Cold War membership and undermine European unity.

Trump groused about NATO throughout his presidency, and frequently misrepresented NATO’s requirement that member nations spend 2% of their GDP on defense. He moved to pull US troops from Germany, which drew warnings from people like Romney, although NATO officials tried to put a positive spin on the move.

#### NATO can be weaponized by the GOP

Ashley Parker, Marianna Sotomayor and Isaac Stanley-Becker April 29, 2022, “Inside the Republican drift away from supporting the NATO alliance,” THE WASHINGTON POST, https://www.washingtonpost.com/politics/2022/04/29/nato-republicans-trump/

Another sign of the party’s isolationist wing emerged Thursday, as the House passed an update to a World War II-era military bill creating a lend-lease program intended to make it easier for the United States to supply Ukraine with military aid. Only 10 lawmakers — all Republicans — voted against the measure.

In an exchange earlier in the week between Secretary of State Antony Blinken, who was testifying before Congress, and Sen. Rand Paul (R-Ky.), Paul pushed back on Blinken’s assertion that over the years Russia has shown a willingness to attack countries like Georgia that are not part of NATO, while giving wider berth to countries that are members of the alliance.

“You could also argue the countries they’ve attacked were part of Russia, or were part of the Soviet Union,” said Paul, who was one of just two senators who voted against a 2018 bill reaffirming support for a NATO, in what was at the time a pointed rebuke of Trump.

“Yes, and I firmly disagree with that proposition,” Blinken responded.

For some foreign policy experts and international allies, the mere fact that nearly one-third of the Republican conference voted against a bill that fundamentally seeks to support both NATO and Ukraine highlights a marked foreign policy evolution in the Republican Party.

“We now are really seeing the true impact of deep, deep political polarization, where it is better to harm the other side than do what’s right for the country,” said Heather Conley, president of the German Marshall Fund. “This deep domestic polarization has now crept into foreign and security policy. There has always been strong bipartisan support for NATO, but everything now has become polarized and can be weaponized against the other side, even if it supports U.S. national security interests.”

## AFF IMPACT

### GOP too fractured to solve an impact

#### Internal divisions stall any GOP agenda even if they retake Congress

Anthony Zurcher May 3, 2022, “Midterms 2022: What will Republicans do if they win Congress?” BBC, https://www.bbc.com/news/world-us-canada-61280069

This year, the Republican Party leadership seems to have settled on a similar path. That means focusing its messaging on dissatisfaction with President Joe Biden and the Democrats, rather than advancing a particular governing agenda.

What will that mean if they do win in November?

Confusion all around

When asked in January what his party would do if it regained control of Congress next year, Senator Mitch McConnell - who would in all likelihood run the chamber if Republicans prevail - was coy.

"That is a very good question," he said. "And I'll let you know when we take it back".

In the House, it's a similar problem. Minority Leader Kevin McCarthy has set up a taskforce to come up with a campaign agenda - something easier said than done. When it was attempted prior to the party's national convention in 2020, Republicans were unable to agree on an electoral platform - the US political equivalent of a British party manifesto. The platform for the re-election of Donald Trump was instead simply a renewal of the 2016 document, even with its dated references to Barack Obama and the "failed" incumbent president.

The apparent lack of focus is being felt by the rank-and-file voters whose enthusiasm the party will need in November.

At the February Conservative Political Action Conference, or CPAC, a gathering of right-wing activists and politicians in Florida, more than one attendee was unimpressed.

"I come to CPAC, and I hear a lot of blah, blah, blah, blah, blah," said Florida resident Bernita Gigowski. "And I just want to yell out, 'but you've been in office for 10 or 12 years and what have you done?'"

"The Republican Party is currently going through some growing pains," said Daniel Hopping, a college student attending the conference.

The lack of a cohesive Republican platform is, in part, a reflection of the changes the party has undergone since Mr Trump won the presidency in 2016, said Mr Hopping.

"We're becoming more of a populist, limited-government, culturally-sound party rather than just, 'let's just cut taxes and have a nice trade deal or something.'"

As was the case for the Democrats during the Trump years, a common foe can help cover obscure intra-party fault lines.

Among Republicans, the divides between the party's big-business, corporate interests, the Christian evangelicals and the white working-class voters who flocked to Mr Trump's America-First rhetoric have been smoothed over but still run deep.

But that temporary unity is fragile, and comes with risks.

After Republicans won the Senate and held the House of Representatives in 2014, dissatisfaction among rank-and-file voters - particularly on issues such as trade and immigration - may have contributed to the success of Donald Trump's anti-establishment presidential campaign. Those divides haven't entirely vanished, and if Republicans take power next year, acrimony over the direction of the party on social issues, trade, foreign policy and immigration could re-emerge.

### Impact turn – GOP bad – Democracy

#### Red wave kills U.S. democracy

Jena Griswold ‘21, October 4, 2021, chair of the Democratic Association of Secretaries of State and Colorado secretary of state, as interviewed by Jeremy Stahl, “The 2022 Races That Could Determine if Trump Steals the Election in 2024,” SLATE, https://slate.com/news-and-politics/2021/10/in-the-2022-midterms-election-integrity-is-at-stake.html

2022 is going to have a huge impact on democracy, because we are seeing the Big Lie proponents running to become secretary of state. In every swing state that has a secretary of state race, there is an extreme Republican candidate that was either at the insurrection, an author of voter suppression, or an advocate of the Big Lie. That includes Mark Finchem. You also have in Arizona, Michelle Ugenti-Rita, who was an author of [a] voter suppression [bill]. It includes in Georgia, where Congressman Jody Hice voted against certifying the 2020 electoral college results and has repeatedly claimed that the elections in Georgia were rife with irregularities. You have Kristina Karamo in Michigan, who falsely claimed former President Trump won Michigan and spent weeks challenging election results. She also, by the way, visited Arizona to see the partisan election review. Then you have Jim Marchant in Nevada, who basically alleged voter fraud in his own congressional loss when he lost by 5 points. And here in Colorado, I’m running against a person who again is spreading the Big Lie.

President Trump recently endorsed multiple Republican candidates for secretary of state who have been spreading the Big Lie. And he keeps making it clear that he’s making disavowing facts and election results a litmus test to an endorsement. And that’s why the 2022 election is going to be so important. Voters will get to choose who they want to oversee the elections. Democracy is literally going to be on the ballot.

#### U.S. democracy implosion goes global, economic breakdown, threatens extinction

Gregory R. Copley ’17, August 19, Dean of the College of Fellows of the International Strategic Studies Association, member of the Order of Australia for contributions in the field of strategic analysis, “What Would A U.S. Civil War Look Like?”. OilPrice, https://oilprice.com/Geopolitics/North-America/What-Would-A-US-Civil-War-Will-Look-Like.html

It may, in other words, be short-lived simply because the uprising will probably not be based upon the decisions of constituent states (which, in the US Civil War, created a break-away confederacy), acting within their own perception of a legal process. It is more probable that the 21st Century event would contage as a gradual breakdown of law and order.

The outcome, to a degree dependent on how rapidly order is restored, would likely be the end, or constraint, of the present view of democracy in the US. It would see a massive dislocation of the economy and currency. It would, then, become a global-level issue.

Humans mock what they see as an impulse toward species [suicide] [death] among the beautiful lemming clan of Lemmus lemmus.1 In fact, these tiny creatures have a societal survival pattern which seems more consistent than that of their human detractors. The pattern of human history shows that civilizations usually end through internal [illness] [problems] rather than at the hand of external powers.

#### \*\*\*Democracy internal\*\*\*

#### If the GOP wins midterms they won’t allow Dem victory in 2024, crushing democracy

Will Bunch ’21, May 11, “A U.S. comeback, or looming civil war in ‘24? | Will Bunch Newsletter,” THE PHILADELPHIA INQUIRER, https://www.inquirer.com/columnists/attytood/us-comeback-or-looming-civil-war-24-will-bunch-newsletter-20210511.html

GOP control of the House — with the now-50-50 Senate very much up for grabs — would end the ambitious pieces of Biden’s agenda, but it also flashes danger for the 2024 POTUS election, regardless of whether the Former Guy or someone else is the Republican nominee. In 2020, Team Trump’s half-baked schemes to overturn Biden’s victory were easily shot down by judges or state election officials, but in hindsight this may have been a trial run for 2024 and making their plan work, even if Biden or his successor gets the most votes.

In Georgia, for example, the most troubling provision in that voter suppression bill that Gov. Brian Kemp signed under a painting of a former slave plantation gives the state’s GOP-led General Assembly effective power over the State Board of Elections and also would allow the state board to take over local county boards in places such as Democratic-controlled Atlanta. Other proposed bills would give state lawmakers powers that they lacked in 2020, to more aggressively probe fraud allegations and possibly certify winners.

“So what happens in 2024 if President Biden or Vice President Harris win the Electoral College, but local Republicans on county boards with majority Democratic votes refuse to certify the election,” writes David Atkins in Washington Monthly, or “when state legislatures who have seized control of certification refuse to certify their state tallies; when a potential Republican majority in the House of Representatives refuses to certify the Electoral College tally?”

Good questions. When Trump supporters who invested heavily in the Big Lie about 2020’s election outcome saw their fantasies collapse, it resulted in the January 6 insurrection on Capitol Hill, where five people died, along with some faith in the stability of U.S. democracy. So how will the other side react in 2024 if an election is actually stolen from the rightful winner? While Democrats are trying to tackle a crisis in real time, Republicans are playing a long game from Phoenix to D.C., with the potential for ripping our nation asunder.

### Impact turn – GOP bad – Trump ‘24

#### GOP win leads to Trump in 2024.

Julian Zelizer ’21, July 25, 2021, CNN Commentator, “The threat November 2022 poses to Biden,” https://www.proquest.com/docview/2554825750/37CC7151C6034A36PQ/98?accountid=10747

A base for 2024: Successful midterm elections can become a platform to prepare for a successful run against the president in his reelection bid. In 1966, for instance, Republicans gained seats in the midterm elections even though Democrats retained control of the House and Senate (which, other than when the Republicans controlled the Senate from 1981 to 1987, the Democrats held from 1955 to 1995). Teaming up with southern Democrats, in 1967 and 1968, Republicans put pressure on President Lyndon B. Johnson to cut Great Society spending and to deal with the inflationary effects of the war in Vietnam, all of which helped Richard Nixon win office in 1968.

To be sure, strong midterm performances don't always have this effect. Though Democrats were devastated when the GOP took control of Congress in 1994, President Clinton was able to decisively defeat Senator Robert Dole in 1996.

In 2023, Republican control of the House or Senate would likely help the GOP. Republican senators hoping to run for the White House in 2024 would have new opportunities for national attention. A Republican House or Senate could shift attention toward questions that would benefit possible candidates who are currently serving as governors. And given the close alignment of Congressional Republicans to former President Trump, this would clearly boost his chances for reelection.

#### Trump in ’24 collapses the economy and causes China war

Damon Linker ’21, August 3, “Trump 2024 could be American democracy's zero hour,” THE WEEK, https://theweek.com/donald-trump/1003257/trump-2024-stop-the-steal

Let's begin at the beginning: Is Trump going to run again? No one can know for sure, but it's looking likely. For one thing, because he's nursing grudges and he wants revenge. For another, because he's under legal threat from various investigations, and if he were to win, he would likely be immunized from punishment until he left office. Then there is his insatiable craving for attention. He received inhuman amounts of it while living in the White House, which means he's been enduring painful withdrawal ever since. In this respect, the continued social media ban on Trump could be increasing the likelihood that he'll run again, since he's incapable of hogging the spotlight in any other way.

But won't Trump have to compete against other Republicans for the GOP nomination? Not really. In addition to him holding commanding leads over potential rivals in every survey of Republican voters, there is the unreality of all such polls. It might be interesting to see that Florida Gov. Ron DeSantis polls best against Trump in a large field. But would DeSantis actually run against Trump in the primaries? Make a compelling case about why voters should prefer him over Trump? I find that hard to imagine, since it would be guaranteed to provoke a furious salvo of attacks from Trump in defense of himself, which would diminish any rival in the eyes of most Republican voters. It's a no-win scenario. (Which is why the only Republicans who might seek to challenge Trump are those, like Utah Sen. Mitt Romney or Wyoming Rep. Liz Cheney, who have no chance at all of winning the nomination and would be running kamikaze campaigns designed to take Trump down a peg in the general election.)

So Trump is quite likely to run — and quite likely to win the Republican nomination if he does. What happens then?

One possibility is that the Democrat wins the general election decisively — so decisively that most of the Republicans in Congress and in red state legislatures currently indulging in absurd conspiracies about the stolen election of 2020 and the insurrectionary violence of Jan. 6 are unwilling to go along with an effort to overturn the results. This would mean Biden, Harris, or whichever Democrat ends up running would have to win swing states like Pennsylvania, Michigan, Wisconsin, Arizona, and Georgia by a couple of percentage points. (The national popular-vote margin will be irrelevant.) In such a situation, the procedures of democratic transition would probably unfold without major incident, no matter how much of a stink Trump tried to make.

Then there's the (unlikely) possibility of Trump solidly defeating his general election opponent. This is improbable because Trump has never won more than 46.9 percent of the vote, and his refusal to accept the results of the last election and incitement of his supporters on Jan. 6 alienated some Republicans and a good number of independents. Trump may be able to win the GOP primaries in a walk, but bettering his 2020 showing in the general election of 2024 will be quite difficult. That is, unless some other event or series of them intervene to severely discredit the Democrats. Like what? Think runaway inflation or other evidence of a sharp economic downturn, continued growth in violent crime, and/or the outbreak of war with China over an attempted invasion of Taiwan.

#### \*\*\*Internal extensions\*\*\*

#### Red wave in ’22 shifts momentum toward Trump’s reelection in ‘24

Margaret Sullivan May 15, 2022. “Perspective: Democracy is at stake in the midterms. The media must convey that,”WASHINGTON POST, https://www.washingtonpost.com/media/2022/05/15/democracy-midterms-vote-integrity-media-coverage/

Koppelman underscored what we should all be clear about by now: that most of the Republican Party publicly touts the lie that Donald Trump won the 2020 election but that the vote was rigged and victory stolen from him. The Republican elected officials who won’t back Trump are being driven out of office by his faithful. “Those true believers think there is no way Trump could lose a presidential election,” he wrote, “and maybe that no Republican nominee could.”

That makes the outcome of this year’s midterm elections extraordinarily consequential. If Republicans take one or both houses of Congress, and if Trump or another Trump-inspired Republican runs for president in 2024, Koppelman added, “there may be no stopping the tide.” These true believers will see to it that the Republican nominee is declared the winner — even if it takes a coup to do so. (Let’s face it: We saw that very thing attempted on Jan. 6 last year when a violent mob stormed the Capitol and demanded the election results be reversed.)

#### GOP winning ’22 gives Trump reason to run in ‘24

AWS ’21, September 17, “Graham told Trump that Trumpism ‘will die’ if the GOP loses in 2022: Book,” https://awsforwp.com/2021/09/17/graham-told-trump-that-trumpism-will-die-if-the-gop-loses-in-2022-book/

Although Trump has not yet formally announced whether he will run for president in 2024, Graham said the former president’s legacy is tied to the party regaining control of Congress, according to an exchange Woodward and Costa described in “Danger.”

“You can sue Biden better than anyone else,” the South Carolina Republican said according to the book. “But you can not do that and complain about losing at the same time. The media is not your friend. They are going to take the waste line you give in a speech about 2020, and it just obliterates all the other things you say about, how Biden is driving the country in the wrong direction. “

Graham told Trump that if he could help Republicans win the handful of seats needed to take control of Parliament and retrieve the necessary seat, put the party back in control of the Senate, then it would help his legacy and give him renewed political capital.

“If we come back in 2022 and resume the House and take the Senate back, you will get your fair share of credit,” the senator said according to the book. “If we do not manage to take Parliament and the Senate back in 2022, I think Trumpism will die. January 6 will be your obituary.”

He stressed: “If we do not win in 2022, we are sad.”

#### Trump is willing to run in ’24 but it’s unclear

Danielle Ong ’21, August 8, “Trump Will Run For President In 2024, Still Leads GOP: Top Republicans,” INTERNATIONAL BUSINESS TIMES, https://www.ibtimes.com/trump-will-run-president-2024-still-leads-gop-top-republicans-3269079

Sean Spicer, Trump’s former press secretary, said that the ex-president has indicated his interest in making another bid for the presidency after watching current President Joe Biden’s response to a variety of issues, including immigration.

“He’s in,” Spicer told the Washington Examiner in an interview for his upcoming book, “Radical Nation: Joe Biden and Kamala Harris’s Dangerous Plan for America.”

The former press secretary, however, added that Trump may be less interested to run in 2024 if the GOP secures the House and Senate in 2022. “There needs to be something that will keep him out,” Spicer added.

The Examiner has not explicitly stated whether Spicer is giving his opinion or whether he has spoken to the former president or a person with knowledge of Trump’s 2024 plans.

Spicer’s remarks come after RNC Chairwoman Ronna McDaniel said Trump “still leads the party” during a Sunday interview with John Catsimatidis on "The Cats Roundtable."

“You know, I always say go back to the voter, and I think when you see the [number] of people that show up to the rallies for President Trump and this $102 million fundraising haul, I think the voters in America — Republicans in America — would absolutely say the president's the most popular Republican and still leads the party,” McDaniel said, as reported by The Hill.

While Trump is yet to formally announce his 2024 bid for the presidency, he has helped the Republican party raise millions of dollars for the 2022 midterms elections.

#### \*\*\*Impact extensions\*\*\*

#### Trump reelection threatens extinction – climate change, China war, disease, social collapse, democracy, human rights

Eve Ottenberg ’21. October 22, “The Rightwing Horror That Won't Go Away,” COUNTERPUNCH, https://www.counterpunch.org/2021/10/22/the-rightwing-horror-that-wont-go-away/

On the very unlikely chance that Trump regains power, how bad would it be? Worse than your worst nightmare. And that’s assuming the powers that be wouldn’t try to resuscitate Russophobia. First, covid would roar back, as Trump would dismantle the Biden architecture of mask and vaccine mandates. Second, he would strip government of career officials and pack it with fanatical Trump parasites, and he would do this at once, having learned from his presidency that he can’t run departments like Justice as his own personal mafia without ditching people marked by any modicum of integrity. Without doubt, he would assault the press in every way possible, up to and including arresting journalists.

Trump would also cripple social security by eliminating the payroll tax. Medicare would be in his sights as well. He would inflame his base with wild fibs about migrants, who, in turn, would be brutalized even worse than they are under Biden. Trump would do everything in his power to pollute the planet and make the climate catastrophe worse. We know all this, because he did it before. The ghastly list of Trump horrors is enormous. But standing at the head of it all, looming over humanity’s future like the shadow of death, is war with China. If the human race survives a Trump Reich without nuclear war starting in Taiwan, the only explanation will be divine intervention.

#### GOP winning midterms propels Trump, risking total breakdown of democracy

Damon Linker ’21, August 3, “Trump 2024 could be American democracy's zero hour,” THE WEEK, https://theweek.com/donald-trump/1003257/trump-2024-stop-the-steal

The real danger would arise in a situation where Trump lost by a narrow margin, setting up a redo of the post-2020 election effort to "stop the steal" — especially if the GOP has taken control of both houses of Congress (as seems likely) in the intervening 2022 midterm election. One possibility is that the Democrat prevails by winning a small number of states that are controlled by Republican legislatures and those elected officials reject the results, pronouncing Trump the winner instead. This would then be followed by a Republican-controlled Congress certifying those results on Jan. 6, 2024. That's the scenario that many Democrats already worry quite a lot about.

But another series of events could be more likely.

Imagine that things are much less clear-cut than an outright steal by the Republicans. Imagine, instead, that Trump goads some legislatures to try for a steal, but others balk, prompting armed protests at state capitals. Conservative media outlets also fracture, with some opposing Trump's moves but others cheering them on as the only thing standing in the way of the progressive imposition of a "theocratic oligarchy."

Many Republicans in Congress, meanwhile, think Trump is full of it, but they've gone so far in endorsing his lies about election fraud going back to 2020, and in whipping up hysteria about the existential threat posed by the left, that they feel boxed in. The growing protests in Washington and around the country, organized by the militia movement, scare them. But so do the protests encouraged by the left in cities across the nation. Trump would be insisting that any outcome that doesn't deliver the White House to him should be considered illegitimate, while Democrats claim the same thing about any outcome that doesn't keep the White House in their hands.

In such a situation, we could end up with more than one slate of electors, with none of them adding up to 270. More than a constitutional crisis, this would be a legitimacy crisis that would raise the very serious prospect of full-blown democratic procedural breakdown, with no person or institution possessing the requisite authority and trust to swoop in and settle the burgeoning dispute.

How likely is it that this exact series of events unfolds in precisely this way? Not very. Contingencies we can't imagine today will undoubtedly intervene and quite possibly send events down a path we can't yet anticipate. Or else one of the less dangerous options sketched above will transpire.

But the very fact that Trump running again for the presidency could set in motion a series of events that brings American democracy to the brink is something that everyone should be pondering and preparing for as we approach our country's next civic reckoning.

### A2 turns the case

#### Europe and the GOP could work together

Ashley Parker, Marianna Sotomayor and Isaac Stanley-Becker April 29, 2022, “Inside the Republican drift away from supporting the NATO alliance,” THE WASHINGTON POST, https://www.washingtonpost.com/politics/2022/04/29/nato-republicans-trump/

But Europeans who were heartened by the outcome of the last American election are beginning to eye upcoming contests, including this year’s midterms and the 2024 presidential race. Their apprehension about a Republican takeover of Congress, which could revive Trump’s brand of foreign policy, is offset by hope that Russia’s invasion of Ukraine will strengthen the Republican Party’s internationalist wing and compel the party to lock arms with Europe.

“I’m very concerned about the situation in America — the split of the society, the concentration on domestic issues, the underestimation of the importance of America’s international role,” said Thomas de Maizière, a former center-right lawmaker and high-ranking government minister in Germany who co-chaired a NATO working group convened in 2020. “But there are Republicans we work excellently with, and I would expect them to take on a larger role if their party takes power.”

Whether that assessment reflects an accurate reading of Republican politics is an open question. The answer, however, is existential in Europe, where the fallout from the war in Ukraine has showcased the importance of the United States and the limits of aspirations for European autonomy on matters of technology and defense, according to lawmakers and diplomats.

Flash points are already coming into view. In 2020, NATO Secretary General Jens Stoltenberg started a working group aimed at strengthening NATO. The group’s final product, “NATO 2030: United for a New Era,” included proposals, such as the creation of a Center for Democratic Resilience, that have been scorned by pro-Trump Republicans, including many of the 63 Republicans who recently voted against the House resolution affirming support for NATO.

The outcome of that vote surprised even Trump’s former ambassador to NATO, Kay Bailey Hutchison, who argued that the U.S. commitment to the alliance has remained ironclad across administrations, despite bellicose rhetoric.

“I was nonplussed by that vote,” she said in an interview.

A diplomat from a Baltic state, who spoke on the condition of anonymity to avoid alienating U.S. partners, called the vote a “Trump effect.”

“But how many voted for it?” the diplomat added. “The mainstream is clearly in favor of NATO and strengthening NATO.”

Similarly, Sen. Thom Tillis (R-N.C.), the co-chair of the Senate NATO Observer Group, who just returned from a trip to the alliance’s headquarters in Brussels, said the recent Republican votes against NATO were “poorly timed,” but he dismissed the 63 House Republicans as an “inconsequential” number.

#### Conservatives want to stop Russia so anti-NATO beliefs are in decline

Ashley Parker, Marianna Sotomayor and Isaac Stanley-Becker April 29, 2022, “Inside the Republican drift away from supporting the NATO alliance,” THE WASHINGTON POST, https://www.washingtonpost.com/politics/2022/04/29/nato-republicans-trump/

Another European diplomat said the war in Ukraine has caused European nations to address some of the complaints leveled by Trump, including insufficient spending on defense and reliance on Russian oil and gas. Those were the two issues raised by the former president when he criticized Stoltenberg at an alliance summit in 2018.

“It should no longer be a big issue for his supporters,” the diplomat said, speaking on the condition of anonymity to be candid on a sensitive issue.

But for some, the changes are not enough. Rep. Warren Davidson (R-Ohio), who voted against the recent resolution, said he objected not to NATO but to its future direction, which in his view places too large a burden on the United States and involves too much promotion of specific values.

The resolution’s affirmation of “unequivocal support” risks being mistaken for unconditional support, Davidson said. When asked whether he could envision the United States exiting the alliance — as Trump considered with former advisers — Davidson said the real issue is rather whether other member nations who are not spending sufficiently on defense should leave the club.

“Is there a point where America would consider pulling out? It’s something we should discuss,” said Davidson, an Army veteran who was stationed in Germany when the Berlin Wall fell in 1989. “The better question is whether there’s a point where we would say to other member countries, ‘This might not be your place — you’re disinvited.’”

Davidson said he objected in particular to the resolution’s endorsement of the Center for Democratic Resilience, which he called an “entity designed to meddle in other countries’ domestic politics.”

Disagreements have broken out among member nations over the erosion of democracy within the alliance, with criticism directed in particular at Turkey, Hungary and Poland. A Central European diplomat said objections to the democracy center reflect admiration for the likes of Hungary’s Viktor Orban in other Western nations.

De Maizière echoed that view, saying his primary concern about upcoming U.S. elections was that “right-wing Republicans are drifting away from this common path of Western values.”

“But I have confidence that you more or less win elections in the middle in America, not at the extremes,” he added. “In the end, perhaps Biden will lose Congress, but I don’t see Trump again as president.”

Radoslaw Sikorski, a Polish member of the European Parliament who chairs the body’s delegation for relations with the United States, said Ukraine “is the second big issue on which Republicans and Democrats agree, after China.”

“Ukraine has given new credibility to the Atlanticist wing of the Republican Party, which I find encouraging,” said Sikorski, a member of his country’s centrist Civic Platform party and a prominent critic of the ruling, right-wing Law and Justice party. “There seems to be competition in being pro-Ukrainian and wanting to stop Putin.”

### A2 Afghanistan reinvasion good

#### U.S. presence in Afghanistan increases instability

Vanda Felbab-Brown ’21, April 15, Initiative on Nonstate Armed Actors Co-Director - Africa Security Initiative Senior Fellow - Foreign Policy, Center for Security, Strategy, and Technology, “The US decision to withdraw from Afghanistan is the right one,” BROOKINGS, <https://www.brookings.edu/blog/order-from-chaos/2021/04/15/the-us-decision-to-withdraw-from-afghanistan-is-the-right-one/>

The Biden administration’s decision to withdraw all U.S. troops from Afghanistan by September 11, 2021 is a wise strategic choice that took significant political courage. The administration correctly assessed that perpetuating U.S. military engagement in Afghanistan has become a strategic liability and a futile investment that lost the capacity to alter the basic political and military dynamics in Afghanistan. That does not mean that desirable political and security developments will follow in Afghanistan after the U.S. military withdrawal. Unfortunately, the possibility of an intensified and potentially highly fragmented and bloody civil war is real, and at minimum, the Taliban’s ascendance to formal power will bring painful changes to the country’s political dispensation.

The basic wisdom of the administration’s decision is the realization that perpetuating U.S. military engagement would not reverse these dynamics and that U.S. military, financial, diplomatic, and leadership resources would be better spent on other issues. Even so, the administration made some serious tactical mistakes in its announcement.

#### Turn – Afghanistan presence trades off with efforts that are more important to U.S. hegemony

Vanda Felbab-Brown ’21, April 15, Initiative on Nonstate Armed Actors Co-Director - Africa Security Initiative Senior Fellow - Foreign Policy, Center for Security, Strategy, and Technology, “The US decision to withdraw from Afghanistan is the right one,” BROOKINGS, <https://www.brookings.edu/blog/order-from-chaos/2021/04/15/the-us-decision-to-withdraw-from-afghanistan-is-the-right-one/>

The Biden administration’s political courage lies in its refusal to be cowed by the possibility that a terrorism threat will grow in Afghanistan after the U.S. withdrawal. That specter has been a key justification for militarily staying on and on. That possibility needs to be weighed against other already materialized strategic threats and realities. Indeed, another wise aspect of the Biden administration’s decision was to stop treating U.S. Afghanistan policy in isolation from other issues and strategic priorities; to date, the tyranny of sunk costs has inflated Afghanistan’s importance.

Now, threats from China, an aggressive Russia, North Korea, and Iran — as well as zoonotic pandemics — are more important strategic priorities. Investing in U.S. Special Operation Forces, top leadership attention, and financial resources to counter those threats can deliver far greater strategic benefits than perpetuating the Afghanistan military effort.

#### Presence in Afghanistan does not solve terrorism – only risk of a turn

Vanda Felbab-Brown ’21, April 15, Initiative on Nonstate Armed Actors Co-Director - Africa Security Initiative Senior Fellow - Foreign Policy, Center for Security, Strategy, and Technology, “The US decision to withdraw from Afghanistan is the right one,” BROOKINGS, <https://www.brookings.edu/blog/order-from-chaos/2021/04/15/the-us-decision-to-withdraw-from-afghanistan-is-the-right-one/>

The Biden administration correctly assessed that the threat of terrorism from Afghanistan today is in fact smaller than from various parts of Africa and the Middle East. In Somalia, for example, al-Shabab’s territorial and governing power are steadily increasing and the group retains a strong allegiance to al-Qaida. The Islamic State (ISIS) in Somalia, while much weaker than al-Shabab, retains persistent capacity. Various al-Qaida and ISIS affiliates robustly operate in Mali and other parts of the Sahel and North Africa. Thus, even though the Taliban is unwilling to sever its connections with al-Qaida, that threat is not radically different from the terrorist threats against the United States and our allies emanating from other locales. Though hopefully the U.S.-Taliban Doha agreement from February 2020 will incentivize the Taliban to prevent al-Qaida from taking actions against the United States and its allies from Afghanistan, and ongoing U.S. policy should be geared toward this objectives through diplomacy, conditional aid and sanctions, and, even, possibly occasional strikes from off-shore.

Moreover, U.S. veterans of such frustrating unending wars are an important source of right-wing armed recruitment in the United States and the threat to public safety, democracy, and rule of law those groups pose here. By minimizing such U.S. military engagements abroad, the United States is taking a step in addressing this important danger.

The Biden administration’s political courage lies in its refusal to be cowed by the possibility that a terrorism threat will grow in Afghanistan after the U.S. withdrawal. That specter has been a key justification for militarily staying on and on. That possibility needs to be weighed against other already materialized strategic threats and realities. Indeed, another wise aspect of the Biden administration’s decision was to stop treating U.S. Afghanistan policy in isolation from other issues and strategic priorities; to date, the tyranny of sunk costs has inflated Afghanistan’s importance.

Now, threats from China, an aggressive Russia, North Korea, and Iran — as well as zoonotic pandemics — are more important strategic priorities. Investing in U.S. Special Operation Forces, top leadership attention, and financial resources to counter those threats can deliver far greater strategic benefits than perpetuating the Afghanistan military effort.

#### U.S. action in Afghanistan can’t solve – not a basis for hegemonic success

Vanda Felbab-Brown ’21, April 15, Initiative on Nonstate Armed Actors Co-Director - Africa Security Initiative Senior Fellow - Foreign Policy, Center for Security, Strategy, and Technology, “The US decision to withdraw from Afghanistan is the right one,” BROOKINGS, <https://www.brookings.edu/blog/order-from-chaos/2021/04/15/the-us-decision-to-withdraw-from-afghanistan-is-the-right-one/>

THE HARD GROUND REALITIES IN AFGHANISTAN

The United States hasn’t achieved its goal of defeating the Taliban. For several years, the Taliban has been steadily ascendant on the battlefield. It is on a path to become the strongest political force in Afghanistan, and a powerful actor in a future Afghan government.

Continuing the U.S. deployment won’t alter this reality. There is no credible path whereby a sustained U.S. troop presence helps bring a desirable peace deal — “desirable” defined as a Colombia-like deal, with minimal political representation for the Taliban in national and subnational government, an amnesty, and fighter demobilization and reintegration assistance. In Colombia, the war was stalled at a much lower level of conflict when negotiations with the leftist guerrillas began, and the basic trends for the Revolutionary Armed Forces of Colombia (FARC) were headed downward. The opposite is the case in Afghanistan, where Afghan security forces by and large remain weak, often reach accommodation with the Taliban, and suffer from many deficiencies.

The U.S. military presence has slowed the Taliban’s military and political gains, but not reversed them (even when American troop levels were 100,000 strong). It has no prospect of accomplishing them with 5,000 or 10,000 troops staying for another five or 10 years, let alone less. Since 2015, the U.S. approach to Afghanistan has been staying and praying — praying that the Taliban will make enough strategic mistakes to do itself in on the battlefield. It has not.

Nor has the United States managed to redress another key malady of Afghanistan: the perpetually parochial, fractious, and corrupt political elite, which engages in disruptive politicking instead of governing, even as Afghanistan has burned in an intensifying insurgency. Neither U.S. and international donor threats to reduce aid nor the ever-clearer and nearer prospect of the U.S. military withdrawal have swayed politicians toward unity against the Taliban and fundamentally improved governance.

Moreover, sustaining a U.S. military deployment in Afghanistan until a peace deal is reached would neglect the fact that any serious negotiations amidst the ground realities require the Afghan government to cede a considerable amount of power to the Taliban. The Afghan government has naturally not wanted to do so, and thus had had no interest in seriously negotiating with the Taliban. As long as there was a prospect for the United States staying militarily and propping up the Afghan government, Kabul has had little incentive to negotiate. Conversely, a firm U.S. withdrawal date — which Trump and now Biden have declared —incentivizes the Taliban not to negotiate until after U.S. troops are gone and the Taliban gains more power.

Supporters of a sustained presence point out that the U.S. withdrawal is abrupt; rather, Washington has repeatedly and ever more strongly signaled it over a decade. In 2014, for instance, the Obama administration was on the verge of going merely to an embassy-level military presence. But the Afghan government and political elites have ignored the steady warnings, hoping instead to entangle the United States with an open-ended military commitment until the Taliban was much weakened, however many years or decades that would take.

### Heg bad

#### Multipolarity is inevitable – maintaining U.S. hegemony prompts superpower conflict

Dr. Nadia Helmy ’22, April 14, “The Chinese theory on “the end of American hegemony” after the Ukrainian war,” MODERN DIPLOMACY, https://moderndiplomacy.eu/2022/04/14/the-chinese-theory-on-the-end-of-american-hegemony-after-the-ukrainian-war/

From my point of view, in my personal belief that the multipolar international system has already begun to become clear, and before the outbreak of the Russian-Ukrainian war in the first place, with its many aspects of applications and features. We can find the analyses done by the “Harvard University” in the USA, emphasizing that China is quickly catching up with the United States of America in terms of (technology, military and strategic capabilities), despite the dominance of the United States of America over international finance and research and development.

Here, China is well aware of the (American desire for global hegemony and the unilateral system to direct the whole world). Therefore, the United States of America is concerned about the Chinese and Russian powers, especially after Russia launched its current attack against Ukraine, due to the interference of the United States of America and the West in Russia’s spheres of influence, with an attempt Ukraine’s inclusion in NATO, with the realization that China is the second largest developed economy in the world and has enormous military defense capabilities, and its Russian ally is a formidable military force that Washington and its allies in NATO fear, which was evident during the Ukraine war, as well as regional influence. Russia and China together have intertwined and connected borders and sprawling geographic spaces internally and externally, in addition to the abundance of resources, and the most important thing for me is encouraging their citizens to (belief in the idea of ​​national tide and a sense of popular nationalism and strength globally in the face of American and Western hegemony to stop and limit their power and call for their national popular leaders to rally with their leaders).

China is seeking to achieve a high degree of strategic cohesion with Russia, with (expanding their alliances globally between the developing countries of the South, which are represented in the African, Arab and Latin American countries). Therefore, the United States of America realizes the strength of the alliance and partnership between China and Russia, and the strong support for each other politically, economically, militarily and technologically. China has also become more aware that through deep political, economic and security cooperation with Russia, China will ensure the possibility of forming a multipolarity, with the presence of more than one international and regional pole around the world, with an emphasis on expanding this through (encouraging more different developing countries to join their alliance to reform the current world system, which is dominated by American policies and undermines the sovereignty of weak and marginalized countries by interfering in the internal affairs of countries to ensure their control over them).

We find that in the face of the American economic power, China and Russia together represent about 77% of the gross domestic product of the United States of America alone, in the current value of the dollar and in comparison to the purchasing power parity of Russia and China together compared to Washington, and in addition, the United States of America is now burdened with debt, which has increased to reach about $30 trillion, with (the US debt ratio exceeds many times the value and proportion of its GDP, which China is well aware of about the decline in US economic power globally).

In view of the United States of America’s understanding of the indicators and axes of power, China and Russia, the United States of America has become more and more promoting confrontational concepts in their confrontation, as the most threatening countries to the world. With the American focus on (the issue of the rise of China and the ideological confrontation with the Communist Party of China as a civilization different from the West and liberal American and Western concepts. As a result, Washington has become more eager to impede and halt Chinese growth in particular and limit the scope and limits of the partnership and alliance between China and Russia). Which the Egyptian researcher has carefully analyzed during the Ukrainian-Russian war, with the American insistence on the need for China to adopt a clear position on that Russian war against Ukraine, and Washington’s attempt to take strict commitments against China to ensure that it does not support Russia economically. This is what China and its communist leaders have become aware of, and are aware of these American methods to drive a wedge between it and Russia and President “Putin”.

The whole world is aware that these close relations and alliances between China and Russia are the cornerstone for establishing and forming a multipolar international system, in the face of US policies that are still seeking to preserve their global dominant uniqueness. Therefore, China and Russia are trying to expand the scope of their international partnerships through (the Chinese Silk Road, launching initiatives for development partnership with developing countries of the South, African, Arab countries, Latin and South American countries), because success in this strategy is enough to break that American hegemony, and is a basic guarantee for the transition for a multipolar world.

Here we analyze the impact of the strategic mistakes committed by the United States of America to destabilize the world, by increasing the intensity of conflict and international polarization, as well as its inability to modernize the global system, to overcome shortcomings, challenges and new competitions, but Washington has created many international crises in large parts of the world, Such as: (Afghanistan, Iraq, Syria, Venezuela)…etc. And its spending of a large budget that exceeded 8 trillion dollars for the war on terrorism, which proved the extent of the American failure and impotence in confronting it after its humiliating withdrawal from Afghanistan and the Taliban movement’s control of the government. These are the internationally failed American policies that caused a state of global division in its confrontation.

Therefore, from my point of view, the United States of America is trying here to (take advantage of the crisis of the current Russian war against Ukraine to unite the front of NATO and its members in the West in the face of Russia and President “Putin” under its leadership) to assert its hegemony and uniqueness globally in the face of China and Russia, which is what it must be aware of. The countries of the European Union, in view of the violation by the United States of its covenants and harm to the interests of its European partners, and the most prominent example to me of this issue, is the (American signing of the Aukus military defense agreement with Australia and Britain in the face of France), which caused the Europeans and France to lose that deal, passing Washington’s interests and its excessive selfishness in dealing with its European allies by giving preference to its interests over it and passing it in the face of them, harming them in practice.

On the other hand, the United States of America failed to adapt to the changing global economy, unlike China, after a number of global economic crises, such as: (the Corona virus pandemic, the global financial crisis in 2008, the Ukraine crisis), and others. Which caused (millions of American citizens to lose their jobs, especially in the field of manufacturing and technology), which the United States of America tried to evade internally by blaming the unfair trade policies pursued by China internationally in confronting them.

Here we will find the extent of Chinese President Xi Jinping’s insistence, in all his political speeches, to emphasize the concept of (the common future of humanity), and to emphasize his slogan around (the Chinese dream), to achieve a well-off society, and to work according to the principle of mutual benefit for all, and international profit for all. With President (Xi Jinping’s focusing on the path leading to the realization of this Chinese dream), through three axes, which are: (the Chinese road, the Chinese spirit, and the Chinese power).

The speeches of Comrade Chinese President “Xi Jinping” are focusing on the keys and mechanisms for implementing this Chinese dream in an internationally multipolar world, and the extent to which this is appropriate for China and the rest of the world. We find that the essence of implementing this Chinese dream internally is to reach an internationally multipolar world away from the concepts of American hegemony. Hence, this Chinese dream of an international multilateral world has become (the essence of Chinese national identity by seeking to restore its influence as a force by following China and the ruling Communist Party leaders for several important policies, including the axes of development and reform policy plans across China). In the end, it reflects all (the components of the basic socialist culture and values ​​of China, as well as that Chinese spirit that is in harmony with the goals of the Chinese state, the nation and all the Chinese people).

Based on this aforementioned analysis, we can conclude that American hegemony has already ended globally or is on the way to disappearing or evading, but achieving (a stable global balance of power) is still possible.

# Resilience Aff: NATO Focus DA Answers

### NATO Uniq: China Split Now

#### NATO allies are divided over China policy

Moller, Seton Hall Assistant Professor, ‘21

[Sara Bjerg Moller, Assistant Professor, School of Diplomacy and International Relations, Seton Hall University, “China’s Rise Is Exactly the Kind of Threat NATO Exists to Stop,” WASHINGTON POST, 3—12—21, <https://www.washingtonpost.com/outlook/chinas-rise-is-exactly-the-kind-of-threat-nato-exists-to-stop/2021/03/11/c3adfad6-8211-11eb-81db-b02f0398f49a_story.html>, accessed 6-8-22]

Regrettably, as with Russia, Europe is divided over how to deal with China. Many European allies are wary of picking sides in the struggle for influence between the United States and its Asian rival. Some, like Germany, even appear outright resentful at the suggestion that they must choose. German Chancellor Angela Merkel rushed last year to conclude the E.U.-China Comprehensive Agreement on Investment — even though the incoming U.S. national security adviser, Jake Sullivan, had strongly signaled that Europe should wait till Biden’s inauguration.

China’s rise is indisputably the most significant geopolitical development of the 21st century. It would be strange for an alliance as potent as NATO to ignore the challenge. A Europe that continues to downplay the danger posed by China’s growing influence in the North Atlantic area could lead Xi to succeed where Trump and Putin failed: He could splinter the alliance.

### NATO Uniq: Cohesion Low Now

#### Non-unique and no internal link – longer term tensions undermine cohesion

Borzillo, 2022

[Laurent, “The Resurrection of Lazarus, or the Second Youth of NATO: The Consequences of the Russian Invasion on NATO” Policy Report Network for Strategic Analysis April 2022 - Issue 17 google Scholar – UT accessed 6.16.2022 GDI-TM]

The longer the conflict continues, the more it potentially risks undermining NATO's cohesion. For the time being, the scenario of a direct military response has been ruled out by the allies because of the absence of a legal obligation to intervene and because of the risks of a direct confrontation with Russia. If this attitude can be explained by Russia's status as a nuclear power (and is comparable to the behaviour of Western countries during the Budapest uprising of 1956, the Prague Spring of 1968, or the Russian invasion of Afghanistan during the Cold War), indirectly it may encourage an increase in war crimes committed by Russia. Therefore, it is not certain that this position of non-intervention will hold if Moscow uses chemical weapons, especially because of public pressure in the West.

In view of the arms deliveries, not to mention the influx of volunteers transiting the border between Ukraine, on the one hand, and Poland, Slovakia and Romania on the other, Russian actions against convoys cannot be ruled out either, which again would entail the risk of both escalation with NATO military involvement and disunity over such an escalation among Alliance members. Moreover, overwhelming Ukraine with weapons could facilitate non-state violence, arms trafficking and terrorism in the long term in Europe. Consequently, there may be short/medium term dissension over the right way to deter Russia and support Ukraine. The Polish attempt to transfer MIG-29s to the Ukrainian armed forces, the debate on a no-fly zone over Ukraine, or the unilateral U.S. embargo on Russian hydrocarbons are all signals of potential future divergence in this regard.

In the medium term, cohesion within the alliance both on the Russian-Ukrainian conflict and beyond remains dependent on American domestic politics. In the event of a Trumpist Congress in 2022, or even a Trumpist president in January 2025, NATO's resurrection could then be seriously compromised, especially in the event of an American exit from the Alliance, even if this no longer seems to be discussed in the United States, at least for the moment.

### NATO Uniq: Expansive Agenda Now

#### Non-unique – NATO already operating outside core mission to check China

Haroche and Quencez, 2022

[Pierre Haroche Research Fellow in European Security at the Institute for Strategic Research (IRSEM, Paris) & Martin Quencez, Research Fellow and Deputy Director of the Paris office of the German Marshall Fund of the United States“NATO Facing China: Responses and Adaptations” Survival 64:3, 73-86, DOI: 10.1080/00396338.2022.2078047 accessed TANF online – UT 6.16.2022 GDI-TM]

A broader definition of European security issues

While China is not a short-term military threat to Europe, its influence is growing in many strategic sectors with direct security implications for the Euro-Atlantic area. For some member states, including the US, NATO must therefore contribute to a better interweaving of security issues with the eco- nomic, technological and industrial policies of the allies. Whether it is a matter of better coordinating mechanisms for screening foreign direct investment in critical infrastructure or strengthening technological cooperation within the Alliance through its Innovation Fund and the Defence Innovation Accelerator for the North Atlantic (DIANA), NATO is increasingly active in these areas, which seem far removed from the core business of a military alliance.

### NATO Link: Article 3 Resilience

#### Resilience key to the alliance—outlined in Article 3

Roepke & Thankey, NATO’s Defence Policy & Planning Division ‘19

[Wolf-Diether Roepke and Hasit Thankey, Resilience and Civil Preparedness staff, Defence Policy and Planning Division, NATO, “Resilience: The First Line of Defence,” NATO REVIEW, 2—27—19, <https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html>, accessed 6-3-22]

The current unpredictable security environment has led to a renewed focus on civil preparedness. NATO and its member states must be ready for a wide range of contingencies, which could severely impact societies and critical infrastructure.

Since the early 1950s, NATO has had an important role in supporting and promoting civil preparedness among Allies. Indeed, the principle of resilience is set out in Article 3 of the Alliance’s founding treaty, which requires all Allies to “maintain and develop their individual and collective capacity to resist armed attack”. This involves supporting continuity of government, and the provision of essential services in member states and civil support to the military.

Through much of the Cold War era, civil preparedness (then known as civil emergency planning) was well organised and resourced by Allies, and was reflected in NATO’s organisation and command structure. During the 1990s, however, much of the detailed civil preparedness planning, structures and capabilities were substantially reduced, both at national level and at NATO.

Events since 2014 – most notably Russia’s illegal annexation of Crimea and the rise of ISIS/Daesh – signalled a change in the strategic environment, prompting the Alliance to strengthen its deterrence and defence posture. Meanwhile, terrorist and hybrid threats (particularly recent cyber attacks) continue to target the civil population and critical infrastructures, owned largely by the private sector. These developments had a profound effect, bringing into sharp focus the need to boost resilience through civil preparedness. Today, Allies are pursuing a step-by-step approach to this end – an effort that complements NATO’s military modernisation and its overall deterrence and defence posture.

#### Resilience strengthens collective defense

Roepke & Thankey, NATO’s Defence Policy & Planning Division ‘19

[Wolf-Diether Roepke and Hasit Thankey, Resilience and Civil Preparedness staff, Defence Policy and Planning Division, NATO, “Resilience: The First Line of Defence,” NATO REVIEW, 2—27—19, <https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html>, accessed 6-3-22]

While civil preparedness is primarily a national responsibility, it is an important aspect of NATO’s security. Indeed, strengthening national resilience provides a better foundation for collective defence. NATO’s approach to building resilience is through an “all-hazards” approach: planning and preparedness that is relevant for all types of threats, whether it be natural disastershazards, hybrid warfare challenges, terrorism, armed conflict, or anything in between. National authorities have realised that the risks and vulnerabilities they face, amplified by the level of interdependence among the sectors, requires a whole-of-government effort as well as more direct cooperation with the private sector.

NATO’s civil preparedness has facilitated and supported national efforts, developing sector-specific guidance and tools to assist national authorities in their effort to meet the ambition established by the seven baseline requirements. These include guidance on a range of issues, including how to deal with the movement of tens to hundreds of thousands of people; addressing cyber risks to the health sector; comprehensive planning for incidents involving mass casualties; and ensuring security of medical supply arrangements. NATO’s civil experts, who are based in Allied nations, have helped assess and provided tailored advice on measures to enhance resilience and levels of civil preparedness.

### NATO Link: Cyber Turn—2AC

#### Cyber cooperation pivots NATO to address the threat posed by China and enables coordination with the EU

Odgaard, Norwegian Institute for Defense Studies Professor, ‘22

[Liselotte Odgaard, Professor, Norwegian Institute for Defense Studies and Non-Resident Senior Fellow, Hudson Institute, “NATO’s China Role: Defending Cyber and Outer Space,” WASHINGTON QUARTERLY v. 45 n., 1, Spring 2022, p. 175-179]

NATO in Cyber and Outer Space

Cyber and space is a promising arena for NATO to address China challenges by building member state resilience. Like the air and sea domains, as areas that belong to no one state and which provide access to much of the globe, they form part of the global commons. Command of the commons has been the key enabler of the US global position of power for many decades.26 However, China wields a sufficient range of sea, air, cyber, and space capabilities such that the global commons is now a contested zone. In contrast to the sea and air domains, cyber and space are sparsely regulated. This lack of international norms enhances the risk of conflict based on misperception, making NATO cooperation pertinent. Adversarial activities toward the US and Europe in the cyber and space domain threaten transatlantic security. These come not just from China, but also from other adversaries such as Russia and Iran. Mechanisms for addressing these challenges in the military sector are essentially generic and not, at least in their basic design, established with a particular country in mind. Thus, cyber and space provide an avenue for NATO to contribute significantly to deterrence of China without having to combat major internal resistance. NATO would also benefit from long-standing US-EU cooperation on cyber and space issues.27

NATO has vowed to clarify Article Five’s collective defense commitment to encompass threats to satellites in space and coordinated cyberattacks. NATO can design this effort to include adversarial behavior from China. The alliance already has an array of instruments to deal with cyber and space challenges from adversaries. These can be extended to encompass China without pronouncing it a threat.28 This approach allows the US and Europe time to adjust their cooperation to take into account the fact that China poses military threats to them both without explicitly using the language of threat at a time when NATO members do not agree if China should be defined as a challenge that can trigger Article Five responses.

Since the late 1990s, the vulnerability of shared space assets to cyberattacks has been a concern for both the US and Europe. For example, in 1998 a USGerman satellite, used for peering into deep space, was rendered useless after it turned suddenly toward the sun, damaging its High Resolution Imager by exposure. NASA later determined that the accident was linked to a cyber-intrusion at the Goddard Space Flight Center. Coordinated cyberattacks have emerged as a major threat to both the US and Europe since the late 1990s. For example, for about eighteen minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed US and other foreign internet traffic to travel through Chinese servers. Other servers around the world quickly adopted these paths, routing all traffic, including government and military traffic, to about 15 percent of the internet’s destinations through servers located in China.29

In the future, the need to enhance situational awareness in space is likely to lead to further integration of space assets between the US and its allies. Civilian entry points are likely to provide a growing opportunity for infiltration. The weak state of cybersecurity in civilian agencies should also be considered. Chinese military doctrine prioritizes weaponry that targets vulnerabilities in the deployment of US and allied power, such as the use of cyberattacks to disrupt surveillance assets, intelligence networks, and command-and-control systems.30 These threats are significant, since next generation systems, including fighter aircraft, destroyers, and special forces, will not function without access to space communication and space-derived data.

Although European and US allies have indigenous space programs outside the NATO framework, cyber security and outer space would be a useful field for joint explorations of how to divert and manage attacks and identify an agency which can coordinate transatlantic responses to attacks. Allies are embedded in a range of information networks which may be disrupted, giving rise to alliance management concerns emerging from attacks. The lack of red lines regarding behavior in cyber and outer space between the US and its allies on one hand, and adversaries such as China on the other, adds to the risk of misperception and escalation, and hence also highlights the need for allied coordination to avoid starting a war by mistake. An improved NATO dialogue on safeguards and alliance consultation could also assist communication with China on arms control and conflict prevention in cyber and outer space, which is not currently taking place.

Looking to the future, NATO’s success in establishing transatlantic mechanisms for cyber and outer space safeguards and consultation will be crucial to allow NATO a key role in taking on the China challenge in ways that help restore faith in NATO’s credibility as a provider of collective defense in all domains. It will also assist NATO in straddling the chasm between member states prioritizing threats from either China, Russia, the Middle East, or North Africa, since cyber and space threats potentially stem from all of them, and the effectiveness of cyber and space defense mechanisms do not necessarily depend on geographical origin.

Improved communication between NATO and the EU will be essential for NATO to successfully address the military aspects of cyber and space threats. The framework for permanent EU-NATO relations, Berlin Plus, was concluded in March 2003. It allows for the exchange of classified information, the EU’s use of NATO assets and capabilities for EU-led crisis management operations, and the establishment of consultation arrangements.31 Due to disagreements over responsibilities and jurisdiction, however, meaningful coordination did not take place until July 2016. On this occasion, NATO and the EU issued a joint declaration stating their intention to work together on security and defense responses to unprecedented challenges emanating from the South and East of the Euro-Atlantic area.32 During Biden’s visit to Brussels in June 2021, NATO promised to strengthen cooperation with the EU on promoting peace and stability including protecting critical infrastructure, strengthening resilience, maintaining a technological edge, and addressing challenges to a rules-based order.33 The EU-US summit statement from the same visit merely reaffirms support for robust NATO-EU cooperation and promises to strengthen the partnership.34 At the level of policy implementation, it is clear when talking to NATO and EU officials that usually they do not coordinate their strategies and tactics for countering China challenges.35

The EU-US summit statement’s negligible mention of cooperation with NATO indicates that the ball is in NATO’s court if strengthening NATO-EU coordination is to take place. French and German concerns about entrapment are a major barrier to meaningful NATO-EU cooperation. The area of cyber and space security may allow NATO to work around this roadblock. In line with the EU’s practice of supporting the efforts of groups of member states to take the lead on issues where EU institutions cannot trump sovereignty, in the area of cybersecurity the EU has decentralized implementation to work around national resistance. This has allowed the EU to respond collectively and effectively to cyberattacks in Europe, primarily through bolstering capacities and law enforcement cooperation.36 However, the EU is not yet a globally influential and effective cyber-power because differences among member states over issues such as whether to prioritize tech sovereignty or Europe’s global tech competitiveness prevent the EU from acting in unison on the global stage.

The first US-EU TTC meeting held in September 2021 was an important step in strengthening the EU’s global position in cooperation with the United States, and hence called into question whether NATO has a role to play in cyber security.37 The next couple of years will demonstrate whether the EU and the US are able to focus on becoming mutually supportive global cyber security guardians by cooperating on strengthening investment screening, export controls, and rebalance global supply chains in semiconductors. The successful implementation on both sides of the Atlantic of the recommendations of the TTC working groups will determine if transatlantic cooperation positions the US and the EU as global partners in guarding cyber space. In part, this will depend on the EU’s ability to forge common positions that meet the US halfway on issues such as tech sovereignty and data privacy, points of contention through which transatlantic relations have been marred by conflict.

The potential convergence of transatlantic views on cybersecurity leaves room for NATO to play a significant role because the EU is a civilian and economic, rather than military, set of institutions. The NATO summit in Brussels in 2018 carved out a role for NATO which the EU cannot fulfill, allowing NATO members to integrate their sovereign cyber capabilities into NATO operations and missions.38 However, compared to the EU’s major role in cyber, NATO’s role is negligible. As EU civil-military cooperation ramps up in enhancing Europe’s autonomous defense profile while allowing US companies a role in this effort, the union looks set to become an even more dominant actor in transatlantic cyber defense. Because NATO is a military organization, it has the procedures and instruments to position itself in a key role in coordinating and implementing the military aspects of cyber defense between the US and Europe. The multinational cybersecurity effort which is confronting the global threat posed by Chinese state-sponsored cyberattacks involves NATO, the EU, Australia, New Zealand, and Japan, and sets NATO off to a good start in enhancing its profile in countering Chinese challenges to transatlantic cybersecurity.39 However, it remains to be seen if it manages to deliver mechanisms that succeed in integrating allied responses in the military sector in a way that complements US and EU cyber defense initiatives.

In outer space, the EU is also increasingly active, recognizing the need to deepen investments in areas such as satellite navigation, earth observation, space situational awareness, and secure communications, which are all central to enhanced space security. The EU has established the EU Agency for the Space Programme, which has oversight over everything the EU does in orbit as a bloc. Moreover, the EU uses the European Space Agency (ESA) as technical advisor and industrial procurement agent. This setup allows the EU to become more agile, dynamic, and innovative in space as rapid industrialization is taking place with US entrepreneurs and well-funded Chinese space programs in leading roles.40 In the pipeline are a next generation of Europe’s satellite-navigation system, Galileo, and an extension of the scope and capabilities of its Copernicus-Sentinel spacecraft, which monitors the state of the planet. The EU focuses on ensuring that Europe has independent space capabilities, but it does not develop instruments such as space weapons systems.41

In the outer space realm, NATO has tremendous potential for playing a key role in developing instruments in the military sector that involve European and US space capabilities. NATO’s decision to declare outer space an operational domain at the London summit in 2019 is a first step in allowing NATO an active role in addressing growing anti-satellite threats from China and Russia.42 With the US as the leading power in outer space and with the EU developing its space platforms to enhance situational awareness and security, NATO has the tools to work out a common transatlantic definition of the anti-satellite challenges that need to be addressed. The establishment of mechanisms that ensure coordination across military NATO commands regarding intelligence gathering and the interface between cyber and space defense, as well as civilian and military occurrences and initiatives, would potentially strengthen the ability of allies to counter anti-satellite threats considerably. As with cyber, NATO must first integrate the space issue into all its organizational and operational structures, and secondly, develop mechanisms that focus on coordination between US and European capacities on the basis of a common understanding of the challenges to be addressed.

### NATO Link: Cyber Turn—Ext

#### NATO is critical—action thwarts Chinese efforts to undermine the liberal order, shores up weak links in the alliance

Odgaard, Norwegian Institute for Defense Studies Professor, ‘22

[Liselotte Odgaard, Professor, Norwegian Institute for Defense Studies and Non-Resident Senior Fellow, Hudson Institute, “NATO’s China Role: Defending Cyber and Outer Space,” WASHINGTON QUARTERLY v. 45 n., 1, Spring 2022, p. 169-170]

Washington increasingly looks to the EU rather than NATO for guidance on Europe’s future security policy. One reason is that NATO’s toolbox is lagging in domains such as cyber and outer space, although cyber and outer space operations are key enablers of actions in all domains including air, sea, and land. One indication of this is the US-EU negotiations surrounding a common response to cyber threats which took place during the first US-EU Trade and Technology Council (TTC) meeting in Pittsburgh in September 2021. In addition, during Trump’s presidency, longstanding US dissatisfaction with Europe’s modest defense spending threatened to put NATO on the backburner in transatlantic security debates.5 Since then, Russia’s invasion of Ukraine has elicited a sea change in German defense policy with the announcement in February 2022 that defense spending will increase to more than 2 percent of its gross domestic output annually.6 While this may be a convincing signal that Europe will finally devote the resources required for its own defense and revive NATO’s central role in transatlantic security, there is also a risk that China will be moved to the periphery of the alliance’s agenda.

On February 11, 2022, during the runup to the Russian-Ukrainian war, the Biden administration published its Indo-Pacific strategy as US Secretary of State Anthony Blinken was in the midst of a Pacific trip to Australia, Fiji, and Hawaii.7 This US prioritization signaled that despite Moscow’s war in Europe, Washington remains committed to strengthening its presence in the Indo-Pacific and competing with China. If the US drops the ball on the Indo-Pacific, Washington is concerned that China might use force against Taiwan.8 Consequently, the key question for the US is how many resources can be tied up in Europe without losing sight of the long-term goal: deterrence of China. As US strategic competition with China increases while NATO is sitting on the fence, failure to develop a transatlantic defense policy that addresses China will leave Europe vulnerable to China’s ability to exploit the weak links in European defense arrangements, which are newly fragmented by the Russian invasion of Ukraine.

EU efforts to build an independent regional defense profile and nurture cooperation between Europe’s defense industry and national defense communities reflect a growing recognition that the region needs to become a self-reliant defense actor. However, Europe still needs to demonstrate that self-reliance does not imply merely focusing on Europe’s periphery. Otherwise, the industrial challenges from China may outcompete Europe’s defense industry. Shipbuilding is a case in point. By 2021, China built 50 percent of all existing ships in the world. Through design collaboration agreements, cyber espionage, and acquisitions, China has copied advanced innovative ship designs. Enormous financial resources from the state allow Chinese companies to enjoy economies of scale by building dual-use factories which not only outcompete Western companies in the commercial shipbuilding industry, but also threaten the production of navy vessels. If not taken seriously, Europe and the US may soon have no choice but to buy frigates from China.10 This example demonstrates the centrality of China for global economic and security developments and should encourage Europe to manifest a position of unified strength in defending NATO member states against Chinese security challenges. This realization will help convince the US and its adversaries that Europe continues to be a credible partner in countering common threats against transatlantic security, whether they appear in or beyond the European region.

China’s challenges to US and European security constitute such common threats across a broad range of sectors. These include gradual reinterpretations of principles of international law, the subversion of universal liberal market economic practices, and cyber insurgencies targeting a wide range of civilian and military entities. These Chinese policies all have major military implications because they are related to developments in the operating principles, capabilities, and priorities of China’s armed forces. Only NATO can offer an integrated transatlantic response to the military aspects of Chinese policies that threaten those sectors across the globe, including European actors. NATO’s involvement is essential if the credibility of the alliance’s security guarantees is to be preserved and an effective response to China’s encroachments on a liberal rules-based order is to be established.

The omnipresent character of the China threat demonstrates that it is long overdue for NATO to position itself as a significant player in addressing Beijing’s challenges to transatlantic security. NATO is key to keeping US and European security policies coordinated when applying mechanisms of deterrence and defense against Chinese challenges. If transatlantic unity of purpose is lost, both the US and Europe are far less likely to succeed in addressing China sufficiently.

#### NATO coordination enables coalitions of the willing within the alliance to solve the Chinese hybrid threat

Speranza, Cetner for European Policy Analysis researcher, ‘20

]Lauren Speranza, Director, Trans-Atlantic Defense and Security, Center for European Policy Analysis, “China Is NATO’s New Problem,” FOREIGN POLICY, 7—8—20, <https://foreignpolicy.com/2020/07/08/china-nato-hybrid-threats-europe-cyber/>, accessed 5-7-22]

Over the past decade, Chinese companies have invested billions of dollars throughout Europe—buying up critical infrastructure and increasing Beijing’s political clout across the continent. As Chinese firms, often with strong ties to the state and Chinese Communist Party (CCP), acquire parts of sensitive ports, pipelines, and telecommunication networks, China’s incursions into Europe’s security umbrella are drawing serious concern.

But NATO, long worried about Russia, has largely been silent on China. Now, that is changing. NATO Secretary-General Jens Stoltenberg recently called on the alliance to stand up to Beijing’s “bullying and coercion,” underscoring how China’s rise is fundamentally shifting the global balance of power. It’s apparent that NATO can no longer ignore the threat. If the alliance hopes to remain competitive, it will need to develop a new strategy for dealing with Beijing.

First, NATO needs a common assessment of China’s hybrid threats—a mix of diplomatic, economic, security, information, and technological actions designed to quietly undermine democratic states and institutions to Beijing’s benefit while avoiding a traditional conflict. While China’s conventional military threat in the Indo-Pacific is far from NATO’s borders, its hybrid activities are happening in the alliance’s own backyard.

Cyber-espionage, intellectual property theft, infiltration of critical infrastructure, debt manipulation, and disinformation are prime examples. While these threats may seem to fall outside of NATO’s purview, they pose serious security risks for the alliance. For instance, China’s desire to invest in Lithuania’s Klaipeda Port may not look like a problem for NATO on its surface. But its investments have worrying strings attached that give China operating control over the infrastructure. That control could decrease allies’ willingness to move military forces—including sensitive technologies—through the port and its surrounding networks. This could lead to disrupted planning and fewer military exercises, decreasing NATO’s ability to defend the Baltic States during a crisis with Russia. This could also open the door for pragmatic collaboration between China and Russia to undermine trans-Atlantic security.

Allies need to forge a shared understanding of these risks through information-sharing and dialogue—no small feat for countries that do not see eye to eye on China. Some are even willing to ignore such vulnerabilities, due to economic benefits or disenchantment with trans-Atlantic institutions. The United States has a critical role to play in getting allies on the same page and setting common goals for countering China’s hybrid activities.

Second, NATO needs to focus on public diplomacy. NATO has an important role to play in the battle against the CCP’s global narratives, which Beijing promulgates through hybrid activities. To defend the trans-Atlantic values on which the alliance is built—freedom, democracy, rule of law, and human rights—NATO should clearly communicate China’s violations of these principles and its propaganda efforts to cover them up. (These include, among others, human rights abuses against ethnic Uighurs in Xinjiang and violations of the U.N. Convention on the Law of the Sea in the South China Sea.) NATO should also enhance its outreach to key partners in the Indo-Pacific, such as Australia, Japan, New Zealand, and South Korea, which can serve as important counterweights to Chinese influence in the region. Effective public messaging also means getting serious about attributing the blame for attacks, as the European Commission recently did over Chinese disinformation around COVID-19, to raise the pressure on Chinese officials. Trans-Atlantic countries have struggled to shape China’s behavior because they cannot prove malign intent or agree to call out Beijing for its subversive efforts. Allies should develop clearer guidelines—what needs to be proved, by whom, and to what degree—to enable collective attribution. NATO is strongest when it speaks with one voice. It should use that voice to demand transparency and change from China.

Third, the alliance should step up its counteroffensive. China’s hybrid actions intentionally blur the lines between what is legally permissible, politically inappropriate, and downright escalatory.

This makes it difficult for leaders to determine appropriate responses, producing a reactionary approach thus far. But an intensifying geostrategic competition has already begun. To compete in this environment, the trans-Atlantic community needs a more proactive approach. Rather than waiting for China to invest in the next major European port, allies should coordinate legislation to prevent the riskiest Chinese acquisitions. And rather than waiting for more Chinese cyberintrusions, allies should collaborate on responsible, targeted offensive cyberactions. Over time, this would help dissuade China from manipulating investments in critical infrastructure, conducting cyber-espionage, and other hybrid activities. While adopting a more offensive posture remains controversial among certain allies, it is gaining traction across Europe and is strongly supported in Washington. Although NATO, as a defensive alliance, should not implement such a counteroffensive, policymakers should leverage it as the primary forum to coordinate actions among willing nations.

Fourth, NATO needs to deepen its cooperation with other key players, such as the European Union and the private sector. Where NATO lacks the mandate and means, the EU and multinational businesses play critical roles in developing, implementing, and enforcing the legislation and financial incentives necessary to counter Chinese hybrid threats. Complementary to that, NATO and its allies can focus on providing intelligence, defending cyberspace, developing capability targets for new technologies, conducting exercises and contingency planning, informing resilience requirements for secure infrastructure, and bolstering deterrence. Despite the political obstacles that impede more formal NATO-EU cooperation, allies should look to the European Centre of Excellence for Countering Hybrid Threats in Helsinki to bring together NATO and EU staff, national officials, and industry voices in one place to align their counter-hybrid policies for China.

The Chinese government’s manipulative efforts around the coronavirus have thrust China’s hybrid activities to the center of trans-Atlantic debates. Policymakers need to seize the moment and respond by “using NATO more politically,” in Stoltenberg’s words. NATO is first and foremost about its nations. In the fight against China’s hybrid threats, these nations bring much more to the table than military power alone. They have access to a broad range of tools—military, political, economic, technological, and information—which the alliance can use to its collective geopolitical advantage in the competition with China. What NATO needs now is a strategy to leverage those tools in a coordinated manner. That will go a long way in solving NATO’s China problem.

### NATO Link: Deterrence Turn—2AC

#### [x] Resilience enhances deterrence

Prior, Center for Security Studies researcher ‘18

[Tim Prior, Head, Risk and Resilience Research Team, Center for Security Studies (CSS) and PhD, Social and Environmental Psychology, University of Tasmania, “Resilience: The ‘Fifth Wave’ in the Evolution of Deterrence,” STRATEGIC TRENDS 2018: KEY DEVELOPMENTS IN GLOBAL AFFAIRS, Ed. O.Thränert & M/ Zapfe, Center for Security Studies, 2018, p. 77-78]

Resilience thinking and being resilient can offer concrete advantages in security policy, and specifically in deterrence. Applied resilience is becoming the cornerstone of security policy, and represents the fifth wave of deterrence.

Modern threats are complex, multiactor, cross-scale problems, which must be met with agile, resilience thinking-style institutional decisionmaking that fits the nature of the problems. Proactively countering complex threats with equally networked and distributed policy responses, guided by resilience, will improve the effectiveness of those security policies. In this context, the increasing resilience of society, critical infrastructure, and organizations – the product of a decade of resilience promotion in security policies – and the concomitant reductions in vulnerability will deter asymmetric threats by denying threatening actors suitable targets for their attacks.

Where classical (nuclear) deterrence was hierarchical and deterministic, based on the known relationships between the actors, and on the simple and well-understood principle of assured destruction, which held the actors in check, modern deterrence is altogether different. Threats are uncertain, and unpredictable; actors are unknown, as are the vulnerabilities they target. As threats have become less state-centered, and more likely to originate from distributed networks, the means of addressing these threats must also change.

The fifth wave of deterrence development is rising at a point when established international security practices are fumbling to respond effectively to security challenges. Resilience thinking presents a potential breakthrough that can increase the ability of established security institutions to improve their links and address complex threats deliberatively. If institutions can accept the current shift toward resilience as an important and practical one, then the “complex adaptive system” of international security is more likely to meet future system changes or disruption in a more prepared state. The fifth wave of deterrence will be characterized by the network-driven, tailor-made solution.

Deterrence is an uncertain art, not a science, and if the decision-making processes that determine deterrence actions do not match the problems, it is unlikely that practical deterrence solutions commensurate to modern threats can be identified and deployed.

Modern approaches to national and international security are already built on networks, but control tends to remain hierarchical and linear. Dealing with complex threats highlights the necessity to move away from traditional reductionist and hierarchical approaches to problem governance, and to engage existing networks with distributed and deliberative approaches.

To a certain degree, policy failures must be accepted as inevitable in a complex, uncertain, and unpredictable security environment. But policy failures will be more likely if policymaking processes are not suited to this current security environment. If policy processes are deterministic, reductionist, and hierarchical, then they are not suited to governing systems that are characterized by nonlinearity, unpredictability of interactions, and uncertain feedbacks. By contrast, if policy processes are designed to match the complex systems and problems they are attempting to govern – i.e., if they are flexible, reactive, and distributed – then they are likely to be more successful.

### NATO Link: Deterrence Turn—Denial

#### Resilience boosts deterrence—by denial

Pernik & Jermalavičius, International Centre for Defence & Security analysts, ‘16

[Piret Pernik and Tomas Jermalavičius, Research Fellows, International Centre for Defense and Security “Resilience as Part of NATO’s Strategy: Deterrence by Denial and Cyber Defense,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. 102]

In broader strategic terms, resilience can be seen as an ingredient of deterrence by denial,or “persuading the enemy not to attack by convincing him that his attack will be defeated—that is, that he will not be able to achieve his operational objectives.”9 Hybrid warfare strategy—essentially a strategy aiming to cause disruption, confusion, destabilization and paralysis (i.e., shape the behavior of a target nation)—can be countered by demonstrating that all those aims are beyond reach due to the target’s resilience. For instance:

• A high level of a society’s competence in critical thinking and in understanding the nature of such hybrid warfare tools as hostile propaganda,political extremism,social protest campaigns or military intimidation—in conjunction with society’s trust in the integrity of the political system, political leadership and government’s communication—negate the advantages of those tools.

#### Resilience strengthens deterrence by denial

Roepke & Thankey, NATO’s Defence Policy & Planning Division ‘19

[Wolf-Diether Roepke and Hasit Thankey, Resilience and Civil Preparedness staff, Defence Policy and Planning Division, NATO, “Resilience: The First Line of Defence,” NATO REVIEW, 2—27—19, <https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html>, accessed 6-3-22]

More resilient countries – where the whole of government as well as the public and private sectors are involved in civil preparedness planning – have fewer vulnerabilities that can otherwise be used as leverage or be targeted by adversaries. Resilience is therefore an important aspect of deterrence by denial: persuading an adversary not to attack by convincing it that an attack will not achieve its intended objectives.

Resilient societies also have a greater propensity to bounce back after crises: they tend to recover more rapidly and are able to return to pre-crisis functional levels with greater ease than less resilient societies. This makes continuity of government and essential services to the population more durable. Similarly, it enhances the ability for the civil sector to support a NATO military operation, including the capacity to rapidly reinforce an Ally.

Such resilience is of benefit across the spectrum of threats, from countering or responding to a terrorist attack to potential collective defence scenarios. Consequently, enhancing resilience though civil preparedness plays an important role in strengthening the Alliance’s deterrence and defence posture.

### NATO Link: Deterrence Turn—Ext

#### Resilience thinking is vital to adapt deterrence to modern threats

Prior, Center for Security Studies researcher ‘18

[Tim Prior, Head, Risk and Resilience Research Team, Center for Security Studies (CSS) and PhD, Social and Environmental Psychology, University of Tasmania, “Resilience: The ‘Fifth Wave’ in the Evolution of Deterrence,” STRATEGIC TRENDS 2018: KEY DEVELOPMENTS IN GLOBAL AFFAIRS, Ed. O.Thränert & M/ Zapfe, Center for Security Studies, 2018, p. 72-74]

The nature of deterrence is facing a phase shift, driven by the multifaceted and complex nature of the modern threat landscape. Realistically, deterrence must be a flexible and proactive occupation, composed of elements that should suit the nature of the threat. The notion of “tailor-made” deterrence begins to address the complexity of modern threat by attempting to introduce a more detailed understanding of the complex threat situation in order to direct a customized response.21

Resilience thinking can be a powerful means of guiding the development of an adaptive tailor-made deterrence approach. The national-international security landscape is illustrated as two interacting “Complex Adaptive Systems” on page 73. The international and national systems interact and respond to one another as they develop and change.22 Within this system, information and control is multidirectional, flowing between the systems – a state of affairs that has been described as “panarchy”.23 This is in contrast to a typical hierarchical system, where control is exerted in a unidirectional manner. Complex human, socio-technical, and human-ecological systems are arranged as panarchies – as systems that feature nested components, open information flow, and constant change. No element in these systems can be thought of as the ultimate point of control.24

Given the complex threat environment, non-hierarchical decision-making processes, like resilience thinking, are particularly suitable because they match the non-hierarchical nature of the challenge to be solved. The ability of decision-makers to embrace emergent opportunities and adapt quickly is imperative. While this ability has always been important, it is the diversity in the current threat landscape that is currently pushing the deterrence phase shift from a hierarchical and deterministic mindset to a networked, non-linear, and deliberative mindset.

#### Resilience adapts deterrence logics to current threats

Prior, Center for Security Studies researcher ‘18

[Tim Prior, Head, Risk and Resilience Research Team, Center for Security Studies (CSS) and PhD, Social and Environmental Psychology, University of Tasmania, “Resilience: The ‘Fifth Wave’ in the Evolution of Deterrence,” STRATEGIC TRENDS 2018: KEY DEVELOPMENTS IN GLOBAL AFFAIRS, Ed. O.Thränert & M/ Zapfe, Center for Security Studies, 2018, p. 74]

Resilience as a Credible Form of Deterrence?

The credibility of resilience as a deterrent option is closely connected to the utility of resilience thinking in the context of complex threats. Resilience is practical under these circumstances because it shifts the focus from preventing complex and diverse threats to mitigating the consequences of these threats through proactive anticipation, preparation, and adaptation. The new complexity of threats (including terrorist, hybrid, and cyber-threats) is disrupting traditional deterrence approaches.

These points speak to the utility of resilience as a deterrent option in complex threat situations. However, like any other deterrent option, resilience must be credible. Given the nature of deterrence as a psychological strategy disruptor, for resilience to be a credible option it must meet three criteria that are typical of all forms of deterrence: commitment, capability, and communication.

The trend towards committing to resilience in security policy is a strong one. Given that there has already been a reasonably long focus on resilience at national and sub-national scales in the contexts of civil protection, critical infrastructure protection, disaster risk management, public preparedness, and risk communication,25 systematically scaling up resilience as a national or international security policy priority will clearly demonstrate a real commitment to resilience in deterrence.

Capability can be established through coherent and systemic development of the practical actions that together contribute to building resilience. These might include establishing comprehensive and multi-thematic vulnerability assessments; describing resilience in multiple contexts, finding commonalities; establishing measurement tools and processes; encouraging flexibility within security organizations to improve the ability to learn, adapt, and respond; and investing in developing coherent practices across security themes and sectors.

#### Ukrainian resistance proves the effectiveness of resilience strategies

Hall & Sandeman, London School of Economics researchers, ‘22

[Jonny Hall, PhD Candidate, International Relations, London School of Economics and Political Science and Hugh Sandeman, Visiting Senior Fellow, LSE Ideas and Project Head of Global Strategies, “NATO’s Resilience: The First and Last Line of Defence,” Strategic Update, LSE IDEAS, 5—22, London School of Economics p. 5]

The determined resistance by Ukraine’s armed forces and civil society against the Russian invasion that began in February 2022 is a vivid demonstration of the central importance of military and societal resilience in the face of external shocks. Civil and military preparedness may help save Ukraine as an independent country. Had Moscow understood more clearly the ability of Ukraine to resist Russian military advances and maintain its sense of national purpose, the Kremlin may have been deterred from launching the invasion.

The war in Ukraine adds further urgency to updating NATO’s thinking about the resilience of alliance members, which will be reflected in the June 2022 Strategic Concept. Resilience in the face of armed attack is a fundamental commitment of NATO’s 1949 Treaty, with Article 3 stating that parties to the treaty will “separately and jointly, by means of continuous and effective self-help and mutual aid … maintain and develop their individual and collective capacity to resist armed attack”.

#### Resilience is a necessary component of deterrence, even if it is not alone sufficient

Kersanskas, Hybrid CoE researcher, ‘20

[Vytautas Kersankas, Deputy Director, Community of Interest on Hybrid Influence, Hybrid CoE, “Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats,” HYBRID COE PAPER 2, Hybrid Centre of Excellence, 3—20, p. 7]

The discussion on how to counter hybrid threats frequently concentrates on two response options. The most common proposal for countering hybrid threats is resilience building. The logic is clear: every state should seek to achieve social coherence and awareness, secure critical infrastructure and transparent and open political systems, thus making it harder for hostile actors to intervene effectively. Resilience also has considerable second order benefits, protecting states from threats like natural disasters or industrial accidents.

Recent years have shown that even the most developed and resilient states are dealing with challenges emanating from the hostile activities of state and non-state actors. Resilience makes it harder, but not impossible, for hostile actors to cause harm by hybrid means. Even though resilience should be at the core of the response to hybrid threats and plays an important part in deterrence, resilience building alone is not sufficient.

The other end of this debate circles around the immediate response to an unfolding hybrid operation. It is straightforward to learn from cases where the evidence of hostile activities is visible to everyone and the response needs to be immediate and swift. In these scenarios, the disruption has already happened, the damage is done, and so the hostile actor has at least partly achieved its intended goal.

This paper suggests that deterrence theory, one of the key pillars of both post-World War 2 and post-Cold War security architecture in the West, could be applied to counter hybrid threats. This approach turns on its head the challenge at the heart of countering hybrid activity – the assertion that hybrid activity cannot be countered until it manifests itself. The paper suggests that effective deterrence blends resilience and crisis response with the ability to impose costs on hybrid aggressors. It shifts the operational model from responsive to preventive, creating a forward looking and strategic approach.

### NATO Link: Tech Focus Good

#### NATO must focus on emergent tech – part of threat environment now

Keil, Senior Fellow, Security and Defense Policy GMF, 2022

[Steven, German Marshall Fund - non-partisan policy organization studying transatlantic interests “NATO Core Tasks in a Contested Global Landscape” German Marshall Fund February 11, 2022 [https://www.gmfus.org/news/nato-core-tasks-contested-global-landscape GDI-TM 6.16.2022](https://www.gmfus.org/news/nato-core-tasks-contested-global-landscape%20GDI-TM%206.16.2022)]

New challenges unconsidered a decade ago are also growing in speed and scope. NATO has no choice but to bolster its engagement in domains like cyber and space that will have a considerable impact on deterrence. Furthermore, massive shifts caused by climate change are challenging the security of NATO members and could create crises in which they will be required to respond. New technologies are creating novel ways to undermine the resilience of national infrastructures and democratic processes, threatening the core of Euro-Atlantic societies. However, technologies, like artificial intelligence, may also help in operational settings and decision-making, or help identify multi-domain hybrid operations. There are challenges and opportunities in these emerging technologies, and they will require added investment and engagement by NATO and its members.

### NATO Impact: China—NATO Focus Bad

#### Focusing on China fractures the alliance and undermines its ability to deter Russia

Coffey & Kochis, Heritage Foundation analysts, ‘20

[Luke Coffee, Heritage Foundation institute director and Daniel Kochis, Senior Policy Analyst, Davis Institute, Heritage Foundation, “NATO in the 21st Century: Preparing the Alliance for the Challenges of Today and Tomorrow,” SPECIAL REPORT n. 235, 8—10—20, p. 17-18]

Individual NATO member states, and even the supranational EU with its particular policy competencies, have more tools to deal with an emboldened China than does NATO as an institution. NATO can deepen its existing engagements with Indo-Pacific countries. This will ease cooperation with these governments and militaries in the future and strengthen them (marginally) against Chinese encroachment. It may also contribute to the governments involved reaching common diplomatic positions, on freedom of navigation for instance. Until China poses a military threat in the North Atlantic Region, as an institution created for the purpose of collective security, NATO should have a very limited role when it comes to dealing the challenges posed by Beijing.

The reflection period offers NATO an opportunity to state clearly what its responsibilities are when it comes to China, and what its approach will be. To ensure that NATO does not lose focus on actual military threats closer to home it must:

\* Acknowledge the Alliance’s limitations when confronting some of China’s non-military threats and push member states to do more. Some of the biggest challenges posed by China to NATO’s member states deal with investments in critical infrastructure, disinformation campaigns, and encroachments in the technology sector using Huawei’s 5G. NATO should not pretend to lead on an issue for which it lacks the needed policy competencies. Therefore, while policymakers should look to NATO to provide a robust conventional and nuclear deterrence for members of the Alliance, only the national capitals, and in some cases the EU, have the political and economic tools that can reduce the economic and political threats posed by China.

\* Not let itself be distracted. With the BRI creeping inside Europe’s borders, the fallout of the COVID-19 pandemic, the mass internment of the Uighur population, and the ongoing 5G debate in Europe, it is no surprise that China is a major concern for Western policymakers—and rightfully so. However, for NATO, the most immediate threat, and the threat for which it was created and for which it has the tools, is Russia. NATO should focus first and foremost on this threat.

\* Be realistic about the military threat facing the Alliance in the North Atlantic area. At the time of this writing, Russian–Chinese military activity in NATO’s area of responsibility as described in Article 6 of the North Atlantic Treaty has amounted to two different exercises, spanning a total of 13 days, consisting of a total of six PLAN ships over the course of the past five years. While NATO should monitor Russian–Chinese military cooperation, the Alliance must recognize that its number one priority is Russia.

\* Not let China divide the Alliance. As seen in the single sentence devoted to China in NATO’s joint statement, there is no agreement inside the Alliance on what role, if any, NATO should play in dealing with Beijing. When Alliance unity in the face of Russian aggression is vital, now is not the time for NATO to divide itself over the issue of China. This only benefits Moscow and Beijing.

Ensure that NATO remains a nuclear alliance. China is a nuclear power with strategic reach. The threats associated with nuclear proliferation make the world more dangerous today than it was during the Cold War, making it critical that NATO maintain its “nuclear culture.” As long as the West could face a nuclear threat from any part of the world, including Asia, NATO needs to remain a nuclear alliance.

Encourage the member states to coordinate a military strategy toward China. While NATO as an institution should limit its military focus on China, for certain member states, China is a main driver of foreign and defense policy. This is particularly true of the U.S., and to a lesser extent, Canada, France, and the U.K. Military training exercises in the Indo–Pacific, or Freedom of Navigation Operations in the South China Sea, should be coordinated on a multilateral or bilateral basis at the member-state level.

### NATO Impact: China—NATO Not Key

#### NATO not key to checking China – focus on Russia, allies do not want to get involved

Haroche and Quencez, 2022

[Pierre Haroche Research Fellow in European Security at the Institute for Strategic Research (IRSEM, Paris) & Martin Quencez, Research Fellow and Deputy Director of the Paris office of the German Marshall Fund of the United States“NATO Facing China: Responses and Adaptations” Survival 64:3, 73-86, DOI: 10.1080/00396338.2022.2078047 accessed TANF online – UT 6.16.2022 GDI-TM]

These efforts are clearly intended to be part of a comprehensive assess- ment of the challenges posed by China. Nevertheless, such a broadening of transatlantic security thinking may be constrained by NATO’s geographic and functional limitations, or by the reluctance of certain member states to embed this kind of political dialogue in the NATO framework. Certainly, NATO is a well-established forum in which European and North American representatives already meet regularly. Among its members, the United Kingdom, having just left the EU, would likely be interested in a politi- cally strengthened NATO that holds ministerial meetings beyond defence issues, notably economic ones.26 However, when it comes to conducting a broader political reflection on China, NATO finds itself in competition with other frameworks, some of which directly include Indo-Pacific powers (the Quadrilateral Security Dialogue, AUKUS, the G7), while others possess a more varied range of instruments in the economic and technological fields, such as US–EU bilateral exchanges (examples of which include the Trade and Technology Council and the Security and Defence Dialogue). Some member states, primarily France, are determined to defend the EU’s prerogatives and are reluctant to see NATO go beyond its original role. The Russian inva- sion of Ukraine may help in clarifying the respective roles played by NATO and the EU in European security, as NATO is clearly refocusing on its core task of collective defence, putting other issues on the backburner.

#### Despite connection between China and Russia threat, US doesn’t view NATO as necessary to combat the threat beyond collaboration with other allies

Haroche and Quencez, 2022

[Pierre Haroche Research Fellow in European Security at the Institute for Strategic Research (IRSEM, Paris) & Martin Quencez, Research Fellow and Deputy Director of the Paris office of the German Marshall Fund of the United States“NATO Facing China: Responses and Adaptations” Survival 64:3, 73-86, DOI: 10.1080/00396338.2022.2078047 accessed TANF online – UT 6.16.2022 GDI-TM]

NATO in the Indo-Pacific

NATO could free itself from its North Atlantic anchorage so that it can contribute directly to military balancing efforts vis-à-vis China in the Indo- Pacific. The logic of this option is primarily political: since China has become the priority of US security policy, NATO, in order to remain attractive to the Americans, cannot avoid updating its own priorities. Moreover, European allies are highly dependent commercially on sea lanes of communication in the Indo-Pacific, notably the Malacca Strait and the China Sea, and therefore have an interest in preventing Chinese hegemony in the region.

Not only would most European states be hard-pressed to provide substantial military capabilities in East Asia, the vast majority would be politically hostile to the idea of getting involved militarily in the region through NATO. French President Emmanuel Macron, for example, appeared to dismiss this option when, just days before NATO’s June 2021 Brussels Summit, he said, ‘As far as I am concerned, China is not part of the Atlantic geography, or there is something wrong with my map.’5 Some states, such as France and Germany, are opposed to taking a belligerent stance against Beijing; others, such as the Central and Eastern European countries, while often eager to meet US expectations, want to preserve NATO’s focus on the Russian threat. The United States is particularly attentive to this issue, and US diplomats have repeatedly stated that China will not draw attention away from other security challenges within the Alliance. The war in Ukraine has reaffirmed the importance of collective defence against Russian actions, for example.6 Rather than contrasting the risks posed by Russia with those posed by China, Washington emphasises their concomitance, and the need to strengthen solidarity among transatlantic and trans-Pacific allies.7 This concomitance was illustrated by the Sino-Russian joint statement of 4 February 2022, in which both countries committed to deepening their strategic partnership.8

In this context, the US does not seem genuinely interested in redefin- ing the Alliance’s geographic priorities, but rather wishes to emphasise the implications of Chinese actions for security and stability in the North Atlantic area. While Washington would like to see better oversight of allies’ various freedom-of-navigation operations in the Indo-Pacific, particularly in the China Sea, NATO involvement is not seen as a priority.

Finally, the recent launch of the AUKUS partnership by Australia, the United Kingdom and the United States illustrates an American preference for ad hoc military coalitions in the Indo-Pacific rather than NATO mobi- lisation.9 For the US, NATO allies are second-tier partners when it comes to China. The top priority is cooperation with regional actors, particularly Australia and Japan. In this context, US expectations are limited to possible support from European allies for partnerships or initiatives that would be led and driven by the Indo-Pacific powers.

### NATO Impact: China—No Resource Tradeoff

#### NATO cannot free up resources

Haroche and Quencez, 2022

[Pierre Haroche Research Fellow in European Security at the Institute for Strategic Research (IRSEM, Paris) & Martin Quencez, Research Fellow and Deputy Director of the Paris office of the German Marshall Fund of the United States“NATO Facing China: Responses and Adaptations” Survival 64:3, 73-86, DOI: 10.1080/00396338.2022.2078047 accessed TANF online – UT 6.16.2022 GDI-TM]

A transatlantic division of strategic responsibilities

A third option would be to acknowledge the transatlantic gap in terms of threat perceptions and geostrategic priorities. If China is the main adver- sary of the United States while remaining merely a ‘challenge’ for European partners focused on more immediate threats, why not divide strategic responsibilities between the US and its European allies? American forces, especially US maritime and air forces, would focus more on the Indo-Pacific, while Europeans would strengthen their capabilities to ensure the security of their own region. In this way, Europe would contribute to American efforts in the Asia-Pacific by making it easier for Washington to free up capabilities and accelerate its ‘pivot’ towards Asia. Similar solutions have been mooted since 2014, when NATO was simultaneously confronted with the Russian threat to the east and the terrorist threat to the south.15

For the United States, ‘rebalancing the strategic burden’ in this way implies that the European states will take on greater responsibility within NATO while the US places limits on its contributions to European securi- ty.16 Thus, the Biden administration’s Interim National Security Strategic Guidance, released in March 2021, encourages allies ‘to invest in their own comparative advantages against shared current and future threats’.17 However, the Biden administration refuses to talk about a division of labour because it does not consider transatlantic cooperation to be a zero-sum game. While competition with China may require a rethinking of US defence priorities, it does not require an American withdrawal from Europe. The Global Posture Review presented by the Pentagon to President Joe Biden in November 2021 reinforces the US military presence and capabilities in Europe, illustrating Washington’s intention to maintain a predominant role in the security of the continent.18 More recently, President Biden reacted to the Russian invasion of Ukraine by deploying additional troops from the United States to Europe. Neither the White House nor Congress, which votes on the budgets of the Pentagon’s European Deterrence Initiative, have questioned the benefits of the United States’ commitment to Europe.

Moreover, many Central and Eastern European member states would see any policy that would facilitate, even indirectly, the departure of American troops from Europe as disastrous. More generally, European allies would be unable to replace US capabilities on the continent in the immediate future.19 Above all, the very logic of a division of labour seems contra- dictory to that of an alliance: if allies act separately in pursuit of distinct, albeit complementary, objectives, can their efforts still be characterised as collective? In the long run, does this approach not risk undermining the foundations of Article 5, according to which an attack against one member is an attack against all?

# Resilience Aff: Security K Ans

## Framework

### Policy Simulation Good

#### Policy simulation provides a template for studying human interactions – even if it doesn’t solve conflict, it helps break down impulses which characterize both interpersonal hostility and global war

Earle 86 [Professor of Psychology, The Ohio State University. International Relations and the Psychology of Control: Alternative Control Strategies and Their Consequences. Political Psychology, Vol. 7, No. 2 (Jun.,1986), pp. 369-375. https://www.jstor.org/stable/pdf/3791131.pdf]

Research into the psychology of control has revealed that control needs are key elements of individual psychological functioning. **This paper** argues that a “need for control’’ framework is also useful for understanding actions and ideologies at the national and international levels. It **critically analyzes prevalent strategies for** exerting control in this domain **and proposes alternative strategies which permit greater fulfillment of control needs**. **These alternatives emerge from an** examination **of** potential similarities **between** satisfaction of control needs **within** the separate **but** parallel domains **of** international relations **and** interpersonal relations. **Political psychology has the potential to** translate **issues of** i**nternational** r**elations** **into the** terms **of** human interpersonal encounter. In my view, **such a translation** enhances **our** ability **to** think creatively about the current world situation. The **students in my** freshman psychology **course** recently surprised me by adopting this approach for an in-class assignment. **I** had **asked** **them to** role-play **a** negotiating **session between the** U**nited** S**tates and the** Soviet Union **on the issue of** arms control. My assumption had been that they would act out the roles of political leaders on both sides, and would proceed by exchanging official positions on arms control issues. Instead, **they took the viewpoint of ordinary Ameri-can and Soviet citizens and exchanged candid remarks** concerning their feelings about the nuclear danger. Their tone of earnest sincerity was in stark contrast to the kind of elaborate posturing, deceitfulness, and strategic “positioning” that usually characterizes this kind of endeavor at the diplomatic level. Having translated the arms race into its smallest constituent parts—the feelings of individual Soviet and American citizens—they had stripped away the layers of pretense and revealed the rigidly arbitrary nature of their country’s “party line.” After the role-play had ended, the students pressed me to admit that, if the political and military leaders on both sides were removed from the picture, much of the current conflict between the two countries could be settled by a consensus of common citizens from both sides. It only occurred to me later that, regardless of the practicality of their solution, my class had arrived at it by a highly unusual means: **They had asserted that the** problems **were** amenable to human control **by acknowledging their own** individual human reactions **to the dangers of continued** international confrontation. I choose to focus here not on the solution my students proposed but on the impulse behind their proposal. The need expressed by these students to render these issues “controllable” in some fashion is a basic one. Perhaps an examination of this need, and the more vs. less healthy ways it can be satisfied, holds the key to a novel approach to international relations. The concept of a “need for control” has recently received much attention within the field of psychology. The belief that one can exercise control over one’s outcomes is said to be critical to psychological well-being (Glass and Singer, 1972; Langer, 1983; Seligman, 1975; Wortman and Brehm, 1975). Research has shown that the negative consequences of a stressful event on physical and mental health can be overcome by a sense of control—i.e., a belief in one’s ability to cope with (respond effectively to) the event (Anderson, 1982; Langer and Rodin, 1976; Perlmuter and Monty, 1979; Weiss, 1972). The accumulating body of research in this area has promising applications for the restoration and maintenance of psychological health in a wide range of human environmental settings. To date, feelings of control have been studied as an attribute of individual psychological functioning. However, the recent work of Fred Rothbaum and John Weisz and their colleagues (Rothbaum et al., 1982; Weisz et al., 1984) suggests that a “need for control” analysis may also be useful for understanding the functioning of individual nations within the international arena. Rothbaum et al. distinguish between primary and secondary forms of control. Primary control is the ability to enhance one’s rewards by doing something to influence existing realities (e.g., other people, circumstances). In secondary control, rewards are obtained by accommodating to existing realities and maximizing satisfaction with things as they are. In other words, people attempt to gain control not only by bringing the environment into line with their wishes (primary control) but also by bringing themselves into line with environmental forces (secondary control). Weisz et al. argue that cultures differ in the extent to which they emphasize primary vs. secondary forms of control. They conclude that the proper relation between the two forms of control involves a dynamic interplay between them, and warn that too heavy an emphasis on either primary or secondary control may be maladaptive for cultures as well as individuals. Extending the logic of Weisz et al. to the realm of international relations, it can be assumed that citizens **and** policymakers alike **define the** requirements **of** national self-interest **in somewhat the** same terms **they use to evaluate their own** individual sense of well-being. For example, there is widespread agreement that a key element of a “healthy” American psyche is a sense of national potency (“primary control,” in our terms) in the international arena. Ronald Reagan’s Presidency has been lauded by both supporters and detractors for its “restoration” of this sense of control after the “humiliating” decade of the 1970s—a legacy of Vietnam, the oil embargo, and the Iranian hostage crisis (cf. Yankelovich, 1982). Whether or not such a felt sense of control (or lack of same) would be sustained by an objective appraisal, it is nonetheless real if it has real consequences for domestic political priorities and foreign policy actions. Given the present context of international relations, is an enhanced sense of control by one nation purchased at the expense of diminished control by other nations? [The Weisz et al. analysis does not attempt to address this key issue.] Under what conditions can this zero-sum notion of control be overcome? If the attainment of a sense of control is indeed an important objective within the world community, then these questions are critical. **The answer may lie in exploring** alternative strategies **for attaining** primary control. For example, **the prevailing strategy requires nations to** maximize their power **vis a vis** potential adversaries. **Yet the** sense of control **thus attained is** always tenuous, **because** (a) **the tech**nological **basis for maintaining** such **relative power may be eclipsed by breakthroughs** on the other side, (b) such technology is subject to dissemination to third parties, thus diluting the power of its former owners, and (c) power that involves the domination of one nation by another (either directly or through surrogates) is bound to be resisted by those subject peoples whose own needs for control have been thwarted. Numerous examples attest to the existence of these needs (under the guise of “nationalism” and “self-determination” or “revolution” and “rebellion”—depending on the orientation of the describer) as a continued source of frustration for the great powers in their attempts to maintain the stability of client states. **Faced with these difficulties of asserting primary control, both the** U**nited** S**tates and the** Soviet Union **have come to rely heavily on** a form of secondary control that Weisz et al. refer to as interpretive control. **This is the attempt to** interpret events **so as to** derive **a sense of** meaning and purpose **from them**. In the current great power struggle, **this assumes the form of** rigidly ideological beliefs **about the** nature **of the** “other side’’ **and the** necessity **of** continued struggle. **It allows** individual persons **and** actions **to be** subsumed **under a** “grand scheme” **of impersonal global forces** (e.g., “good” vs. “evil”). The interpretive route to control works to the extent that it provides a reassuring sense of order and predictability. However, **this** unifying vision **is** purchased **at the** expense **of an** empirically based analysis **of what the** rest of the world **is doing and** why. Reality is distorted **to fit the** dichotomy of rightness (on one’s own behalf) vs. transgression. The selective “management” of information about foreign policy successes vs. failures is essential to this enterprise [the U.S. invasion of Grenada provides a recent example; see e.g., Middleton (1984) and Nelson (1983)]. Unfortunately, such selective information-gathering seriously impairs foreign policy. Numerous authors have described occasions on which great powers have become the captives of their own over-simplified world views (e.g., Didion, 1983; Tuchman, 1984; Sick, 1985). Extended use of this secondary control strategy requires a blurring of the distinction between international politics and fiction. The Soviet Union does not enjoy a monopoly in this regard. Within the last year, the Vietnam War veteran has been resurrected as an American hero, and American audiences have eagerly imbibed his cinematic revenge against the North Vietnamese in “Rambo,” “Missing in Action,” and their television counterparts. A related phenomenon is the president’s identification with the on-screen personas of fellow actors Clint Eastwood and Sylvester Stallone, whose adherence to simplified credos belie the gnawing complexities of value choices in the real world. Such reactions are likely not unique to Americans or to their current president. Instead, they are symptomatic of the frustrations incurred by nations who have failed in their attempts to exert active control over world events. The control needs themselves are legitimate; the strategies that are currently employed for satisfying those needs are not. Use of such measures guarantees that the cycle will repeat itself—i.e., that unrealistic thinking and erroneous judgment will serve as the basis for future foreign policy actions. The question remains: If the nations of the world cannot afford continued reliance on such an ineffective (and unbalanced) “mix” of control strategies, what are the alternatives? As suggested above, the answer lies in exploring alternative conceptions of “control.” Rather than conceiving of control as a subject-object relationship, in which the “object” is a fixed quantity (of land, resources, subject populations) to be apportioned among contending powers, one could instead consider it in the context of a subject-subject relationship, a dy-namic system in which control needs are realized by the exercise of mutual influence. **An** analogy **between the realms of** international relations **and** interpersonal relations **may serve to illustrate this distinction**. **In a** personal relationship **that is** subject-object-based**, each party has a** mutually exclusive sphere **of** self-interest (“turf”) **to be protected**; **the** relationship **must be** negotiated **on the basis of how much turf each party will cede to the other in exchange for similar consideration**. **A** failure of negotiation **may lead to** unilateral attempts **by either/both parties to grab some of the other’s turf**. “Compromise” **and** “confrontation” **thus** define **the parameters of this type of relationship**. Alternatively**, a personal relationship may be** subject-subject-based**, to the extent that the relationship is not primarily directed toward the issue of sharing vs. hoarding** (of a separate domain of self-interest) **but rather toward a redefinition of self and self-interest in terms of the relationship**. **Satisfaction** in such a relationship is not derived from the amount of turf seized from, or conceded by, the other party. Instead it **obtains from the opportunity to exert positive influence over the other’s outcomes**, and in turn to be the beneficiary of the other’s positive consideration and favorable regard (cf. Kelley, 1979; Kelley and Thi-baut, 1978).

#### Policy simulation is good – promotes action and can’t solve without politics

Hodson 10 [Derek, professor of education – Ontario Institute for Studies @ University of Toronto, “Science Education as a Call to Action,” Canadian Journal of Science, Mathematics and Technology Education, Vol. 10, Issue 3, p. 197-206]

**The** final (fourth) level of sophistication in this issues-based **approach is concerned with students findings ways of putting their values and convictions into action, helping them to prepare for and engage in responsible action, and assisting them in developing the skills**, attitudes, and values **that will enable them to** take control of their lives, **cooperate with others to bring about change**, **and work toward a more just and sustainable world in which power, wealth, and resources are more equitably shared.** Socially and environmentally responsible behavior will not necessarily follow from knowledge of key concepts and possession of the “right attitudes.” As Curtin (1991) reminded us, it is important to distinguish between caring about and caring for. It is almost always much easier to proclaim that one cares about an issue than to do something about it. Put simply, our values are worth nothing until we live them. Rhetoric and espoused values will not bring about social justice and will not save the planet. We must change our actions. A **politicized ethic of care** (caring for) **entails active involvement in** a local manifestation of **a particular problem or issue, exploration of the complex sociopolitical contexts in which the problem**/issue **is located, and attempts to resolve conflicts of interest.** FROM STSE RHETORIC TO SOCIOPOLITICAL ACTION Writing from the perspective of environmental education, **Jensen** (2002) **categorized the knowledge** that is **likely to promote sociopolitical action** and encourage pro-environmental behavior **into four dimensions**: (a) **scientific and technological knowledge** **that informs the issue** or problem; (b) **knowledge about the underlying social, political, and economic issues**, conditions, **and structures** and how they contribute to creating social and environmental problems; (c) **knowledge about how to bring about changes** in society through direct or indirect action; **and** (d) **knowledge about the likely outcome or direction of possible actions and the desirability of those outcomes.** Although formulated as a model for environmental education, it is reasonable to suppose that Jensen's arguments are applicable to all forms of SSI-oriented action. Little needs to be said about dimensions 1 and 2 in Jensen's framework beyond the discussion earlier in the article. With regard to dimension 3, **students need knowledge of actions that are likely to have positive impact and knowledge of how to engage in them.** **It is essential that they gain robust knowledge of the social, legal, and political system(s)** that prevail in the communities in which they live **and develop a clear understanding of** how **decisions** are **made within** local, regional, and **national government** and within **industry, commerce, and the military. Without knowledge of where and with whom power of decision making is located and awareness of the mechanisms by which decisions are reached**, **intervention is not possible.** Thus, **the curriculum I propose requires** a concurrent program designed to achieve a measure of **political literacy, including knowledge of how to engage in** collective **action with individuals who have different competencies, backgrounds, and attitudes** but share a common interest in a particular SSI. Dimension 3 also includes knowledge of likely sympathizers and potential allies and strategies for encouraging cooperative action and group interventions. What Jensen did not mention but would seem to be a part of dimension 3 knowledge is the nature of **science-oriented knowledge** that **would enable students to appraise the statements, reports, and arguments of scientists, politicians, and journalists and to present their own supporting or opposing arguments in a coherent, robust, and convincing way** (see Hodson [2009b] for a lengthy discussion of this aspect of science education). Jensen's fourth category includes awareness of how (and why) others have sought to bring about change and entails formulation of a vision of the kind of world in which we (and our families and communities) wish to live. It is important for students to explore and develop their ideas, dreams, and aspirations for themselves, their neighbors and families and for the wider communities at local, regional, national, and global levels—a clear overlap with futures studies/education. **An essential step in cultivating the critical scientific and technological literacy on which sociopolitical action depends is the application of a social and political critique** capable of challenging the notion of technological determinism. We can control technology and its environmental and social impact. More significantly, **we can** control the controllers and **redirect technology in such a way that adverse environmental impact is substantially reduced** (**if not** entirely **eliminated**) **and issues of freedom, equality, and justice are kept in the forefront of discussion during the establishment of policy**.

#### Scholarship and practice can be co-constitutive – ivory tower can be emprically broken down with policymaking experience

Bertucci et al 2014 (Mariano, [fellow @ Center for Inter-American Policy and Research @ Tulane University], Fabián Borges-Herrero [Assistant Professor of Political Science at CSUSB], Claudia Fuentes-Julio [faculty @ institute of international relations @ Pontifical Catholic University of Rio de Janeiro], Toward “Best Practices” in Scholar–Practitioner Relations: Insights from the Field of Inter-American Affairs, *International Studies Perspectives*, 15.1, accessed 7-15-2019, GDI-ATN)

The literature on scholar–practitioner interactions in International Relations (IR) is dominated by a sense of chasm.2 Practitioners generally conceive scholarly outputs as abstract discussions specifically tailored to satisfy the intellectual demands of other scholars rather than responding to the pressing issues policymakers must deal with on a daily basis. Many scholars, in turn, disdain the oversimplifications and lack of analytical rigor they often attribute to policy officials. IR is often described as a self-regulated field in which professional success depends almost entirely on one’s reputation among peers. In this field, there is a strong incentive to produce highly specialized and methodologically rigorous research because this type of work, as opposed to teaching or public service, is what a scholar’s career advancement is predicated on. Hence, IR scholars focus on generating novel arguments that will impress other scholars, rather than policymakers. Policymakers, on their part, want to know how events occur and pursue knowledge specific to the policy process, that is, about what policy levers to activate in order to shape outcomes in the desired direction, as opposed to knowing why events occur and producing general explanations that abstract from the workings of policy processes (George 1993; Kruzel 1994; Lepgold and Nincic 2001; Jentleson 2002; Walt 2005; Nau 2008; Nye 2008a; Krasner 2011). This perceived gap, according to some observers, is growing larger. Even though there have been several examples of how the study of international relations could and did contribute useful insights to foreign policy practitioners (e.g., research on nuclear strategy and arms control was widely used by U.S. policymakers during the Cold War and research on “democratic peace theory”—that democracies do not fight each other—has recently entered popular discourse and also shaped policy in the United States), these contributions have allegedly become more scarce as IR scholars increasingly turn to theoretical models that only qualified insiders can penetrate and that policymakers consider irrelevant (Nye 2008a:654). Missing from the literature on scholar–practitioner interactions in IR is a more systematic focus on the experience of those trained social scientists with professional trajectories as such that have often played important roles in government.3 The experience of these “in-and-outers” suggests that the gap might not be as wide as it may seem. In the field of Inter-American affairs, for example, scholars both in Latin America and in North America often have access to policymaking as direct as those of business interests.4 Two of the most influential Latin American presidents of the last 30 years, Fernando Henrique Cardoso of Brazil and Ricardo Lagos of Chile, have social science PhDs. President Rafael Correa of Ecuador has a PhD in Economics. Three of the last four Mexican presidents— Carlos Salinas, Ernesto Zedillo, and Felipe Caldero´n—have had graduate training in the social sciences. Most Latin American Finance Ministers and Central Bank presidents in recent years have PhDs in Economics. Some of the bestknown Latin American foreign policy practitioners of recent years—former Foreign Ministers Jorge G. Castan˜eda of Mexico and Celso Lafer of Brazil, as well as Mexico’s late Deputy Foreign Minister Carlos Rico, and Professor Marco Aure´lio Garcia of Brazil, personal foreign policy advisor to Presidents Lula and Dilma Rousseff—came from academia. Chile, which has had one of the most noteworthy international policies in recent years, has relied heavily on social scientists: former Foreign Ministers Jose´ Miguel Insulza (now Secretary General of the Organization of American States), Ignacio Walker and Juan Gabriel Valde´s; former Deputy Foreign Ministers Angel Flisfisch and Heraldo Mun˜oz (now head of the United Nations Development Program’s Regional Bureau for Latin America), for example (Lowenthal 2010).

#### Fiat is good -- foreign policy simulations teach students how allies and adversaries respond to U.S. policy -- fosters ideological reflexivity, accurate policy prediction, and argumentative agency.

**Esberg and Sagan ’12** [Jane and Scott; 2012; Special assistant to the Director at New York University’s Center on International Cooperation; Professor of Political Science and Director of Stanford's Center for International Security and Cooperation; *The Nonproliferation Review*, “NEGOTIATING NONPROLIFERATION: Scholarship, Pedagogy, and Nuclear Weapons Policy,” p. 95-96; GR]

These government or quasi-government think tank simulations often provide very similar lessons for high-level players as are learned by students in educational simulations. Government participants learn about the importance of understanding foreign perspectives, the need to practice internal coordination, and the necessity to compromise and coordinate with other governments in negotiations and crises. During the Cold War, political scientist Robert Mandel noted how crisis exercises and war games forced government officials to overcome ‘‘bureaucratic myopia,’’ moving beyond their normal organizational roles and thinking more creatively about how others might react in a crisis or conflict. The skills of imagination and the subsequent ability to predict foreign interests and reactions remain critical for real-world foreign policy makers. For example, simulations of the Iranian nuclear crisis\*held in 2009 and 2010 at the Brookings Institution’s Saban Center and at Harvard University’s Belfer Center, and involving former US senior officials and regional experts\*highlighted the dangers of misunderstanding foreign governments’ preferences and misinterpreting their subsequent behavior. In both simulations, the primary criticism of the US negotiating team lay in a failure to predict accurately how other states, both allies and adversaries, would behave in response to US policy initiatives. By university age, students often have a pre-defined view of international affairs, and the literature on simulations in education has long emphasized how such exercises force students to challenge their assumptions about how other governments behave and how their own government works. Since simulations became more common as a teaching tool in the late 1950s, educational literature has expounded on their benefits, from encouraging engagement by breaking from the typical lecture format, to improving communication skills, to promoting teamwork. More broadly, simulations can deepen understanding by asking students to link fact and theory, providing a context for facts while bringing theory into the realm of practice. These exercises are particularly valuable in teaching international affairs for many of the same reasons they are useful for policy makers: they force participants to ‘‘grapple with the issues arising from a world in flux. Simulations have been used successfully to teach students about such disparate topics as European politics, the Kashmir crisis, and US response to the mass killings in Darfur. Role-playing exercises certainly encourage students to learn political and technical facts\* but they learn them in a more active style. Rather than sitting in a classroom and merely receiving knowledge, students actively research ‘‘their’’ government’s positions and actively argue, brief, and negotiate with others. Acts can change quickly; simulations teach students how to contextualize and act on information.

### Cede the Political

#### Applying theory to action is key – otherwise we cede the political to insider technopols.

Bertucci et al 2014 (Mariano, [fellow @ Center for Inter-American Policy and Research @ Tulane University], Fabián Borges-Herrero [Assistant Professor of Political Science at CSUSB], Claudia Fuentes-Julio [faculty @ institute of international relations @ Pontifical Catholic University of Rio de Janeiro], Toward “Best Practices” in Scholar–Practitioner Relations: Insights from the Field of Inter-American Affairs, *International Studies Perspectives*, 15.1, accessed 7-15-2019, GDI-ATN)

Inter-American affairs are marked by a stark dichotomy. On the one hand, there are close relations among a considerable number of scholars and policymakers, and especially the emergence of “technopols” who move back and forth between academia and politics (e.g., Domı´nguez 1997). On the other hand, a much smaller number of scholars focus on theoretical issues without addressing explicit policy concerns, thus adhering to the pattern that characterizes most other subfields in Political Science. A third group, prominent in U.S. and in Canadian academia, shuns any involvement with policymakers but approaches the issues from a politically committed anti-establishment position. Even though many scholars and practitioners in the field of Inter-American affairs have had considerable experience with each other, some scholars have become practitioners, and some practitioners have re-entered academia, the fruits of their interaction have on the whole not been substantial. Scholars have often been critical of U.S. and Canadian practitioners for their failure to rigorously disaggregate among country experiences; flawed policymaking by misleading analogy; and loose conceptualization of such processes as democracy promotion, populism, and the rule of law. Few social scientists, on the other hand, have been able and willing to apply rigorous analyses and methodologies to policy issues. Policy officials working on Inter-American affairs often lament the lack of policy relevance of academic theorizing. Scholars and practitioners in this field tend to talk past each other, with little impact in either direction.

## Perm

### Methodological Pluralism

#### **IR theory should embrace a plurality of approaches – best prevents bad policy and IR theory**

Zambernardi 2015 (Lorenzo, University of Bologna, Italy, “Politics is too important to be left to political scientists: A critique of the theory–policy nexus in International Relations,” European Journal of International Relations, 8/15/15, LibGen.io accessed 7/13/19 GDI-JEM)

I am not sure if these arguments support Feyerabend’s (1975) maxim that ‘anything goes’, but they certainly support the epistemological and political liberal view that plu-ralism must flourish. Hence, theoretical and methodological diversity should be encour-aged. The only acceptable and healthy protection from poor IR theory and, most importantly, from bad policy is not the silencing of particular approaches or the conver-gence towards a particular methodology, but a mutual criticism that avoids ending up in intellectual standardization. Although a dialectic link between theory and practice should characterize the interaction between the two, the relationship should not be resolved in terms of synthesis. In other words, the gap between scholarship and policymaking is not to be bridged. IR theorists’ public duty — starting and contributing to public debates — can be better developed when scholars are aware that they have no demiurgic role (Panebianco, 1999). Whether scholars are naturalists or not, the most important contribution that IR theorists can make to foreign policy and international politics is neither to ‘speak truth to power’ (Morgenthau, 1966; Wallace, 1996) nor to ‘discipline power with truth’ (Krasner, 1996: 125), but rather discipline power with a variety of truths and encourage the self-educa-tion of practitioners. These are the two main functions that IR theory can perform for policymaking. Whether these arguments are applicable to political science more generally is an issue that has not been debated here and that is left open for discussion by other scholars in their respective intellectual domains.

#### **Multitude of approaches good – allows for greater debate among academics and more comprehensive analysis of consequences**

Zambernardi 2015 (Lorenzo, University of Bologna, Italy, “Politics is too important to be left to political scientists: A critique of the theory–policy nexus in International Relations,” European Journal of International Relations, 8/15/15, LibGen.io accessed 7/13/19 GDI-JEM)

Debates and disputes regarding international affairs have the great advantage of ensuring that rival explanations and policy advice can be taken into account for each problem (Panebianco, 1999): ‘The role of scientific research and analysis is therefore not the heroic one of providing truths by which policy may be guided, but the ironic one of preventing policy being formulated around some technical conclusions’ (Collingridge and Reeve, 1986: 32). Indeed, while the general public is very likely to ignore academic debates, there is strong evidence that policymakers follow research and scholarship on international affairs on a regular basis (Avey and Desch, 2014: 229). I am not arguing that different theories freely compete in the marketplace of ideas. Nor do I support the claim that theoretical competition is a key requirement for the growth of political knowledge. As we all know well, the settlement of political disputes in the public arena is rarely based only on the quality of the argument proposed, but also often on the values and the political and economic power behind those arguing. In the political arena, arguments rarely confront each other in a fair manner with the purpose of reaching truth and improving understanding. Actually, they are often used as ammunition for political competition. Theoretical proliferation, the clash of competing arguments and mutual criticism can neither ensure that the best theories will survive nor prevent major mistakes, but they can avoid errors becoming uncontested truths. The positive contribution of IR, then, results not from the intentions and purposes of single political scientists, but rather from the involuntary effects of all scholars’ contribu-tions. Although social scientists are aware of unintended consequences on political real-ity (Boudon, 1977; Merton, 1936), they seem to forget that they are part of the same reality they are studying and that, as social individuals, they produce unintended effects too. The paradox is that the work of scholars plays this ironic role especially when theo-rists disagree about the decisions to be made (Panebianco, 1999). As Ralf Dahrendorf (1968: 240, 247) maintained, the: only adequate response to the human condition of uncertainty ... is the necessity of maintaining a plurality of decision patterns, and an opportunity for them to interact and compete.... Uncertainty demands variety and competition ... and political conflict, and institutions that provide suitable conditions for this conflict. In so doing, different theories enable us to look at present and future conditions in differ-ent ways in all the three major stages of the policy process: problem recognition, the formation and refining of policy proposals, and politics (Kingdon, 1993).The existence of a multitude of contradictory theories in the discipline should be seen not as a problem, but rather as a positive and desirable condition. Although pluralism tends to fragment the IR community, only a scientist conception of political knowledge at can regard theoretical diversity as a hindrance to healthy policymaking. Thus, a variety of approaches and methods is beneficial not only for intellectual reasons (Mearsheimer and Walt, 2013; Smith, 2004), but for political reasons as well. Indeed, ‘critical debate is the sole adequate procedure in view of the fundamental limitations on our knowledge’ (Dahrendorf, 1968: 251).

#### **Combination of theories key to avoid dogmatism – allows best pursuit of better IR theory**

Mearsheimer 2013 [John J. and Stephen M., University of Chicago, and Walt, Harvard University, “Leaving theory behind: Why simplistic hypothesis testing is bad for International Relations,” European Journal of International Relations, 2013, <https://mearsheimer.uchicago.edu/pdfs/Leaving%20Theory%20Behind%20EJIR.pdf> accessed 7/14/19 GDI-JEM]

The study of IR should be approached with humility. There is no single theory that makes understanding world politics easy, no magic methodological bullet that yields robust results without effort, and no search engine that provides mountains of useful and relia-ble data on every question that interests us. We therefore favor a diverse intellectual community where different theories and research traditions coexist. Given how little we know, and how little we know about how to learn more, overinvesting in any particular approach seems unwise. As Schrodt (2006: 336) wisely observes, ‘we need all the help we can get to figure out this whacko world.’ What matters most, however, is whether we create more powerful theories to explain key features of IR. Without good theories, we cannot trust our empirical findings, whether quantitative or qualitative in nature. Unless we have theories to make sense of them, we cannot even keep track of all the hypotheses that scholars keep piling up. There are many roads to better theory, but that should be our ultimate destination.

## Security Good

### 2AC Engagement Turn

#### Even if security and risk calculation are flawed, engaging in them creates discourse of social welfare and promotes a democratic civic culture that checks political exclusion and loss of value to life

Loader & Walker 7 [Ian, Criminology All Souls College @ Oxford (England), Neil, Regius Professor of Public Law and the Law of Nature and Nations @ Edinburgh Law. *Civilizing Security*. 5-18]

Faced with such inhospitable conditions, one can easily lapse into fatalistic despair, letting events simply come as they will, or else seek refuge in the consolations offered by the total critique of securitization practices – a path that some critical scholars in criminology and security studies have found all too seductive (e.g. Bigo 2002, 2006; Walters 2003). Or one can, as we have done, supplement social criticism with the hard, uphill, necessarily painstaking work of seeking to specify what it may mean for citizens to live together securely with risk; to think about the social and political arrangements capable of making this possibility more rather than less likely, and to do what one can to nurture practices of collective security shaped not by fugitive market power or by the unfettered actors of (un)civil society, but by an inclusive, democratic politics. Social analysts of crime and security have become highly attuned to, and warned repeatedly of, the illiberal, exclusionary effects of the association between security and political community (Dillon 1996; Hughes 2007). They have not, it should be said, done so without cause, for reasons we set out at some length as the book unfolds. But this sharp sensitivity to the risks of thinking about security through a communitarian lens has itself come at a price, namely, that of failing to address and theorize fully the virtues and social benefits that can flow from members of a political community being able to put and pursue security in common. This, it seems to us, is a failure to heed the implications of the stake that all citizens have in security; to appreciate the closer alignment of self-interest and altruism that can attend the acknowledgement that we are forced to live, as Kant put it, inescapably side-by-side and that individuals simultaneously constitute and threaten one another’s security; and to register the security-enhancing significance and value of the affective bonds of trust and abstract solidarity that political communities depend upon, express and sustain. All this, we think, offers reasons to believe that security offers a conduit, perhaps the best conduit there is, for giving practical meaning to the idea of the public good, for reinventing social democratic politics, even for renewing the activity of politics at all. These, of course, may prove to be naïve hopes, futile whistling in a cold and hostile wind. It is in addition true that the project of civilizing security is ultimately a question not of social theory but of political praxis. But if such a project is ever to be thematized as a politics it requires, or at least can be furthered by, some form of theoretical articulation; one which reminds us, as C. L. R. James (1963) might have said, that those who know only of security of security nothing know. It is with this overarching purpose in mind that we have been moved to write in the way that we have about security today. Our argument in this book is that security is a valuable public good, a constitutive ingredient of the good society, and that the democratic state has a necessary and virtuous role to play in the production of this good. The state, and in particular the forms of public policing governed by it, is, we shall argue, indispensable to the task of fostering and sustaining livable political communities in the contemporary world. It is, in the words of our title, pivotal to the project of civilizing security. By invoking this phrase we have in mind two ideas, both of which we develop in the course of the book. The first, which is relatively familiar if not uncontroversial, is that security needs civilizing. States – even those that claim with some justification to be ‘liberal’ or ‘democratic’ – have a capacity when self-consciously pursuing a condition called ‘security’ to act in a fashion injurious to it. So too do non-state ‘security’ actors, a point we return to below and throughout the book. They proceed in ways that trample over the basic liberties of citizens; that forge security for some groups while imposing illegitimate burdens of insecurity upon others, or that extend the coercive reach of the state – and security discourse – over social and political life. As monopoly holders of the means of legitimate physical and symbolic violence, modern states possess a built-in, paradoxical tendency to undermine the very liberties and security they are constituted to protect. Under conditions of fear, such as obtain across many parts of the globe today, states and their police forces are prone to deploying their power in precisely such uncivil, insecurity instilling ways. If the state is to perform the ordering and solidarity nourishing work that we argue is vital to the production of secure political communities then it must, consequently, be connected to forms of discursive contestation, democratic scrutiny and constitutional control. The state is a great civilizing force, a necessary and virtuous component of the good society. But if it is to take on this role, the state must itself be civilized – made safe by and for democracy. But our title also has another, less familiar meaning – the idea that security is civilizing. Individuals who live, objectively or subjectively, in a state of anxiety do not make good democratic citizens, as European theorists reflecting upon the dark days of the 1930s and 1940s knew well (Neumann 1957). Fearful citizens tend to be inattentive to, unconcerned about, even enthusiasts for, the erosion of basic freedoms. They often lack openness or sympathy towards others, especially those they apprehend as posing a danger to them. They privilege the known over the unknown, us over them, here over there. They often retreat from public life, seeking refuge in private security ‘solutions’ while at the same time screaming anxiously and angrily from the sidelines for the firm hand of authority – for tough ‘security’ measures against crime, or disorder, or terror. Prolonged episodes of violence, in particular, can erode or destroy people’s will and capacity to exercise political judgement and act in solidarity with others (Keane 2004: 122–3). Fear, in all these ways, is the breeding ground, as well as the stock-in-trade, of authoritarian, uncivil government. But there is more to it than that. Security is also civilizing in a further, more positive sense. Security, we shall argue, is in a sociological sense a ‘thick’ public good, one whose production has irreducibly social dimensions, a good that helps to constitute the very idea of ‘publicness’. Security, in other words, is simultaneously the producer and product of forms of trust and abstract solidarity between intimates and strangers that are prerequisite to democratic political communities. The state, moreover, performs vital cultural and ordering work in fashioning the good of security conceived of in this sense. It can, under the right conditions, create inclusive communities of practice and attachment, while ensuring that these remain rights-regarding, diversity respecting entities. In a world where the state’s pre-eminence in governing security is being questioned by private-sector interests, practices of local communal ordering and transnational policing networks, the constitution of old- and new-fashioned forms of democratic political authority is, we shall argue, indispensable to cultivating and sustaining the civilizing effects of security. Security and its discontents Raising these possibilities is, of course, to invite a whole series of obvious but nonetheless significant questions: what is security? What does it mean to be or to feel secure? Who or what is the proper object of security – individuals, collectivities, states, humanity at large? What social and political arrangements are most conducive to the production of security? It is also to join – in a global age that is now also an age of terror – a highly charged political debate about the meanings and value of security as a good, and about how it may best be pursued. It is these questions, and this debate, that we want to address in this book. Security has become the political vernacular of our times. This has long been so in respect of ‘law and order’ within nation states. Authoritarian regimes are routinely in the habit of using the promise and rhetoric of security as a means of fostering allegiance and sustaining their rule – delivering safe streets while (and by) placing their citizens in fear of the early morning knock at the door (Michnik 1998). Democratic societies too have over the last several decades come to be governed through the prism of crime – a phenomenon especially marked in the USA, Britain and Australasia, though not without resonance in other liberal democratic states (Garland 2001; Simon 2006; see also Newburn and Sparks 2004). But security has also since 9/11, and the ‘war on terror’ waged in response to it, become a pervasive and contested element of world politics, impacting significantly on the ‘interior’ life of states and international and transnational relations in ways, as we shall see, that escalate the breakdown of once settled distinctions between internal and external security, war and crime, policing and soldiering (Kaldor 1999; Bigo 2000a). Today, security politics is riven by disagreements over the pros and cons of self-consciously seeking security using predominantly policing and military means; by disputes about how and whether to ‘balance’ security with such other goods as freedom, justice and democracy; and by conflicts between a conception of security as protection from physical harm and wider formulations of ‘human’ or ‘global’ security. In the face of these debates we are aware that the title and ambitions of this text are likely to meet with one of three possible responses. They will be seen by some as offensive to the benign intentions and purposes of governments and security actors. They may be viewed, alternatively, as the naïve, wrong-headed pursuit of an oxymoron. Or they may be dismissed – by those who share our broad ambition to civilize security – as too limited in their grasp of what the idea of security can and should mean. We want to probe a little further into each of these anticipated reactions. In so doing, we can begin to pinpoint the limitations of certain established dispositions towards, and public discourses about, security, as well as indicating how the debate about security can be moved to a different – we think more fruitful – place.1 The first – currently hegemonic – response issues from a lobby that seeks fairly unambiguously to promote security and that takes exception to the idea that security needs civilizing. Security, on this view, is an unqualified human good. The protection of its people from internal and external threats stands consequently as the first and defining priority of government. Far from needing to be balanced with democratic rights and freedoms, security is a precondition for the enjoyment of such goods. Far from needing ‘civilizing’, security is the foundation stone and hallmark of civilization. Security, moreover, can and should be directly and consciously pursued using what Joseph Nye (2002) calls ‘hard power’ – by enabling, resourcing and enthusiastically backing the military, intelligence agencies and the police. It is these agencies that will protect the state and its citizens, and these agencies whose purposes and effectiveness must not be hamstrung by excessive legal rights and safeguards that give succour to the enemy, or by forms of democratic deliberation that obstruct decisive executive action. This – stripped to its essentials – is the discourse that has animated countless ‘wars on drugs’ and ‘crackdowns’ on crime and disorder in both democratic and authoritarian states over recent decades, and which since 9/11 has fuelled and justified what may turn out to be a permanent ‘war on terror’. This disposition towards, and identification with, security has long antecedents dating back to Jean Bodin and Thomas Hobbes, and is deeply sedimented in the present (Robin 2004). It represents the clearsighted and hard-headed outlook of a good many politicians and police officers. It holds – for anxious citizens – a deep emotional allure. But it is not without some serious shortcomings, two of which warrant an introductory note. It proceeds, first of all, in ways that gloss over the paradoxes that attend the pursuit of security (Berki 1986: ch. 1; Zedner 2003). It has little to say, and rarely pauses to reflect upon, the most profound of these; namely, that the state’s concentration of coercive power makes it simultaneously a guarantor of and a threat to the security of individuals. Security, as Berki (1986: 13) puts it, is inescapably a problem for and a problem of the state – a condition we deal with more fully in later chapters (see also N. Walker 2000: ch. 1). Nor does the security lobby grasp clearly the implications of how human beings are mutually implicated in one another’s in/security – as both an everpresent potential threat to the security of each, and at the same time a necessary precondition for giving effect to such security. Still less does the security lobby register and absorb the fact that security is, in an important sense, destined to remain beyond our grasp – ‘more within us as a yearning, than without us as a fact’ (Ericson and Haggerty 1997: 85). Not only does this mean that there can never – in a paradox rich with implications – be ‘enough’ security measures, which hold out a promise of protection while always also signifying the presence of threat and danger. It also warns us that responding to demands for order in the terms in which they present themselves (i.e. zero-tolerant police, tougher sentencing, more prisons, ‘wars’ against drugs, or crime, or terror) can be little more than a bid to quench the unquenchable. The effacing of paradoxes such as these is closely connected to – indeed a key contributor towards – the second and most deleterious shortcoming of the security lobby. This is its tendency to make security pervasive, to proceed in ways that treat and thereby produce ‘security’ – or, more accurately, security rhetoric and activity – as a dominant, emotionally charged element of political culture and everyday life. Security – as Buzan et al. (1998) usefully remind us – is not only a condition of social existence, a description of social relations marked by order and tranquillity. It is also a political practice, a speech act, one way of framing and naming problems. To call something ‘security’ – to make what Buzan et al. (1998: 25) call a ‘securitizing move’ – is to suggest, and to seek to mobilize audiences behind, the idea that ‘we’ face an existential threat that calls for immediate, decisive, special measures. It is, in other words, to seek to lift the issue at hand – whether it is crime, or drugs, or migration – out of the realm of normal democratic politics, to claim that as an emergency it demands an urgent, even exceptional, response. The security lobby – blessed as it invariably is with ‘blind credulity and passionate certainty’ (Holmes 1993: 250) – makes precisely this move. It connects with and articulates public insecurities about crime, or disorder, or terror in terms that institutionalize anxiety as a feature of everyday life and link security to a conception of political community organized around binary oppositions between us/them, here/there, friends/enemies, inside/outside. In encouraging ‘emotional fusion between ruler and ruled’ around the question of fear (Holmes 1993: 49), it generates a climate that inhibits – even actively deters – critical scrutiny of the state’s claims and practices. By translating security into Security, into a matter of cops chasing robbers, soldiers engaging the enemy, it risks fostering vicious circles of insecurity (atrocity – fear – tough response – atrocity – fear – and so on) that ratchet up police powers, security technologies and their attendant rhetoric in ways that it becomes difficult then to temper or dismantle. In all these ways, the security lobby makes ‘security’ talk and action pervasive, or what we shall call shallow and wide, reproducing ‘security’ on the surface of social consciousness and rendering it dependent on the visible display of executive authority and police power. In so doing, it fails to get close to the heart of what it is that makes individuals objectively (or intersubjectively) and subjectively secure – it is unable, that is, to understand, still less to create, the conditions under which security becomes axiomatic, or deep and narrow. For us, these are vital distinctions, ones that we revisit and develop as our argument unfolds. The second response to our stated ambitions – the one likely to regard the enterprise as hopelessly misplaced – is concerned above all to counter security. This emanates from what we may call the ‘liberty lobby’ which disputes the suggestion that security can be civilized. Security, on this view, is a troubling, dangerous idea. Security politics – especially in the form we have just set out – is seen as authoritarian and potentially barbarous – ‘contrary to civil well-being’ (Keane 2004: 46). It is a politics that privileges state interests (and conceptions of security) over those of individuals; that is inimical to democratic values; that possesses a seductive capacity to trample – in the name, and with the support, of ‘the majority’ – over civil liberties and minority rights; that is, in short, conducive to the very violence that it purports to stamp out. Security, consequently, is something that must either be curbed in the name of liberty and human rights or, given its close police and military associations, abandoned as a value altogether. Let us briefly introduce two strands of this critical disposition. The first – common to human rights movements across the globe – seeks to constrain the power of security by questioning its imperatives, and fencing in its demands, with an insistence on protecting or enhancing the democratic freedoms and individual rights that security politics is indifferent to, throws into a utilitarian calculus, chips away at, or suspends. From this standpoint, habeas corpus, access to legal advice, limits on detention and police interrogative powers, jury trials, rights of appeal and the like are the expression and tools of a desire to preserve a space for individual liberty in the face of the forceful demands of an overweening state and global state system – whether in ‘normal’ or ‘exceptional’ times.2 A second stance – associated with those working under the loose banner of ‘critical security studies’ (Krause andWilliams 1997) – deepens and radicalizes the impulse and insights of the first. This holds that security is irredeemably tainted by its police/military parentage, and by its authoritarian desires for certainty. On this view, security is a political technology that must ‘continue to produce images of insecurity in order to retain its meaning’ (A. Burke 2002: 18) in ways that make it, at a conceptual level, inimical to democratic politics; or else it is a practice deeply tarred by its intimate empirical relation to the formation and reproduction of state-centric interests and xenophobic, anti-democratic political subjectivities and collective identities (R. B. J. Walker 1997). The conclusion in either case is the same. Security, it is claimed, has to be abandoned, the dual analytical and political task being to unsettle and deconstruct security as a category so as to find ways of thinking and acting beyond it (Dillon 1996; Aradau 2004). There is much of value in this critique of uncivil security – a great deal, in fact, which we are sympathetic towards. But these critical stances also share certain lacunae. Each, in particular, expressly or implicitly intimates that security – understood as being and feeling free from the threat of physical harm – is a problem, a conservative sensibility and project that is all too often hostile to the values and institutional practices of democracy and liberty (Huysmans 2002). The result is that each operates as a negative, oppositional force, one that evacuates the terrain that the security lobby so effectively and affectively occupies in favour of a stance that strives either to temper its worst excesses, or to trash and banish the idea altogether – a stance that appeals in part because so few others appear motivated to defend the liberties which are being imperilled. There is, on this view, little or no mileage in seeking to think in constructive terms about the good of security and the kind of good that security is. There is little point in fashioning a theory and praxis that explores the positive – democracy and liberty-enhancing – ways in which security and political community may be coupled; in reflecting upon what it means, and might take, to make security axiomatic to lived social relations. There can, in short, be no politics of civilizing security. Proponents of the third – ‘human’ or ‘social security’ – response share with us both a desire to transcend this received security–liberty dichotomy and, in their own way, an ambition to civilize security. On this view, however, such a project requires that security be rescued from a taken-for-granted association with the ‘threat, use and control of military force’ (Walt 1991: 212), and extended to other domains of social and political life (e.g. de Lint and Virta 2004).3 We can usefully highlight two variants of this position – one international, the other domestic. The former takes its cue from the United Nations Human Development Report 1994, which introduced, and sought to mobilize opinion behind, the concept of ‘human security’, an idea which has subsequently been taken up in further work conducted under the auspices of the United Nations and the European Union (Commission on Human Security 2003; Barcelona Group 2004; cf. Paris 2001). It seeks to decouple security from questions of war and peace and deploy it as a device aimed at urging governments to treat as emergencies such chronic threats as hunger, homelessness, disease and ecological degradation – the latter, for instance, being described by the Commission on Global Governance (1995: 83) as ‘the ultimate security threat’. The domestic version of the argument draws from the insight that there is no policing or penal solution to the problem of order the conclusion that crime control – or harm reduction – is ultimately a matter of, and dissolves into, questions of economic and social policy more generally. This is a commonly held disposition within both sociological criminology and social democratic politics, one which has in recent years informed a critique of situational crime prevention, crime science and other forms of technocratic crime control, and underpinned the promotion of multi-agency, social crime prevention (Crawford 1997; Hope and Karstedt 2003). On this view, security conceived of in a ‘shallow’ manner as freedom from physical harm or threat is both inseparable from a more profound sense of ‘well-being’ or ‘ontological’ security and, therefore, also dependent upon the broader institutions and services of social welfare (Fredman forthcoming). There is, once more, much to applaud in this attempt to extend the meanings and application of the idea of security. It reminds us that freedom from physical coercion is but a part of any rounded conception of human flourishing. And it pinpoints the limited and often counter-productive role that security politics and policing institutions play within this wider project. But there are difficultie

### 2AC AT Rejection Alt

#### Appeals to security are not necessarily “securitizing” – critical approaches ignore situated practices that contest traditional security. We have to pragmatically evaluate it in each individual context

Nyman 2016 [Jonna, Lecturer in International Politics at the Univ of Sheffield, “What is the value of security? Contextualizing the negative/positive debate,” *Review of International Studies*, <https://lra.le.ac.uk/bitstream/2381/37156/1/Nyman_The%20value%20of%20security%20RIS_FinalMarch2016.pdf>, accessed 7/11/19, GDI-JCR]

Having clarified the different uses of these terms, I propose an alternative approach to overcome these tensions, which I label the pragmatist frame. This brings the contributions of the analytic and normative frames together, but focuses on studying the value of security in context. This focuses on how security is currently used by different actors, to illustrate that it can be, but isn’t always, a ‘good thing’. Although there is not enough space to introduce a fully-fledged new theoretical framework here, the final section is devoted to exploring this further. Here I draw on the pragmatist philosophy of Dewey and James, practice-centred approaches and contextualism. Drawing on Ciută’s argument that security does not have an unchanging ‘essence’ or meaning12, I suggest that it also has no inherent value: this has serious implications for the negative/positive debate. If the value of security is contextual and unfixed, the focus should shift from defining what makes security practices positive or negative in the abstract, to studying actual situated security practices in context and using this to make conclusions about the value of security in that particular case. Reflexivity is essential here: such analysis has to be accompanied by a shift from fixed normative commitments towards normative awareness. This may in turn help practical analysis (and critique) of existing notions of security and security policy. While further research is needed, I hope this contribution will open space for exploring a new way forward for understanding the value of security. The paper’s central contribution is thus to clarify the debate over the value of security, drawing out the different uses of the terms ‘negative’ and ‘positive’ and proposing an alternative pragmatist route. Because the focus here is on the debate over the value of security and how security is currently used, it does not tackle the bigger question of what or which issues should or shouldn’t be constructed as security issues, as this is beyond the scope of the paper. However, studying the ethics of security implies a normative approach, where the analyst/s is recognised as ‘active participants in the security discussion’13. The paper begins with a discussion on the ethics of security, distinguishing between securitization and the construction of security. It then examines the negative/positive debate, drawing out the analytic and normative frames in the key contributions on the topic. Lastly, it develops the pragmatist frame drawing on these uses and building on them to create a pragmatic, contextual and practice-centred understanding of the value of security. The final section discusses the implications. Critical security studies emerged in the 1990s as a critique of dominant state-centred security studies and politics, to question what security is and who it is for. Most authors writing in this tradition agree that the meaning of security is constructed. Consequently, critical security studies has engaged with ideas on the value and ethics of security directly, with two of the most influential early approaches presenting contrasting views. The Copenhagen School study security as securitization, viewing security as negative and usually best avoided14. Meanwhile, the Welsh School define security as emancipation, emphasising its positive value and potential15. Alongside this, there have been ongoing debates over the referent of security, including attempts to attach normatively positive adjectives to security to overcome the negative aspects, from global security to human security, which have made important contributions16. These perspectives have provoked growing debate over the nature, or value, of security. While it doesn’t use the language of the negative/positive debate, the Welsh School’s understanding of security is closely aligned with the analytic frame, and is therefore discussed in more detail later. This section now turns to discuss the influence of the Copenhagen School’s securitization theory on the negative/positive security debate. Many of the contributions in the negative/positive debate explicitly use securitization as a starting point or even as shorthand for security. The Copenhagen School argue that issues ‘become’ security when a (usually elite) actor constructs them as such through security speech-acts and this designation is accepted by the relevant audience, moving the issue from the realm of politics and democracy into a realm of security where extraordinary emergency measures are enabled17. Securitization is seen to have ‘inevitable negative effects’, including ‘the logic of necessity, the narrowing of choice, the empowerment of a smaller elite’18. The Copenhagen School argue that security cannot escape its traditional connotations because of how it is used in the field of practice: in historical terms, it is national security19. They view the realm of security as opposed to normal politics and based on these assumptions they argue that in most cases ‘security should be seen as a negative, as a failure to deal with issues as normal politics’20. As a result, they suggest that while securitization may sometimes be necessary most issues are best dealt with outside of the security sphere, or ‘desecuritized’ 21. The limits of securitization theory have been covered elsewhere so will not be dealt with indepth here22. Many more recent contributions to the negative/positive debate draw on securitization theory, but the debate suffers from a lack of distinction between ‘security’ and ‘securitization’23. Following McDonald, I argue that securitization only represents a particular type of security construction. While arguing that ‘the meaning of a concept lies in its usage and is not something we can define analytically or philosophically according to what would be “best”’24, Buzan et al. simultaneously limit the meaning of security to very specific usages by particular actors. Ciută discusses this in-depth, arguing that the Copenhagen School’s theoretical definition of security takes precedence over situated security practice, limiting analysis to how security works when situated actors ‘happen to act in theoretically prescribed ways’25. Consequently, securitization theory neglects security when it doesn’t fit the framework, such as when it is framed using a different language of security that does not rely on friend/foe distinctions and non-democratic procedures. These do not enable emergency measures and are therefore not cases of securitization. Based on their definition of security, the Copenhagen School broadly favour desecuritization. However, in privileging a particular notion of ‘security’ that can only be articulated by those in a position of power, they overlook the ways in which other actors already contest dominant notions of security and threat, articulating alternative, more positive, concepts of security26. The Copenhagen School struggle to see security when it does not follow their rules. Therefore, I suggest that securitization theory presents a narrow, particular understanding of security, rather than the understanding of security. While critical approaches to security have been concerned with both the politics and ethics of security they have tended to assume security has a universal logic27. The emerging debate on the value of security presents a more nuanced perspective, exploring which characteristics or features make security negative or positive28. Yet, as noted in the introduction, there are clear variations between key authors’ definitions of ‘negative’ and ‘positive’ security and these differences are not addressed or made explicit. Some of this confusion is inevitable, reflecting the fact that different approaches have developed from distinctive literatures, focus on different dimensions of security and have different normative commitments. Most obviously some focus on security as a state of being, while others analyse security as a process or practice: those who focus on security as a state of being tend to be more optimistic about its positive potential, while those who study security as a process tend to point to the problematic features or consequences of existing security processes29. However, the two are not always easy to separate30, and few authors who focus on security as a state of being overlook security as a process. The different uses of these terms matters and needs to be acknowledged, since it stalls the debate as people talk at cross purposes. While recognising that security can be positive or negative, authors also continue to define what is negative and positive in the abstract. The debate over the value of security raises important questions about the kind of politics we desire. To move forward we need a common language, or at least open recognition when we are talking about different things. We also need to recognise that what is good usually depends on the context: this is discussed further in the final section.

#### Security is not inherently good or bad. The Aff can only be evaluated based on its specific advantages and disadvantages

Nyman 2016 [Jonna, Lecturer in International Politics at the Univ of Sheffield, “What is the value of security? Contextualizing the negative/positive debate,” *Review of International Studies*, <https://lra.le.ac.uk/bitstream/2381/37156/1/Nyman_The%20value%20of%20security%20RIS_FinalMarch2016.pdf>, accessed 7/11/19, GDI-JCR]

The alternative frame I propose bridges the analytic and normative frames but focuses on analysing how security is used in different contexts to gain practically useful knowledge60. I retain the normative use of positive and negative as good and bad respectively, to recognise that security can be problematic, but use the analytic frame to suggest that while we cannot define what characterises ‘good’ or ‘bad’ security in the abstract, the ‘goodness’ of different security practices in a context should be understood on a spectrum. I call this the pragmatist frame, since it draws on the pragmatist philosophy of Dewey and James to shift the debate away from developing objective definitions or criteria for when security is good or bad and towards seeking practically useful knowledge about the value of security, which is contingent and context-dependent. Empirically, this lends itself to practice-centred analysis, and here I draw on a wider notion of practice following Adler and Pouliot. Lastly, it brings in contextualism. Contextualist contributions on the meaning of security tell us that security means different things in different contexts, that it doesn’t have an unchanging ‘essence’61. The meaning and the practice of security is contested and produced through ‘a process of negotiation’62. I suggest here that if security is contingent, it cannot be inherently good or bad. Rather, we can only understand the value of security by studying how it works and what it does in different empirical contexts. Bringing pragmatist, practice and contextualist literatures together and into this debate provides an important new lens through which to understand the value of security. While the space to explore the practical implications of this is limited here, the final parts of this section considers how the framework could be used to study the value of security and tackles some of the limitations and questions it raises. Pragmatism is a philosophical approach drawing on the work of authors like John Dewey and William James. It has grown in popularity in IR63 but remains overlooked in debates over security ethics64. A pragmatic approach does not aim to uncover or produce an objective ‘truth’ that is ‘out there’, but rather to gain practically useful knowledge65. Dewey and James are united in emphasising the importance of uncertainty and rejecting settled ‘truths’, ‘fixed principles, closed systems, and pretended absolutes and origins’66. They suggest instead that truth is contingent on context and experience, and never fixed: thus the ‘quest’ for truth is never settled. Cochran refers to this as a ‘weak foundationalism’ allowing contingent ethical claims67. Following this, James emphasises a shift away from first principles and categories, towards last things and consequences – an idea or practice is ‘good’ if the results are deemed to be good, and only for as long as the results are deemed to be good68. Ultimately, good ideas are ideas which ‘are also helpful in life’s practical struggles’69 and the value of a thing depends on what that thing does or leads to in practical terms: what sensations, habits or actions it will produce70. This will in turn vary in different cases and at different times. Dewey also emphasises practice and individual experience as necessary for ethical enquiry71. Pragmatism thus suggests that to understand the value of security, we need to conduct detailed empirical enquiry to see how different actors use it in different contexts and how individuals experience it, asking what do different security practices do? What actions and habits do they produce, and how do they affect life experiences? While the answers to these questions remain contingent, a pragmatic contingent ethics allows us to suggest alternatives while emphasising reflexivity. We can therefore understand when security is good or bad in a particular situation. Methodologically, pragmatism emphasises abduction and starting at the middle level, instead of starting from abstract theoretical principles or inferring propositions from facts72. In this way, we can analyse when human beings experience security as a ‘good’ (and vice versa). This shifts the discussion away from the abstract potential of security to be ‘good’ or ‘bad’, towards empirical research analysing what it ‘does’ in different contexts. The way in which pragmatism is used here lends itself to practice-centred analysis. Practicecentred approaches study practices and how they (re)produce particular ideas and realities73. Here I draw on a wider notion of practice following Adler and Pouliot, which fits more logically with pragmatism. Thus ‘practice’ includes discursive practices as well as ideas, power relations, policies and physical practices undertaken in the name of security74. Vitally, practices are distinguished from behaviour or actions because they are ‘socially meaningful patterns of action’75. A wider understanding of practice allows us to study a range of security practices and processes, including contestation and resistance to hegemonic security practices. This means that we can study a range of actors beyond elites, while recognising the importance of power. Pragmatism is vague on research methods but practice approaches can provide a clear toolkit for how to study security in a way that is compatible with a pragmatic approach76. It also gives us an empirical starting point: security practices.

#### Critiquing bad forms of securitization requires opening up the concept with new understandings based social good

Nyman 2016 [Jonna, Lecturer in International Politics at the Univ of Sheffield, “What is the value of security? Contextualizing the negative/positive debate,” *Review of International Studies*, <https://lra.le.ac.uk/bitstream/2381/37156/1/Nyman_The%20value%20of%20security%20RIS_FinalMarch2016.pdf>, accessed 7/11/19, GDI-JCR]

So where do we look for security?84 I have already suggested security practices as a starting point. Authors used here focus largely on discourse, while this paper suggests going beyond that to consider practices more broadly. Thus, at its most basic, we should start by looking at actual security practices in a particular context and asking what they do. I have emphasised the need for detailed empirical enquiry to see how different actors use security in different contexts and how individuals experience it, asking what different security practices do, what actions and habits they produce, and how they affect life experiences. Situated in-depth case studies lend themselves most obviously to such analysis of the value of security. They are also more likely to provide situated and practically useful knowledge. Bubandt’s study of security practices in Indonesia in an excellent example here: he analyses how state and global security notions/structures are contested or absorbed at local levels, and how local notions feed back into both. While the focus in his study is on the meaning of security the methods could be equally useful for studying its value. An analysis could study global, state and/or non-state security practices, considering both more ‘high profile’ practices with a lot of influence and marginalised or ‘smaller’ everyday security practices85. This necessarily needs to include a consideration of power: where it lies and how this is reproduced. Thus, a contextualised and practice-centred approach to the value of security looks at how different actors understand and practice security and analyses what these different understandings and practices of security do. The following questions may be useful when undertaking such an analysis: • Who are the key actors? • Who is empowered to practice security and who is not? • How do different actors represent security? • What practices do they undertake, what do they do? • What do they emphasise or call for? • What do they want to protect, how and from what? • What does the practice aim to do, and what does it do? • What effects do the practices produce? • What actions and habits do they produce, and how do they affect life experiences? • Are they helpful in daily struggles (the pragmatist test)? • Do they protect, enable or constrain referents? • What are the ethical implications of the practices studied? This is not an exhaustive list but it does provide a starting point. The answers to these questions will vary in different contexts. Which actors/practices are important to study will also depend on the project and case/s studied. We also need to recognise the interconnectedness of security issues86. For example, a security practice may be helpful to the daily struggles of some but produce insecurity for others. Thus, the wider ethical implications of the practices analysed need to be taken into consideration. We are also left with the normative problem of which actors we choose to study: which practices do we study, whose voices do we listen to, and why? Pragmatism does not give satisfying answers to questions about power: whose daily struggles should practices be helpful to, and who gets to decide if the results of a practice are good? McDonald pursues a normative agenda drawing on emancipation, concerned with ‘locating immanent possibilities for emancipatory change’ by opening space for alternative voices87. While I am sympathetic to this approach, it is worth remembering that alternative is not necessarily ‘better’ in ethical terms: consider right-wing groups using security to advocate for closing EU borders to refugees escaping war, for example. So who do we listen to and study, and on what basis do we make this decision? In most cases and contexts studied, there will be a range of actors practicing and articulating security. Covering a range of actors will help to capture different ways of practicing security, which will then allow for more depth when we consider the ethical implications of these security practices. This doesn’t mean all studies have to cover all actors: a study could focus on a single state, non-state groups, or one or more international organisation/s: but in each of these there will likely be some contestation, resistance and disagreement. By analysing how security is contested in different spaces, we also recognise that security is a ‘situated interactive activity’88 and needs to be understood, and studied, as such. To give another example, Bilgic studied security in Tahrir square, focusing on how protesters experienced and practiced security during one week. He draws on feminist work to rethink emancipation, emphasizing how ‘individuals and social groups’ themselves articulate security: ‘that is, their own expressions of how security is understood by them’89. A similar approach could be used to understand the value of different security practices in such a case. Looking at gender, resistance and human security, Hoogensen and Stuvoy suggest that ‘the way to understand and to establish knowledge about security in empirical terms is to enter people’s life-worlds and access local experiences of in/securities’ 90. These examples both emphasise smaller scale security practices and experiences of security, but studies could equally analyse how different actors within the United Nations practice security within that institutional setting and the value of such practices, for example. My own work has looked at how different actors within the United States and China practice energy security, and the value or ethical implications of different security practices in this context91. The introduction to this article noted the importance of considering the role of the analyst in normative analysis. A pragmatic focus on practice partly removes this problem, by focusing on detailed empirical enquiry as opposed to imposing analytical criteria for what makes particular security practices ‘good’ or ‘bad’. In particular, focusing on individuals’ (or groups) own articulations of security92, and evaluating these normatively. However, we cannot fully avoid normative judgement, which is where Ciută’s emphasis on normative awareness and reflexivity is useful. Reflexivity and positionality requires acknowledging the role of the researcher in the research process and in interpreting the data93. Security analysts are not neutral, and will always arrive with preconceived ideas and opinions about the concept and value of security. This only makes openness about normative commitments more important so these can be recognised and interrogated. The role of the security analyst is always political: the key is ‘to be aware of [and explicit about] the political significance of analysis’94. The normative commitments of the analyst will also likely vary between cases studied in contextual security analysis. For example, in my analyses of energy security practices I emphasise the connections between human well-being and environmental security, for the simple reason that without environmentally sustainable energy security practices in the longer term there will be no individual experiences, no human well-being to consider, no daily struggles to be helpful to, as the planetary ecosystems on which human survival depend will collapse. What is ‘good’ therefore depends on the context and what different security practices do in that context, as well as the analyst. This is why we need to be clear and open about normative commitments. Recognising the subjective and context-dependent nature of the value of security will in turn fuel and forward the debate instead of getting gridlocked in debates over the impossibility of an objectively defined ‘good’. However, a pragmatist frame also recognises the need to keep these categories open. So how do we determine what is and isn’t security, and thus which practices to study? The focus here is on analysing how security is used and using this to further understanding of the value of security. Thus the focus is on studying existing security practices, and what they ‘do’ in different empirical contexts – taking a broad interpretation of ‘practice’. Here I mean specifically practices undertaken in the name of security 95 . This doesn't mean security couldn’t be something else, or that there aren’t further things that could or should be secured (which currently are not), but the focus here is on how different existing practices of ‘security’ in empirical contexts can help us understand the value of security. Here, I argue in favour of pluralism and diversity: rather than narrowing down what we mean by ‘security’ to very specific uses or particular (elite) actors, looking at a more diverse range of actors and a more diverse range of meanings of security (beyond survival), serves to illustrate that the value of security depends on the context. Security studies needs to open up for the possibility that ‘security’ can mean very different things, and that in these cases it is characterised by very different processes and outcomes. Similarly, it is important to view the value of security in non-binary terms. Security is contested: consequently, to understand security it is necessary to study the full range of security constructions – from more problematic and undesirable security practices, to limited practices which secure us from threat, to more emancipatory practices, by a wide range of actors and in a range of empirical contexts, to really interrogate the value of security. In a sense this means accepting the range existing definitions and approaches to the value of security and studying how they work in practice. The value of security matters: both because problematic security practices can do a lot of harm and because ‘good’ or ‘positive’ security practices can help us advance towards the kind of world that we want. However, the current debate over the value of security causes confusion. This paper has clarified the debate by separating out two different ‘frames’ used by key authors. The analytic frame draws on positive/negative liberty and peace, and thus defines negative security as the absence of threat, and positive security as added enabling possibilities beyond survival: here positive and negative security work together. The normative frame uses value judgements and deploys the terms positive and negative in a normative sense, often drawing on securitization theory. Consequently, this frame suggests that negative security is bad and to be avoided, while positive security is desirable. These frames have their roots in different literatures and although both theorise the value of security they look at different aspects, leading to somewhat different research agendas. This causes confusion and has stalled the debate. This paper has argued that the value of security depends on how it is used in different empirical contexts, developing a pragmatic framework for understanding the value of security in context. This approach allows us to recognise that security can be bad, but that it can also be something worth striving for, while avoiding imposing abstract theoretical definitions of ‘good’ and ‘bad’. Bourne and Bulley suggest abandoning attempts to establish secure ethics, arguing that we should instead be ‘treating moral choice as explicitly unsure, uncertain and insecure’ 96. Accepting this, a pragmatist frame helps us move forward with a practical research agenda that avoids defining the ‘good’ in theoretical terms while allowing us to evaluate the normative implications of different existing security practices in a particular context. Thus the paper opens space for empirically grounded research on the value of security. The paper focuses on clarifying the existing debate and suggesting an alternative, so it presents a conceptual analysis rather than an empirical application. There is therefore much potential for future research on the value of security in different contexts. Beyond this, two problems caused by this framework that require further research come to mind. Firstly, what about cases where some experience security as a good, but others do not? The ongoing debate over the surveillance society provides an excellent example: some experience surveillance as reassuring, while others find it an imposition on their freedom to go about their daily lives unwatched. In such cases the role of the analyst becomes much more complicated and needs to be considered in more depth. Secondly, what about those who cannot practice security? This framework is merely intended to understand the value of different existing security practices. More research is needed into the silences and gaps this creates, as it overlooks those who cannot speak or practice security but may be deeply affected by insecurity, whether this be silenced or marginalised groups or non-human elements in need of protection, such as local or global ecosystems. This paper has clarified the debate over the value of security and suggested a new framework for analysing it in context, but while it pushes the debate forward it also raises new questions. Security is powerful and contains potential for harm as well as ethical progress. Understanding the value of security is crucial in order to move towards the kind of world that we want.

### 2AC Pragmatism Turn

#### Epistemology critique must move beyond rejection and prescribe pragmatic policy decisions

Rytövuori-Apunen 05 (Helena, University of Tampere adjunct professor of IR focusing on qualitative research in International Relations and Peace and Conflict Research, “Forget ‘Post-Positivist’ IR!: The Legacy of IR Theory as the Locus for a Pragmatist Turn,” Cooperation and Conflict: Journal of the Nordic International Studies Association, 40.2, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.862.8155&rep=rep1&type=pdf, accessed 7-15-2019, GDI-ATN)

For the interpretatively oriented scholars the ideal of cumulative knowledge, which Keohane outlines in terms of scientific inference, obviously speaks for its own limitations (cf. also King et al., 1994). But avoiding this Scylla need not mean the Charybdis where critical IR lives on the ‘border lines’ (Ashley, 1989) or chooses to remain at the critical edges of the alleged mainstream and, in effect, in this way leaves the authority of respectable research (variously claimed by notions such as solid, systematic, empirically based, etc.) to the mainstream that is the target of its criticism. Although I applaud the movement that takes distance from the founding fathers of the discipline by looking for alternative insight in something like la Boótie (Bleiker, 2000) or versions of Buddhism (Chan, 2000), I also miss the epistemic reflections that, on this basis, can put critical IR better on par with the conventional mainstream. Since the post-behaviouralist phase of the discipline (Alker and Biersteker, 1984; Banks, 1985; Holsti, 1985), the movement towards a more global IR has meant acknowledgement and encouragement of the situation of incommensurable ‘paradigms’ or contrasted images. Although fruitful in the emancipatory sense, this logic is now also conducive to what many argue is already the state of IR: dispersion of the discipline into an increasingly scattered field of International Studies. The ‘post’-culture that has dominated critical IR during the past decade or two has already performed its task. It is time to move beyond the concept that, in its disbelief in (an often caricaturist notion of) ‘science’ and critique of extreme forms of rationality, has produced a bifurcated and (as I will argue in greater detail below) not altogether adequate account of the historical discipline. The stagnant condition of our disciplinary debates has been described by for example Patomäki and Wight (2000). In addition, Neufeld, whose work I will touch upon in the following, outlines the dualistic condition of the field as a point of departure for his reflections (1995: 46–69). Like these writers, I, too,seek to reconstruct and on this basis open up new avenues for IR theory. I share Patomäki and Wight’s notion that ‘post-positivism’ has left us with an ontological void, but unlike the Critical Realism proposed by these authors my suggestion for new directions is not a conception of ontological realism and the epistemological and methodological pluralism that logically relates to such critical scientific enterprise.1 In relation to Neufeld, my conclusions on IR theory are similar, but the argument itself is very different. While Neufeld reconstructs IR theory in the perspective of the emancipatory ideas of classical critical theory (the Frankfurt School and Habermas), my argument deals with the promise of pragmatism. Unlike Neufeld’s argument, in the epistemic sense it is not limited to a critical reading in a theoretical perspective (i.e. a relation between the words in the text and the reader; on this reading strategy see, e.g. Skinner, 1988). Moreover, what I have to say has been motivated not only by the IR writers mentioned above but also by some recent introductions of pragmatism (Millennium 31: 3, issued in January 2002, article references below). By presenting pragmatism as a new alley of inquiry which continues from (and hence takes for granted) the situation of disciplinary debates described as an opposition between positivists and post-positivists, these recent contributions fail to appreciate how pragmatism grows from and ties into the web of previous discourse. Hence a key point in pragmatism itself, the question of how knowledge emerges on the grounds of previous knowledge and experience, is not fully realized. Richard J. Bernstein (1983) has emphasized (and a number of other authors have reiterated the point) that the incommensurability — of forms of life, traditions, epistemologies — which Rorty speaks for (and here follows other philosophers of uncertainty and critics of analytic philosophy) need not, and should not, be taken to suggest total exclusivity of concepts and frameworks (cf. also Kuhn, 1970). Rather, the hermeneutical moment speaks for the openness of experience, understanding and language, and proposes that we look for some points of possible agreement and disagreement. For Bernstein, this means a possibility to contribute to the movement beyond objectivism-and-relativism, two sides of the same coin that he calls the Cartesian Anxiety. In the same way, I take the hermeneutical moment as a possibility to approach our field of study, IR, as a potentially global field which, in principle, possesses a domain of total knowledge, although this does not mean a logic of hegemony operating with some generic concept(s). Inspired by Umberto Eco’s notion of knowledge as an encyclopaedic network, I like to think of IR as a discursive web that, in the potentiality of its connections, is global, although any actual piece of knowledge or point of view is always only local (Eco, 1984: 68–86).2 In the broadly pragmatist sense, we can speak of IR as a web of justified beliefs (conventional and with a habitual ground) which, in a variety of ways, seeks to make sense of the world and to solve the intellectual irritation (C. S. Peirce) and the moral dissatisfaction (John Dewey) that belong to human openness and an inquiring attitude towards reality.This approach calls for an understanding of epistemology that reaches beyond the postmodernists’ rejection of the ‘iron cage of reason’. We can begin with the notion that epistemological issues basically deal with the grounds we have for accepting and rejecting beliefs. Reason is only one possibility among human faculties and, beyond being postulated, can also open up as existential (the quest for certainty arises from the fundamental experience of uncertainty). It can also take the conventionalist form of agreed practice, such as rules and procedures of inference.

#### Pragmatism creates better epistemology and is able to actualize analysis of lived experiences

Rytövuori-Apunen 05 (Helena, University of Tampere adjunct professor of IR focusing on qualitative research in International Relations and Peace and Conflict Research, “Forget ‘Post-Positivist’ IR!: The Legacy of IR Theory as the Locus for a Pragmatist Turn,” Cooperation and Conflict: Journal of the Nordic International Studies Association, 40.2, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.862.8155&rep=rep1&type=pdf, accessed 7-15-2019, GDI-ATN)

The task of this paper is to seek the locus in quo pragmatist approaches can emerge in IR’s field of knowledge and through articulated disagreement with previous discourse contribute to an increasingly global discipline beyond the logic of universalism/dispersion. I argue that seeing the locus for pragmatism, i.e. seeing more to it than another approach and a ‘new alley of inquiry’, requires rectifying the distortions created by the postpositivist self-comprehension. An alternative explanation to what Frost calls the ‘positivist bias’ can be sought by examining the specific theorycentred orientation in IR and also the discursive mechanisms and the social processes by which this relation to the world becomes the privileged knowledge that is ‘orthodoxy’. ‘Orthodoxy’ appears when the theory-centred attitude to knowing, which emphasizes theoretical perspective and conceptual logic, loses its footprints in its colloquial interpretations and presents reality ‘as it is’ (naturalized ontology). I will now discuss what the disagreement, the articulation of which I argue is required for maintenance of the idea of the corpus of knowledge as a web of discourse, can mean as a research orientation. I point to a way of inquiry which starts with Dewey, but in the epistemic sense draws from C. S. Peirce’s conception of ‘reality’ as pragma and the pragmaticist logic of inquiry. I propose that a focus in the current introductions of pragmatism on the Deweyan inheritance of classical pragmatism (Millennium 31: 3) does not help us to solve the epistemological issues pertinent in the situation which already builds on and looks beyond the ‘linguistic turn’ and calls for methodical solutions that fit together with these more recent tendencies. The Missing Piece: The Interpretative Aspect of ‘Discourse’ and ‘Culture’ The identification of what I suggest is a paradigmatic feature of the disciplinary mainstream and the legacy of IR Theory (capital letter to mark out this legacy) makes it possible, through ontological criticism, to point out two opposed epistemic paths, one based on the primacy of theory, the other proceeding from the primacy of practice. Opposed to the approach that models the world (produces a ‘world picture’, as Martin Heidegger says)22 is the orientation that proceeds from and seeks to refine what already, in some way, is present in our experience. Above, I have criticized the tendency to read disciplinary tradition in a way which, rather than focusing on analytical difference, subsumes instances of previous theory under a shared characterization and thereby suppresses the potentiality that as possibility of interpretation exists in the historical body of knowledge. In the same vein of argument, it is important to note that the opposition of epistemic positions is not only inter- but also intra-textual. For example Organski’s ambition to ‘organize the mass of [...] information to which we are all exposed’ arises from the experience that the international distribution of power is constantly shifting and that this moment, along with the importance of internal determinants of power, has been neglected by the balance of power theory (Organski, 1958: vii; 1961: 373–5). Analysing how concepts relate to historical experience and the dissatisfaction felt about previous approaches provides a point of departure for a reconstruction of theory that, from within the theory, opens up possibilities of interpretation that also challenge the theory-centred ambition (on the parallel to Descartes, see Toulmin, 1990: 56–137). Recontextualization offers a way to redress the biases of decontextualized theory, and this does not mean a Romanticist emphasis on ‘intrinsic meaning’ and the unique in experience (cf. Ashley, 1989: 278). The nexus of theory and practice, which is there in the text but which, beyond the text, deals with a historically situated moral agency, offers a point of departure for an epistemic turn that transcends the bifurcation of empiricist and rationalist epistemology. The question I have in mind is about the ‘how’ rather than the ‘what’ of specific experience. It is about the modes of encountering and making sense of the world, modes that through their habitual and institutional mechanisms can also become modalities of professional activity, such as the theory-centred episteme discussed above. A pragmatist re-interpretation of the texts of the early realists, for example, can elucidate how the ideals and guidelines for statesmanship and diplomacy arise from a world-experience that is different from but also partly similar or isomorphic to ours, and what commensurability there is, on this basis, in the logics of practice which in the different historical contexts generate policies in order to control perceived threats. Such inquiry and assessment of the legacy of IR theory seeks to sustain a living discourse diachronically through time without turning into a study of past historical praxis.23 Without bypassing the ‘weight of the discourse’ (Foucault),24 it starts out with situated moral agency and collective human intentionality and, on this basis, recognizes the inseparability of lived experience and the structures of experience that organize instances of experience. In the ontological sense, pragma means that whatever ‘is’ for a human interpretant exists not by a substance but by the regularities that endow it with its being. In the pragmatist research orientation, pragma (from the Greek word ‘business’, originally ‘a thing done’)25 means more than a way of carrying out the ‘business’ of research. It involves a critical assessment of the body of previous knowledge and requires that a new practice brings some advancement in relation to it. Like William James, John Dewey – the most influential pragmatist figure in social science and an author to whom the present-day discussion in IR in most cases makes reference – was interested in the question of how the powers of habit that maintain life serve to channel all thought, including the original of creative invention, and how the disposition of habitual responses evolves in the encounter of new types of problems. Dewey’s pragmatist ethics sought to cure the social and individual alienation that in his argument originates from the legacy of Western thought in ontological formalism, i.e. a dogmatic application of Plato’s idealism. Dewey emphasized that the ‘physician is lost who would guide his activities of healing by building up a picture of perfect health’; instead, the physician needs to employ ‘what he has discovered about actual cases of good health and ill health and their causes to investigate the present ailing individual so as to further his recovering; recovering, an intrinsic and living process ...’ (Owen, 2002: 670). Void of the inside knowledge, which involves a reflective relationship to previous practice, praxis (an established or customary practice) is like touching without realizing how by the same act one is being touched, i.e. the static position and alienation which Dewey argued were at the root of social problems (Dewey, 1981: 620–43).

### 2AC AT Forever War

#### Conflicts have discernable causes and resolutions---specific proposals are key---removing intervention as a tool is worse

Singh 19 [Michael, M.B.A., Harvard University (Baker Scholar); B.A., Princeton University, Lane-Swig Senior Fellow and managing director at The Washington Institute and a former senior director for Middle East affairs at the National Security Council, 11/6/19, “Why the talk of ‘endless wars’ misses the mark”, https://www.washingtonpost.com/opinions/2019/11/06/why-talk-endless-wars-misses-mark/]

It’s a notion that is difficult to resist — who exactly is for “endless war,” after all? — and rooted in deep public frustration with the costly but seemingly fruitless interventions of the post-9/11 era. But **as a guide to** policymaking, **opposition to** “forever wars” **is not useful**. **Such terms conflate three separate concerns, each of which demands separate consideration.** First and most fundamentally, **opposition to “endless wars” reflects skepticism regarding the deployment of U.S. military forces overseas, and of intervention as a policy tool.** According to the Defense Department, there are about 200,000 U.S. service members deployed overseas in nearly 170 different countries or territories — a remarkable number given that there are just 195 countries in the world. **Yet the differences among the** **United States’** **various military missions are stark**, **and each deserves** independent scrutiny rather than blanket opposition or, for that matter, knee-jerk support. **It should be obvious that the 55,000 U.S. troops in Japan are engaged in different work than our 5,200 or so service members in Iraq**. Less well-recognized, however, is how much **even one combat mission in the Middle East differs from another. At its height, the Iraq War involved** almost **160,000 U.S. soldiers.** **The** U.S. military **mission in Syria**, on the other hand, has **involved** roughly **2,000 soldiers** who have rallied a local partner force 70,000-strong, enabled a coalition air campaign, and provided a platform for civilian stabilization activities. It was an altogether more economical deployment, and perhaps even a model for future interventions. Yet both President Trump and his critics have lumped Syria in with Iraq and Afghanistan as another example of “endless war.” The second concern covered by the term “endless war” is the seeming overemphasis on the broader Middle East in U.S. foreign policy in recent decades; critics use the term to inveigh against involvement in Syria or Afghanistan far more often, than say, Somalia. As we engage in what seems an inevitable shift away from the Middle East, however, we will find that the real problem is less the prioritization of the Middle East than the heavily military focus of U.S. policy there. External intervention in the region clearly hasn’t always promoted stability — just see post-2003 Iraq. And major wars aren’t the only problem. The United States also sends the lion’s share of our global security assistance — training and equipment — to the Middle East. Yet as events of the past several years attest, these programs have an underwhelming record of delivering security. On their own, military intervention and security assistance can’t solve the deeper problems that drive conflict, such as stagnant economies or repressive political systems. Nor have they stemmed the growth of violent extremism, which has seen a manifold increase since the terrorist attacks of Sept. 11, 2001. Yet, ironically, even as we have grown weary of intervening, we have also decreased our commitment to promoting economic reform and political liberalization, or to the diplomatic leadership required to prevent conflicts or resolve them short of war. Finally, worries about “endless war” often stem from a mismatch between stated U.S. objectives and the means we are willing to use to achieve them. This has been a bipartisan malady, and the causes are complex. Our immense military and economic advantages lead us to set unrealistic goals, and the impatience of our politics sometimes leads us to withdraw support even from achievable missions Syria provides examples of both fallacies. One can fault President Barack Obama, who insisted that “Assad must go” but failed to devise a strategy that could come close to delivering such an outcome. But one can also fault Trump, who refused to spend even the funds that Congress appropriated for stabilization in northeastern Syria and who has reduced a successful 2,000-troop mission to one consisting of several hundred — apparently without scaling back its objectives. **There is no catch-all approach that will end the “endless wars.” One thing we clearly shouldn’t do**, however, **is** to **renounce military intervention as a policy tool.** **The use or the threat of military action has** often **been a force for** peace and stability — see, **for example, Cold War deployments to Europe, or the NATO mission in the Balkans during the 1990s.** **If we reduce interventions by ignoring problems around the world, our solace will be temporary as small, far-off crises grow into large, unavoidable ones. The real antidote to “endless war” is more** disciplined policymaking. The United States needs to adopt strategies that will reduce the need for interventions, **reinvigorating our use of tools like diplomacy, deterrence, and economic statecraft.** And when intervention becomes necessary — which it inevitably will — we should use force economically and with clear, realistic aims in mind. **A less engaged** United States **benefits neither the world nor ourselves; a** United States **energetically committed to policies designed to prevent conflict will advance not only our own interests, but those of humanity writ large.**

#### Endless war is a myth – withdrawal is what created the current crisis with Russia

Carafano 19 [James Jay Carafano, a leading expert in national security and foreign policy challenges, is The Heritage Foundation’s vice president for foreign and defense policy studies, E. W. Richardson fellow, and director of the Kathryn and Shelby Cullom Davis Institute for International Studies. Carafano holds a master's degree and a doctorate from Georgetown University as well as a master's degree in strategy from the U.S. Army War College. “What Those Decrying America’s "Endless Wars" Are Really Talking About.” https://www.heritage.org/defense/commentary/what-those-decrying-americas-endless-wars-are-really-talking-about]

From the presidential candidate debate stage to new think tanks, voices from both left and right are demanding an end to America’s endless wars. Only one problem: We’re not fighting any endless wars. No matter. The endless-war warriors want us to do less on the world stage. Even in this age of great power competition, these “new” isolationists would prefer America step off the playing field and wave from the sidelines. It’s a strategy that would work well for Beijing, Tehran and Moscow – but not for the U.S. No one is denying we’ve seen plenty of wars – and long ones at that. The U.S. has fought more than it ever wanted, including the global war on terrorism and related conflicts in Iraq and Afghanistan. But America’s endless war days have ended – at least for now. That’s not to say we don’t have troops in combat zones around the world. But, by any reasonable definition, America just isn’t at war. We are, for sure, dealing with the aftermath of conflicts in Iraq and Afghanistan. But President Obama’s withdrawal of U.S. forces from Iraq marked the end of that war, and he transitioned the effort in Afghanistan all-out fighting to an advice-and-assist mission. Today, what America does around the world is pretty much what it has been doing since 1945 – providing forward presence, deterrence, counterterrorism, training, assistance, and freedom of navigation. That’s important work and a heavy lift, but it ain’t war. So what the carpers are really complaining about is not “endless wars” (an admittedly powerful albeit dishonest catch-phrase), but U.S. foreign policy in general. So the question is: what foreign policy do they want instead? The U.S. is a global power with global interests and responsibilities. That’s not a choice; it’s just who we are. No one today is arguing that the U.S. can child-proof the world to make America safe. The overly ambitious efforts of the George W. Bush era clearly created as many problems as they solved. But, walking away from problems doesn’t work well either – as the Obama team more than amply demonstrated. They ended the war in Iraq. And, for that, we got a war with the caliphate. They ended the war in Afghanistan. For that, we got the resurgence of the Taliban. The reset with Russia produced a war in Ukraine. Tried to buy Iran off, and that didn’t work. And they stood by as China moved to make the South China Sea its own and North Korea’s Kim built out his nuclear arsenal. Trump has tried to stake out a middle ground. He isn’t interested in being the world’s babysitter, but he is willing to stand up and demonstrate sufficient resolve to protect America’s interest. He has managed to do that – and finish off the Caliphate – without starting any new wars. So where are the endless wars? Or, more to the point, what’s so bad about this administration’s foreign policy? Look around, and you’ll see Russia stonewalled in Crimea. Iran just failed to close the Straits of Hormuz. The DPRK is negotiating. The Stars and Stripes proudly sail the South China Seas, and there is nothing Beijing can do about. Apparently, that’s not good enough for the end the endless-war warriors. They want us to do even less. But “do less” is a poor prescription for dealing with the world as it is. History supplies overwhelming evidence that weakness and indifference do not deter aggression and exploitation, they invite it. What America needs now are discussions about how to prudently exercise its power in a complex world: what’s the right balance of multilateral action, prodding allies, making compromises, and standing strong. What we don’t need are politicians and pundits who suggest that, if America simply does nothing, our enemies and competitors will behave just as they should and everything will be just fine.

### 2AC AT Fear

#### The problem is that we don’t fear enough. Debate around existential risks is key to civic engagement and academic research to develop risk mitigation strategies.

Javorsky 18 [Emilia, a Boston-based physician-scientist focused on the invention, development and commercialization of new medical therapies. She also leads an Artificial Intelligence in Medicine initiative with The Future Society at the Harvard Kennedy School of Government. Why Human Extinction Needs a Marketing Department. January 15, 2018. https://www.xconomy.com/boston/2018/01/15/why-human-extinction-needs-a-marketing-department/]

**Experts at Oxford** University **and elsewhere have estimated that the risk of a global human extinction event** this century—or at least of an event that wipes out 10 percent or more of the world’s population— **is around** 1 in 10. **The most probable culprits** sending us the way of the dinosaur **are** mostly anthropogenic risks, meaning those created by humans. These include climate change, nuclear disaster, and more emerging risks such as artificial intelligence gone wrong (by accident or nefarious intent) and bioterrorism. A recent search of the scientific literature through ScienceDirect for “human extinction” returned a demoralizing 157 results, compared to the 1,627 for “dung beetle.” I don’t know about you, but this concerns me. Why is there so little research and action on existential risks (risks capable of rendering humanity extinct)?

**A big part of the problem is a** lack of awareness **about the** real threats **we face** and what can be done about them. **When asked to estimate the chance of an extinction event in the next 50 years, U.S. adults in surveys reported** chances ranging from 1 in 10 million to 1 in 100, certainly not 10 percent. **The** awareness **and** engagement issues **extend to the** academic community **as well, where** a key bottleneck **is a lack of talented people** studying existential risks. **Developing viable** risk mitigation strategies **will require widespread** civic engagement **and** concerted research **efforts**. Consequently, **there is an** urgent need **to improve the** communication **of the** magnitude **and importance of** existential risks. The first step is getting an audience to pay attention to this issue.

#### Fear of death is critical to prevent violence and make life meaningful – discussion is key – our framing is productive

Williams 11 (Michael, International Affairs Prof @ University of Ottawa, “Securitization Theory: How Security Problems Emerge and Dissolve,” pg. 219-220) \*\*\*edited for ableist language

Fear has generally had a bad name in modernity. It has been seen as something to be banished -freedom from it was the target of one ofFranklin Roosevelt's 'four freedoms', and it is today one of the unifying elements of the Human Security agenda and, in certain forms at least, of Critical Security Studies. From a different but equally hostile perspective, some philosophic accounts see modernity as based in fear, and its (generally destructive) preoccupation with security as a consequence of this more basic foundation. To still others, fear is an instrument which, far from being part of the existential condition of modernity, has been made more powerful and effective by the structures of modem politics. 5 Each of these three views, despite their apparent (and by no means insubstantial) differences, are united in their basic vision off fear as negative. And there is no doubt that their assault on the politics of fear and its negative effects is an indispensable element of any serious analysis of security. Yet it is also the case that to reject fear completely, or to see it as wholly antithetical to security is both analytically and politically blinding[ineffective]. In contrast to these modem views of fear, many older traditions of thought exhibit a rather different sensibility, and provided a more nuanced and potentially more productive view of the politics offear. To take one example, in the eyes of perhaps the greatest political philosopher of fear, Thomas Hobbes, the human condition was dominated by multiple and often contradictory and competing forms of fear: the fear of death itself; the fear of violent death at the hands of others, which marked a fear of dishonor ( of Pride and the sense of self) more than it did of mere mortality;6 fear of the unknown and unknowable future and its potential hazards (Blits 1989).7 Fear, in short, was everywhere, and while Hobbes freely admitted that he might have felt its effects more acutely than many people, he was convinced nonetheless that it dominated the human condition, and that a complete escape from fear was possible only temporarily in sleep, and ultimately, in death. Yet Hobbes did not view fear wholly negatively. Indeed, he believed that the absence of fear could be as dangerous as its over-abundance. Disregard of the fear of death as a result of vanity and the search for glory or honour, he believed, could lead to the worst forms of conflict, while misplaced certainly (belief in the security of knowledge) could result in dogmatism, intolerance and violence in the name of universal truths. Recognizing these dangerous beliefs and fearing their consequences, however, could act as a positive constraint on human excesses, and foster peace. Fear arising from the absence of specific forms of fear (of, for instance, conflicts arising from Vain-glory or religious zealotry that overwhelmed the fear of death, or that arose from a failure to acknowledge the limits human knowledge and an unwillingness to live with the fear presented by the inability to control an essentially uncertain future) could lead to a politics that restrained these beliefs and behaviours. In other words, the fear off fear (and of the practices likely to lead to extreme fear) could act as a check upon the politics of fear. However difficult it might be to achieve, fear was in principle capable of supporting forms of positive, pacific action.

### 2AC Consequentialism Good

#### Failing to prevent a horrible outcome is just as bad as causing it – don’t side with moral evasion

Nielsen 93 [Kai Nielsen, Professor of Philosophy, University of Calgary, Absolutism and Its Consequentialist Critics, ed. Joram Graf Haber, 1993, p. 170-2] we do not endorse gendered language

Forget the levity of the example and consider the case of the innocent fat man. If there really is no other way of unsticking our fat man and if plainly, without blasting him out, everyone in the cave will drown, then, innocent or not, he should be blasted out. This indeed overrides the principle that the innocent should never be deliberately killed, but it does not reveal a callousness toward life, for the people involved are caught in a desperate situation in which, if such extreme action is not taken, many lives will be lost and far greater misery will obtain. Moreover, the people who do such a horrible thing or acquiesce in the doing of it are not likely to be rendered more callous about human life and human suffering as a result. Its occurrence will haunt them for the rest of their lives and is as likely as not to make them more rather than less morally sensitive. It is not even correct to say that such a desperate act shows a lack of respect for persons. We are not treating the fat man merely as a means. The fat man's person‑his interests and rights are not ignored. Killing him is something which is undertaken with the greatest reluctance. It is only when it is quite certain that there is no other way to save the lives of the others that such a violent course of action is justifiably undertaken. Alan Donagan, arguing rather as Anscombe argues, maintains that "to use any innocent man ill for the sake of some public good is directly to degrade him to being a mere means" and to do this is of course to violate a principle essential to morality, that is, that human beings should never merely be treated as means but should be treated as ends in themselves (as persons worthy of respect)." But, as my above remarks show, it need not be the case, and in the above situation it is not the case, that in killing such an innocent man we are treating him merely as a means. The action is universalizable, all alternative actions which would save his life are duly considered, the blasting out is done only as a last and desperate resort with the minimum of harshness and indifference to his suffering and the like. It indeed sounds ironical to talk this way, given what is done to him. But if such a terrible situation were to arise, there would always be more or less humane ways of going about one's grim task. And in acting in the more humane ways toward the fat man, as we do what we must do and would have done to ourselves were the roles reversed, we show a respect for his person. In so treating the fat man‑not just to further the public good but to prevent the certain death of a whole group of people (that is to prevent an even greater evil than his being killed in this way)‑the claims of justice are not overriden either, for each individual involved, if he is reasonably correct, should realize that if he were so stuck rather than the fat man, he should in such situations be blasted out. Thus, there is no question of being unfair. Surely we must choose between evils here, but is there anything more reasonable, more morally appropriate, than choosing the lesser evil when doing or allowing some evil cannot be avoided? That is, where there is no avoiding both and where our actions can determine whether a greater or lesser evil obtains, should we not plainly always opt for the lesser evil? And is it not obviously a greater evil that all those other innocent people should suffer and die than that the fat man should suffer and die? Blowing up the fat man is indeed monstrous. But letting him remain stuck while the whole group drowns is still more monstrous. The consequentialist is on strong moral ground here, and, if his reflective moral convictions do not square either with certain unrehearsed or with certain reflective particular moral convictions of human beings, so much the worse for such commonsense moral convictions. One could even usefully and relevantly adapt herethough for a quite different purpose‑an argument of Donagan's. **Consequentialism** of the kind I have been arguing for **provides so persuasive "a theoretical basis for common morality that when it contradicts some moral intuition, it is natural to suspect that intuition, not theory, is corrupt**."" **Given the comprehensiveness, plausibility, and overall rationality of consequentialism, it is not unreasonable to override even a deeply felt moral conviction if it does not square with such a theory**, though, if it made no sense or overrode the bulk of or even a great many of our considered moral convictions, that would be another matter indeed. **Anticonsequentialists** often **point to the inhumanity of people who will sanction** such **killing of the innocent, but cannot the compliment be returned by speaking of the even greater inhumanity, conjoined with evasiveness, of those who will allow even more death and far greater misery and then excuse themselves on the ground that they did not intend the death** and misery **but merely forbore to prevent it?** In such a context, such reasoning and such **forbearing to prevent seems to me to constitute a moral evasion**. I say it is evasive because **rather than steeling himself to do what in normal circumstances would be a horrible and vile act but in this circumstance is a harsh moral necessity**, **he allows, when he has the power to prevent it, a situation which is still many times worse. They\* tries to keep their\* `moral purity' and avoid `dirty hands' at the price of utter moral failure and what Kierkegaard called `double‑mindedness.' It is understandable that people should act in this morally evasive way but this does not make it right.**

#### Moral uncertainty proves extinction outweighs – if you aren’t 100% sure their arg is true, keep people to figure things out

Bostrom 12 [Nick Bostrom, Faculty of Philosophy & Oxford Martin School University of Oxford. Existential Risk Prevention as Global Priority. 2012. www.existential-risk.org/concept.html]

These reflections on moral uncertainty **suggest an alternative, complementary way of looking at existential risk**; they also suggest a new way of thinking about the ideal of sustainability. Let me elaborate.

**Our** present understanding **of** axiology **might well be** confused. **We** may not now know — at least not in concrete detail — **what outcomes would count as a big win for humanity**; we might not even yet be able to imagine the best ends of our journey. If we are **indeed profoundly** uncertain **about our** ultimate aims, then we should recognize that **there is a great option value in** preserving — and ideally improving — **our ability to** recognize value **and to** steer the future **accordingly**. Ensuring **that there will be a** future **version of** humanity with great powers and a propensity to use them wisely **is** plausibly **the best way available to us to** increase **the** probability **that the future** will contain **a lot of** value. **To do this,** we must prevent **any** existential catastrophe.

## Realism Good

### 2AC Realism Good

#### Even if realism’s foundations are problematic, it’s theoretically useful for understanding IR – rejecting it outright is ahistorical and causes worse violence by greenlighting ethically untenable positions like the alt

Abraham 17 [Kavi Joseph, Johns Hopkins University. “Making Machines: Unlikely Resonances between Realist and Postcolonial Thought,” https://academic.oup.com/ips/article-abstract/11/3/221/3798787]

This passage marks out one of the biggest obstacles to connecting realist and postcolonial thought: race. One would be hard pressed to find in realist theorizations anything resembling a supple understanding of race and racism (Vitalis 2015)— though Carr (2001b, 107) demonstrates a comparatively great deal of reflexivity on postcolonial liberation (see fn. 2 above). Even in Williams’s (2005) “wilful” realist tradition, there is scant discussion of how an embedded ethic of critical self-limitation fared in the context of racial or other forms of radical difference. Absent an engagement with the analytics of postcolonial thinking, or the diverse ways in which white supremacy, patriarchy, and heteronormativity inflect past and present liberal imperial formations, willful realism does not address the categories that threaten to push prudential skeptics toward violent responses, that pose limitations to an ethos of limits. As evidenced in Morgenthau, failure to think critically about race opens up the way for Morgenthau’s theoretical practice to be driven toward resentful rather than careful ends. It is at this juncture that those concerned with contemporary imperial formations are confronted with a number of possible responses: one is to deem realism, in all its complex and contradictory manifestations, as a failed, unethical, and fundamentally racist/imperial project. A second response is to politically align against liberalism, while holding this partnership at arm’s length. A third response, derived from Ayoob’s (2002) subaltern realism, is to work on an epistemic register, selectively taking insights from realist traditions that help better explain the neocolonial world. Morgenthau’s racist interjections should be critiqued and confronted—perhaps by outlining the innumerable non-Western contributions to the making of so-called Western modernity (Hobson 2004)—but this failing does not delegitimize other realist insights. What is important for Ayoob’s (2002) accommodationist stance is to combine plausible realist insights with other categories that can grasp the extent of global politics, including the dynamics of the postcolonial experience, better. The final response is the one I advance. To adopt a mode of argumentation concerned with building a counter-imperial machine is to neither dismiss constituencies that become caught up in imperial formations, nor merely to tactically align with them; rather, establishing resonant connections among postcolonial and realist lines of thought, highlighting shared dispositions to difference, is to push the latter toward repositioning itself on new ethical lines that limit contemporary forms of violence. To recover a minor position in realism is not to accept all realist positions, nor is it to synthesize or convert any theoretical line into a coherent framework. It is, however, to amplify the shared spirituality that informs both realist and postcolonial thinking, drawing constituencies toward prudential rather than imperial defenses of difference. It is to furnish current research agendas with an anti-imperial focus, to seek the creative possibilities that may arise when divergent constituencies meet, interfuse, and shift. Thus, our response to Morgenthau, as to other realists, is to cultivate the connections that do exist, not for epistemic reasons but for a political project that strengthens counter-imperial movements. Thinking from the Present By way of conclusion, it is important to reiterate the politics that motivates a theoretical project of linking realist and postcolonial thinking. If the ends of this project were to simply gather critiques of liberalism and its relationship to imperial practices, then certainly a return to classical realist thought adds little epistemic value over and above postcolonial approaches. However, the ends of this argument are to outline and energize a counter-imperial machine, to cultivate a shared spirituality that can gather diverse and divergent constituencies to confront dangerous practices. In my estimation, countering an imperial machine that operates in complex ways and at complex sites requires a political strategy as unwieldy and diffuse, linking constituencies that we may otherwise dismiss. That a tradition of realism regularly circulates through halls of power across the globe should be reason not to reject righteously but rather to leverage its authorized status. We can talk about imperialism, knowledge production, and race here, while they can talk about anarchy, power, and self-interest there—or we can theoretically work on the lines of thought that reverberate among us. To reiterate, building a countermachine is not driven to “pragmatic” reconciliation or consensus and, thus, remains distinct from the “eclecticism” of other plural approaches popular in IR today. While the combinatory logic of paradigmatic synthesis has its place, the connections between realist and postcolonial thought articulated here are made in a far more agonistic manner. Rather than produce something like a “postcolonial-realism,” this argument involves pushing contemporary realist scholarship toward new research agendas and new forms of critique that both capture a spirit internal to its own traditions while confronting the realities of contemporary global politics. It engages with minor positions along the realist canon to orient today’s realism away from the logic of great power politics operating under anarchy toward an understanding of how the logic of liberal order permits forms of imperial intervention. Needless to say, drawing together realist and postcolonial thought, as this essay has done, can be met with analytical skepticism and political hostility. A mode of argumentation that refuses comparisons of theoretical cores or non-truncated readings of select theorists strikes a note of analytical evasion. To this there is no defense—other than that already discussed at length. On the other hand, if the expressly political purpose of this work is accepted, the argument anticipates strong political reservations: why align the project of postcolonial theory with realism, an unethical tradition of militarism and realpolitik? To this I would respond that while a kind of strategic essentialism has its place, reducing “realists” to a coherent body of thought not only obscures the complexity of their thinking (see never-ending interpretations of Machiavelli as an example) but reproduces the narrative of transhistorical unity that some realists use to authorize unethical policy programs in the first place. More critically, however, in embodying an unproductive ahistoricism, it poses conventional realist categories of anarchy, selfinterest, and military power as the political problem to confront whereas the present historical context demands attunement to how some of these drives (militarism, national interest) connect with discrete problems of liberalism and imperial practices. In fact, there are good reasons to think that the dominance of (neo)realism in IR is overstated (Walker and Morton 2005; Maliniak et al. 2011) and that the ascension of liberal IR theory is sociologically tied up with the present hegemony of a US liberal world order (Sterling-Folker 2015). In other words, while realism may have been a productive foil in Cold War bipolarity, we must theorize from the present. In doing so, we may find that countering imperial formations may benefit from resonances established not just among postcolonial, feminist, poststructural, and other “critical” theorists but contemporary realists who identify links between liberalism and imperialism (Walt 2013). Indeed, if realism as a policy program defending the national interest is entangled with current militaristic and imperial interventions, we should push the premise of this statement, that difference should be defended, in anti-imperial and prudential directions. Doing so may allow new openings to emerge in the present sense of closure, new strategies to think and defend alternative politics. In this way, we may more fully embody postcoloniality by not being satisfied with either narrow critique or brash conversion but rather attentive translation.

#### Prefer realist ethics – accepting the uncertainty of anarchy creates the conditions of possibility for contingent ethical decision-making that embraces the incalculability of life – reject their deterministic framing

Lundborg 19 [Tom, Associate Professor of Political Science and Director of Studies at the Swedish Defence University, “The ethics of neorealism: Waltz and the time of international life,” European Journal of International Relations, Vol. 25(1) 229–249]

**Derrida’s notion of** **the** violent opening of ethics **fits** remarkably **well with the** two core assumptions **of Waltz’s theory** of international politics: **the** anarchic structure **of the** international political **system** **and states’** desire to survive within this system. On this basis, it can be argued that there is, indeed, an ethics of neorealism. **It is found in the** ‘**Waltzian baseline’** **rather than in attempts to use that baseline** to establish law-like patterns of behaviour.12 To grasp the ethics of neorealism, it is therefore necessary to shift focus from causal laws and testable hypotheses, to the structural conditions that shape and affect the behaviour of states in a non-deterministic manner.13 Hence, the ‘structure’ in Waltz’s theory **has to be grasped as an open structure** **that leaves ample room for** chance and contingency. Crucially, **if we could know** for certain **what states will do** on the basis of either the structure of the system or some predetermined motives of the subjects within the system, **the** uncertainty **of international life would** disappear and the ‘politics’ of international politics would lose its meaning.14 **Rather than trying to rectify the lack of certainty** **by creating a stronger sense of certainty, it is** therefore imperative **to** *affirm* the **uncertainties created by the system**. **It is important,** moreover, **to oppose the distinction between** ethical desirability **and** political possibility, **since the** reproduction of this **distinction** blocks from view **the conditions of** international life that make ethical thinking and action possible in the first place. Positivist social science and liberal interpretations of Kant are thus, very crudely put, the main obstacles to grasping the ethics of international life. In resisting both moves, **neorealism** does not **seek to close down** **the** violent opening of ethics **inherent in the** structure of anarchy, for example, **by formulating metaphysical ideals** **informing states how they** *should* **act or how they** *ought* **to become friends rather than enemies**. **There can be** no absolute friendship between states, **and no state can ever offer** absolute hospitality to another state. **At the heart of every** inter-state **relation**, **there is** mistrust, uncertainty and incalculability. **To positively affirm the latter** **is not to say that uncertainty** or incalculability **is good per se.** Rather, **it implies that they are** seen as basic and irrefutable conditions of international life, which, consequently, are not even desirable to overcome. Hence, it also implies that as long as there is international life, there must be ‘the ominous shadow of the future [that] continues to cast its pall over interacting states’ (Waltz, 2000: 39). Crucially, Waltz’s reference to this shadow should not be read as an expression of determinism. It expresses rather an affirmation of uncertainty: the ‘uncertainty of each about the other’s future intentions and actions’ (Waltz, 1979: 105). In order to give friendship in international politics a chance, so to speak, the possibility that a friend suddenly becomes an enemy must never be eliminated. Attempts to create absolute trust in inter-state relations are therefore not only impossible to achieve in the practical sense, but essentially undesirable.15 Along similar lines, Derrida explains how friendship is possible only if one remains open to the deception of the other, since it is precisely the unconditional openness to whatever may happen in the encounter between self and other that makes it possible to develop any sort of friendship in the first place (Derrida, 2005: 219). Even if we were to accept Alexander Wendt’s (1999) distinction between different ‘cultures of anarchy’, some of which are more ‘friendly’ than others, it is not self-evident that a culture in which friendship is prioritized over enmity is actually a better one. This is because in order to exclude the possibility that a friend may suddenly become an enemy, one must first eliminate the time of international life that makes the self–other encounter possible in the first place. For the same reason, the key message of democratic peace theory — that all states should become democracies in order to minimize or eliminate the possibility of wars — is not only practically impossible, but also ethically undesirable. It is impossible to verify because there is no democracy that is immune to corruptibility (Waltz, 2000: 10), but, in addition to that, it can be seen as undesirable since the notion that all states must conform to the same universal ideal cancels out their freedom to act, to take moral responsibility and so on. The undesirability of a system that eradicates violence, borders and discrimination is further underlined by Waltz (1979: 111–114) in his discussion of the ‘virtues of anarchy’. Therein, he attacks the idea of transforming the international system into a world government. Not only would such a transformation ‘be an invitation to prepare for world civil war’ (Waltz, 1979: 112), but it would take away the constitutive violence at the heart of inter-state relations in the structure of anarchy. The constant possibility of war in the international system means that states will always be wary of provoking others in the search for security. As he puts it: The constant possibility that force will be used limits manipulations, moderates demands, and serves as an incentive for the settlement of disputes. One who knows that pressing too hard may lead to war has strong reason to consider whether possible gains are worth the risks entailed.… The possibility that conflicts among nations may lead to long and costly wars has … sobering effects. (Waltz, 1979: 113–114) In this way, **the** conditions of peace in the international system **can be said to rest on the constant** possibility of war. **In making this point**, **Waltz argues** *against*moral universalism. Hence, unwittingly or otherwise, **he** also opens up space for ethical negotiation **by recognizing the finitude of the political subject**, **who is free to interact with others only on the condition that self and other do not have to conform to the ‘same’ universal ideal**. **The subject is** thus **able to take** moral responsibility **and ponder on how to make ethical decisions**, which, without difference and alterity, would turn into a strictly formal procedure based on the ‘mechanical application of rules’ (Zehfuss, 2009: 146). Responsibility and ethical decisions are, thus, made possible precisely by the impossibility of predetermining what is the ‘right’ decision in any given context. As Derrida argues, irrespective of how thorough the decision-making procedure is, and regardless of how much knowledge is acquired before taking a decision: the instant of the decision, if there is to be a decision, must be heterogeneous to this accumulation of knowledge. Otherwise, there is no responsibility. In this sense only must the person taking the decision not know everything. Even if one knows everything, the decision, if there is one, must advance toward a future that is not known, that cannot be anticipated. (Derrida, 2002b: 231) The impossibility of anchoring the decision in rational calculation is, in this sense, what creates the chance for any decisions to be taken at all. The instant of the decision belongs, then, not to a fully present moment in which the subject calculates the future consequences of the decision, but to a future that is incalculable (see Derrida, 2002a). It is precisely this incalculability, and the uncertainty of the future, that Waltz’s conception of anarchy positively affirms. Rather than making the instant of the decision obsolete by transforming the decision into a mere application of rules, anarchy makes the ethical decision ‘possible’. **Even if Waltz** repeatedly **claims** that **the desire to survive is** a **purely pragmatic** assumption made strictly for the purpose of constructing an explanatory theory, **it is not neutral** or innocent. First and foremost, Waltzian **neorealism expresses an ethics due** **to the way it** affirms states’ desire to survive **by stipulating** the necessary **conditions of their survival**. **More precisely**, **it** affirms the uncertainty of international life **by** refusing to reduce **the play of relations between states to a** calculable formula **or a regulative ideal**, **and that rather** embraceschance **and** contingency **as central features of the anarchic system** — features that make states simultaneously free and insecure.16 **In this light, the primary significance of Waltz’s theory** **is** not as an explanatory theory, but **as a theory that affirms the time of international life**, defined by the uncertainty of the future **and the logic of the erasable mortal trace**.17 It is this notion of the future **that makes it possible for states**, as finite political subjects, **not only to survive**, **but also to try to take moral responsibility and** make ethical decisions. Why universal ethical ideals are both impossible and undesirable What are the implications of my reading of Waltzian neorealism as an ethics? First of all, **it contributes** to **a new understanding of the** difficulties inherent **in any attempt to theorize what it might mean to** replace the structure of anarchy **with an** international or world political **order** that is supposedly ‘more’ ethical. **If ethics is inextricably interlinked** **with** the structural **conditions of survival**, then any attempt to challenge neorealism from an ‘ethical’ perspective **must do so by** replacing one structure **of survival** with another, **and** there can be no guarantees that the new structure will be less violent. **While this does not** in any way **prevent such attempts from being made**, **it does highlight the** risky nature **of trying to resolve problems of war and violence** in international politics **on** ethical terms. For example, the idea of creating a new form of political community that transcends the exclusionary borders of states may seem naturally desirable (e.g. Linklater, 1982). Yet, regardless of how sophisticated theories become in terms of articulating the content and meaning of such a community, there can be no guarantees that attempts to actualize it will not result in even more violence. There are no guarantees, as John Mearsheimer (1994: 44) puts it, **that ‘a** fascist discourse **far more violent than realism will not emerge as the** new hegemonic discourse**’**.

#### Realism is necessary and inevitable – we must deal with how states actually act based on the international system, not how we wish they would

Parsi 05 [Trita, founder and president of the National Iranian American Council, “Israel-Iranian Relations Assessed: Strategic Competition from the Power Cycle Perspective”, in Homa Katouzian and Hossein Shahidi, Iran in the 21st Century, GDI – MJS]

Realism is the dominating paradigm in international relations. Characterized by its hard-boiled willingness to see the world as it is and study international relations as an objective reality, it lacks normative guiding principles. It deals with what is and not with what ought to be. Using the metaphor of anarchy to describe the international system, realists argue that the only order is that which emerges from competition between states-the system's principal actors under anarchy. Realists posit that states are rational actors whose primary purpose is to secure their own survival, irrespective of their internal political makeup. Security, in turn, is achieved by maximizing power. In the words of Kenneth Waltz, the international system is a self-help system in which a nation's security cannot be ensured except through their own actions.18 Yet, it is not a world of constant conflict. Stein describes the realist worldview as not necessarily one of perpetual warfare, but of perpetual conflict since crises are recurring and inevitable.19 Tracing their intellectual lineage to Machiavelli and Thucydides, realists refrain from putting their faith in international law and institutions, arguing that treaties cannot affect the fundamental principles of international relations. Neo-realism shares the basic assumptions of realism, but takes a systemic approach and emphasizes the structure of the international system and its affect on the interacting units and vice versa. Waltz posits that a system is composed of a structure and interacting units in which the definition of the structure is free of the attributes and the interactions of the units. The maneuverability of the states is limited by the structure of the system, which constitutes the setting in which states interact.

### 2AC Threats Real

#### Examining whether threats are real and whether our security responses are ethical is the only effective middle ground

Floyd ’19 [Rita, Department of Political Science and International Studies Senior Lecturer in Conflict and Security, “Introduction” in The Morality of Security, Cambridge Core, April 2019, pp 10-12, <https://doi.org/10.1017/9781108667814>]

Securitization has been heavily debated in the scholarly community. Among other things much discussion has focused on the issue of whether securitization is satisfied simply by audience acceptance of the securitizing move, or whether it has to involve extraordinary measures (Balzacq, Le´onard and Ruzicka, 2015). All securitization scholars accept, however, that security threats are socially and politically constructed, or in other words that: ‘Security issues are made security issues by acts of securitization’ (Buzan et al., 1998: 204). This has allowed scholars to recognize what Jef Huysmans calls ‘the political force of security’ whereby ‘[s]ecurity is a practice not of responding to enemies and fear but of creating them’ (2014: 3). An exclusive focus on the constructedness of security means, however, that securitization scholars tend to ignore whether or not the threats that inform securitization are real or otherwise. And as Thierry Balzacq argues, this has had the disadvantage of securitization scholars overlooking the fact that securitizing moves that refer to ‘brute threats’ are more likely to succeed because, ‘to win an audience, security statements must, usually, be related to an external reality’ (2011b: 13). Balzacq’s observation is important in the context of this book as it goes some way towards paving the way for the inclusion of objective existential threats into securitization analysis. As I will argue in this book, real threats are important for the purposes of just securitization theory as only these may constitute a just reason19 for securitization. The Copenhagen School’s refusal to ‘peek behind [threat construction] to decide whether it is really a threat’ (Buzan et al., 1998: 204) and the just war tradition’s insistence on real threats as just causes, appear to suggest insurmountable differences at the meta-theoretical level between the two theories. Importantly, however, the Copenhagen School’s unwillingness to, as they put it, ‘peek behind’ threat construction, does not stem from a denial that real threats exist (after all Wæver (2011: 472) recognizes that ‘lots of real threats exist’),20 but from the belief that the study of threat construction is ultimately more fruitful than pondering the presence of real threats (Buzan and Hansen, 2009: 213; Buzan et al., 1998: 204). Beyond this, the decision not to try and examine whether security threats refer to real threats is also – at least in part – driven by a strong normative conviction. Thus by focusing on the political force of security as opposed to whether or not threats are real, Wæver and the Copenhagen School highlight the fact that securitization is/was not inevitable; things could have been treated in a different way (for example, perceived threats could have been criminalized or simply politicized). This enables scholars following this logic to highlight that securitizing actors bear responsibility for framing things in this way. Wæver calls this ‘the politics of responsibility’ (2011: 472), which he explains as follows: ‘The securitization approach points to the inherently political nature of any designation of security issues and thus it puts an ethical question at the feet of analysts, decisionmakers and activists alike: why do you call this a security issue? What are the implications of doing this – or of not doing it?’ (Wæver 1999 cited in Wæver, 2011: 468; emphasis added). The significance of the fact that securitization is a political choice cannot be overstated; however, it is also the case that decision-makers are likely to consider securitization the right political choice when they believe that they are in fact dealing with a real threat. In other words, the possibility of framing the issue differently will not be tempting if they believe that there is a real threat. Given that the Copenhagen School and their followers cannot tell them anything about the actual objective existence of the threat, the framework seems of limited persuasiveness here; it is simply the securitizing actor’s belief against the scholar’s argument that things could and perhaps should be different. Indeed the Copenhagen School recognizes ‘our inability to counter securitization (say, of immigrants) with an argument that this is not really a security problem or that the environment is a bigger security problem’ as the securitization approach’s ‘main disadvantage’ (Buzan et al., 1998: 206). I propose that if the ethical goal of securitization analysis is that securitizing actors take responsibility for their actions, then a better strategy is to begin by (helping them in) judging the objective existence of a threat, because unless there is a real threat, securitization is most definitely the wrong political and ethical choice. Importantly, however, as I argue in this book, the existence of a real threat does not automatically necessitate securitization (indeed this remains a political choice), neither does it – by itself – render it morally permissible; the presence of real threats is rather one important requirement for securitization to be justified. In other words, just securitization is informed by the idea that securitizing actors are not only responsible for choosing to securitize, they ought to be responsible for securitizing in an ethical manner. In my view, the fact that the original variant of securitization theory excludes objective existential threats not on ontological, but at least partially on normative grounds means that a variant of securitization theory that includes real threats is at least permissible, provided, of course, that a theoretical framework that shows how we can know that threats are real is delivered. In this book, such a framework is set out in Chapter 2. 21 [FOOTNOTE 21 BEGINS 1 Some scholars may object to the possibility of combining insights of opposed theories on the grounds of inconsistency – for example, critical security studies, with its postmodern roots, with insights gained from analytical, moral and political philosophy. Interestingly, Wæver has faced similar charges of inconsistency for combining elements that ordinarily don’t go together (notably, Wæver refers to himself as a poststructural realist). To these critics Wæver offers this persuasive riposte: ‘This criticism presupposes that these larger groups are internally consistent and mutually isolated. On the contrary, we all know numerous examples of internally consistent theories that draw on several traditions – and many more examples of theories that stay within their “box” and yet are horribly inconsistent. Therefore, investigations of the internal consistency and productivity of research traditions should focus on distinct theories, not loose collections hereof’ (Wæver, 2015:124). Generally speaking, I am critical of the tendency to confuse theory with ideology, and thus disallowing and discounting anything outside of one’s perceived and tightly regulated theoretical remit. In the past in IR such thinking has led to bad scholarship; thankfully now scholars are working to dispel artificially imposed dichotomies, such as that on the relationship between causation and discourse (Kurki, 2008). FOOTNOTE 21 ENDS]

#### Some threats are real and not constructed – action is key to prevent them

Knudsen 1 [Olav, PoliSci Professor at Sodertorn, Post-Copenhagen Security Studies, Security Dialogue 32:3]

Moreover, I have a problem with the underlying implication that it is unimportant whether states 'really' face dangers from other states or groups. In the Copenhagen school, threats are seen as coming mainly from the actors' own fears, or from what happens when the fears of individuals turn into paranoid political action. In my view, this emphasis on the subjective is a **misleading conception of threat**, in that it discounts an independent existence for what- ever is perceived as a threat. Granted, political life is often marked by misperceptions, mistakes, pure imaginations, ghosts, or mirages, but such phenomena **do not occur simultaneously** to large numbers of politicians, and **hardly most of the time**. During the Cold War, threats - in the sense of plausible possibilities of danger - referred to 'real' phenomena, and they **refer to 'real' phenomena** now. The objects referred to are often not the same, but that is a different matter. Threats have to be dealt with both ín terms of perceptions and in terms of the phenomena which are perceived to be threatening. The point of Waever’s concept of security is not the potential existence of danger somewhere but the use of the word itself by political elites. In his 1997 PhD dissertation, he writes, ’One can View “security” as that which is in language theory called a speech act: it is not interesting as a sign referring to something more real - it is the utterance itself that is the act.’24 The deliberate disregard of objective factors is even more explicitly stated in Buzan & WaeVer’s joint article of the same year.” As a consequence, the phenomenon of threat is reduced to a matter of pure domestic politics.” It seems to me that the security dilemma, as a central notion in security studies, then loses its foundation. Yet I see that Waever himself has no compunction about referring to the security dilemma in a recent article." This discounting of the objective aspect of threats shifts security studies to insignificant concerns. What has long made 'threats' and ’threat perceptions’ important phenomena in the study of IR is the implication that **urgent action may be required**. Urgency, of course, is where Waever first began his argument in favor of an alternative security conception, because a convincing sense of urgency has been the chief culprit behind the abuse of 'security' and the consequent ’politics of panic', as Waever aptly calls it.” Now, here - in the case of urgency - another baby is thrown out with the Waeverian bathwater. When real situations of urgency arise, those situations are challenges to democracy; they are actually at the core of the problematic arising with the process of making security policy in parliamentary democracy. But in Waever’s world, threats are merely more or less persuasive, and the claim of urgency is just another argument. I hold that instead of 'abolishing' threatening phenomena ’out there’ by reconceptualizing them, as Waever does, we should continue paying attention to them, because **situations with a credible claim to urgency will keep coming back** and then we need to know more about how they work in the interrelations of groups and states (such as civil wars, for instance), not least to find adequate democratic procedures for dealing with them.

#### **Miscalc threats are real**

Mearsheimer 09 [John, R. Wendell Harrison Distinguished Service Prof at the Univ of Chicago, “Reckless States and Realism”, *International Relations* 23, <https://pdfs.semanticscholar.org/c297/97d80c833dea55d9fd1654b3961e66495ade.pdf>, accessed 7/9/19, GDI – MJS]

**To assume that states are rational is to say that they are aware of their external environment and they think intelligently about how to maximize their prospects for survival**. In particular, **they try to gauge the preferences of other states and how their own behavior is likely to affect the actions of those other states, as well as how the behavior of those other states is likely to affect their own strategy**. When they look at the different strategies that they have to choose between, they assess the likelihood of success as well as the costs and benefits of each one. Finally, states pay attention not only to the immediate consequences of their actions, but to the long-term effects as well. Nevertheless, **rational states miscalculate from time to time because they invariably make important decisions on the basis of imperfect information**. **They hardly ever have complete information about any situation they confront, which forces them to make educated guesses. This is due in part to the fact that potential adversaries have incentives to misrepresent their own strength or weakness, and to conceal their true aims.** But even if disinformation were not a problem, **states are often unsure about the resolve of opposing forces as well as their allies, and it is often hard to know beforehand how one’s own military forces, as well as those of adversaries, will perform on the battlefield**. Therefore, **rational states sometimes guess wrong and end up doing themselves serious harm.**

### 2AC AT Root Cause

#### Monocausal, ideological explanations of international relations fail and obscure the proximate dynamics that causal war and violence.

Rotter 8 [Andrew, Colgate history professor. 2008. “The Cultural History of Foreign Relations” in A Companion to American Cultural History, pp. 430-3]

Studies on cultural transmission have opened diplomatic history to new subjects and new interpretations, and constructively complicated its assumptions about what constitutes foreign relations. Some culturalists believe, however, that studies of fashion, tourism, and musical theater fail to address real power relations between nations. Fashion and tourism and musicals, they say, may reveal something about one people’s attitudes toward another; but to understand why nations behave as they do, it is essential to bring the state back into the analysis. How, for example, do such cultural analysands as race, gender, and language help us parse hard power, including the mechanics of empire and the conduct of war? Can the Geertzian approach explain not just the context but the content, and even the cause/effect, of US foreign relations? To be sure, many of the previously cited books do concern power; and the distinction between “cultural transmission” and “culture as power” may be artificial. Let us consider several specifi c ways in which historians have tried directly to connect attitudes, images, values, and prejudices to the practice of foreign policy, and the exercise of state power. Begin with race. For some years, scholars have noted that white racism has influenced US policy toward non-white others. For Michael Hunt, racism is one of three main elements of American ideology (1987). Reginald Horsman (1981) and Richard Slotkin (1985) have shown that white acceptance of racist social science during the nineteenth century enabled brutal treatment of Native Americans, Mexicans, and Filipinos, among others. John Dower’s War Without Mercy (1986), a harrowing account of the Pacifi c War, demonstrates that white Americans and Japanese killed and maimed each other remorselessly because of their mutual racism. During the Cold War, US policy toward Africa was guided in part by the assumption that black Africans were unready for, and perhaps incapable of, self-government. In South Africa (Borstelmann 1993), Zimbabwe (Horne 2001), and all across the African continent (Noer 1985), white Americans sheltered too long and lovingly racist white minority governments that frustrated black aspirations to democracy. Domestic race relations also played a role in US foreign policy. The rising civil rights movement after 1945 exposed American racism and embarrassed a succession of presidents trying to win the Cold War with the claim that communists represented tyranny, the Americans and their allies freedom. African Americans often identifi ed with black freedom fi ghters in Africa, and vice versa, as both groups struggled against white power structures that denigrated and oppressed them. African Americans spoke out against racism at home and racist colonialism abroad, prompting State Department offi cial (and later secretary of state) Dean Rusk to admit that race discrimination in the United States was “the biggest single burden that we carry” into the arena of diplomacy. A good deal of scholarly attention has been paid recently to the impact of domestic race relations on US policy making (Horne 1986; Plummer 1996; Von Eschen 1997; Krenn 1999; Dudziak 2000; Gallicchio 2000; Borstelmann 2001; Anderson 2003). Along with race, gender has increasingly become an important analysand for historians of foreign relations. Joan Scott’s infl uential essay “Gender: A Useful Category of Historical Analysis,” fi rst published in 1986, questioned why historians seemed to think that gender was “irrelevant to . . . issues of politics and power”; in her view, “high politics itself is a gendered concept” (Scott 1996: 48). Emily Rosenberg responded to this challenge (1990) and gradually thereafter, foreign relations historians began to apply gender analysis to their studies of diplomacy, imperialism, and war. Some saw gender as a way to consider the role of women in international encounters, as occasional makers of policy (Jeffreys-Jones 1995), as agents of foreign relations through non-governmental organizations (Tyrrell 1991), or as those on the receiving end of imperial power (Enloe 1990; Moon 1997; Findlay 1999; Goedde 2003; Shibusawa 2006). Some studies of gender included consideration of sexuality and/or race. Other scholarship involving gender has concerned the role played by cultural constructions of the masculine and the feminine in shaping images of selves and others in US foreign policy. The United States has typically seen itself as a masculine nation, honor-bound to protect allegedly feminine others, or to discipline those whose fl ighty and effeminate misbehavior threatens international stability. The quest for manliness has been associated with certain American presidents; as Kristin Hoganson has written, “historians have turned Theodore Roosevelt into a virtual poster boy for the utility of gender in foreign relations history” (Hoganson 1998; Bederman 1995; Dalton 2002). Frank Costigliola has discovered signifi cance in the gendered language of Cold Warrior George Kennan, who repeatedly warned against the “penetration” of the “West” by Soviet expansionism (Costigliola 1997). The fear of appearing soft on communism drove John F. Kennedy to insist on masculine toughness in his policy toward the Soviet Union and Vietnam (Dean 2001). Other historians have claimed that the United States is periodically seized by a “crisis of masculinity” that fi nds an outlet in an aggressive foreign policy, regardless of who is president. Rendering international others as feminine has enabled the United States, and other imperial nations, to naturalize or justify interference in others’ affairs. Paternalism guided US policy toward Latin America and the Caribbean; the North Americans sought to control allegedly fl ighty and emotional Haitians, Cubans, and Puerto Ricans (Renda 2001; Perez 1998; Findlay 1999). The annals of US foreign relations are populated by tremulous Chinese, cowering Hindus, tough Muslims and weeping Muslims, manly Israelis, effete Frenchmen, and so forth. The “tough” and “manly” won praise and support from the United States. The “weak” and “soft” required fi rm, masculine guidance. If foreign relations historians have confi rmed that gender is “a useful category of historical analysis” even within realms of power, they have nevertheless found that gender alone, like race alone, has explanatory limits. The challenge for historians, as Hoganson puts it, “is shifting from demonstrating the relevance of gender to situating gender alongside strategic, economic, political, and other factors” (1998: 316). Some historians have opened their cultural analysis to a greater number of variables, by looking carefully at the language of foreign policy makers or those groups that influence them. Language, particularly in its metaphors, can convey a host of meanings infl ected by the culture that produces it. Kennan’s language in his famous “Long Telegram” (1946) was gendered – it feminized the Russian people, for whom Kennan had an almost sexual affection, and cast as rapacious the current Soviet leadership – but it also indulged in references to illness, as in the “Kremlin’s neurotic view of world affairs” and Soviet leaders being “affl icted” with insecurity (Costigliola 1997). Geoffrey Smith has associated gender, pathology, and perceptions of national security in his explanation of the Red (fear of communism) and Lavender (fear of gay people) Scares that swept the United States in the late 1940s and early 1950s (Smith 1992). Homosexuality was purportedly a sexual perversion, a disease, and a risk to national security because gays were readily blackmailed by their communist handlers. Increasingly, historians of foreign relations are trying to do justice to the complexity of culture and the disparate ways it affects perception and decision making. It is never neat work. Who is to say, for example, whether race or religion more insistently conditioned US policy toward Muslim Pakistan and Hindu India during the 1950s? How did interwoven ideas concerning gender, race, and class shape North American initiatives in Puerto Rico or Cuba at the beginning of the twentieth century? A number of scholars have skillfully blended the discrete elements of culture to offer satisfying explanations of American encounters with others (Stephanson 1995; Dower 1999; Bradley 2000; Connelly 2002; Klein 2003). The most direct result of the poststructural challenge to the history of US foreign relations has been the emergence of postcolonial or subaltern studies, a movement closely associated with the late Edward Said, whose Orientalism (1978) was its foundation text. Postcolonial scholars admired Marx and especially the Italian Marxist Antonio Gramsci, but revealed their poststructural affi liations through their interest in literature, subjectivity, prisons, schools, and discourse, and through their footnotes, which cited more Foucault than Marx. The postcolonialists were emphatically interested in empire and power. While they were clear in their condemnation of colonialism, they looked imaginatively at the relationships empire created between the dominant nation, its agents, and colonized “subalterns” (Subaltern Studies, 1988– 2000). Perhaps the most important contribution of the subaltern scholars was their ascription of agency to the weaker parties in the colonial relationship – men and women who, in spite of having limited power, shaped their own identities and forged resistance despite their subordinate status. Gender and often race figured prominently in these works. Said and the Subaltern Studies quickly found their way into the arguments (and the footnotes) of foreign relations culturalists. Essays in Cultures of United States Imperialism (Kaplan & Pease 1993) used poststructural theory to expand the horizons of historians more comfortable sorting through diplomatic correspondence than contemplating the prosthetics of empire, stuffed gorillas at New York’s Museum of Natural History, and Tokyo Disneyland – all subjects of essays in the Kaplan–Pease anthology. As Rosenberg has noted, much of the foreign relations history inspired by poststructuralism has focused on the formal American empire: on the Philippines, and especially on Latin America (Joseph et al. 1998; Rosenberg 1999; Rafael 2000; Renda 2001). Adopting postmodern theory, regarding empire as an engagement of cultures, and exploring mutual images and attitudes as displayed in the media, in fi ction, and in travel literature, these scholars have nevertheless combed the archives in search of affi liations between the offi cial language of diplomacy and the broader discourse of encounter. It would be satisfying to report that culturalism has swept the field, and achieved the stature of realist, revisionist, or even post-revisionist accounts of US foreign relations. There is no question that culturalism has gained a measure of respect, certainly among younger entrants to the fi eld, and with some older scholars as well. Yet resistance remains. Some seems churlish: that cultural infl uence is harder to measure than, say, trade fl ows during the 1930s is self-evident, and hardly disqualifi es culture as a meaningful category of analysis. But there is thoughtful criticism as well. Culture is an elastic concept; if it includes and explains everything, it threatens to explain nothing in particular. Culture, moreover, can occlude the operations of cause and effect. Exploring how selves see themselves and others does not necessarily illuminate *why* selves or others *act* as they do. And cultural perceptions are likely to depend on interests: Americans during the Pacific War hated and dehumanized the Japanese, but cherished the Chinese as honest, virtuous, and quaint. Above all, critics have charged, culture in the end has not much to do with power. Oppression is not, they say, about ridicule, stereotype, or ideas based on gender, race, or religion. Language does not kill people; war is not a discourse. In its affection for Geertzian context, its emphasis on image, culturalism neglects what is most important about US foreign relations.

#### Root cause logic is reductive and false —it subverts change

Morson 7 [Gary, Professor of Slavic Studies, Russian Literature and History at Northwestern, “Anna Karenina In Our Time: Seeing More Wisely,” P. 152-4]

If Levin resembled so may intellectuals in his time and ours, he might seek “root cause” (as we would call it today) of all these failures. Much as the generals an historians satirized in War and Peace mistakenly seek the cause of historical events in a single decision, an much as revolutionaries often reduce the complexities of social ills to a single conspiracy or institution, so **intellectuals** often **view complexity as a delusion to be explained away by a few simple underlying laws. It is just this habit of thought that feeds utopianism, because if the diversity of evil an misery had a single cause, then one could eliminate it by changing only one thing What could be easier? Abolish private property**, alter the way children are educated, pass laws to regulate morals according to a given code, and evil will disappear or, at least, radically diminish. Behold, I make all new things But Levin learns that there is no single cause for what has gone wrong. **Looking back on the twentieth century**, we may wonder whether the root cause of the worst human misery is the belief that there is a root cause of human misery. In fact, many things happen contingently, just “for some reason.”¶ Friction¶ When l.evin attends the elections, he tries to handle some business for his sister, but discovers that somehow it cannot be done. In Dostoevsky, the reason would be "administrative ecstasy," the sheer delight bureaucrats take in making petitioners cringe, plead, or wait. But nothing of the sort happens here, and the problem is not one of intent at all. No one has any interest in thwarting Levin, so he cannot understand what goes wrong.¶ When conspiracy theorists find they cannot accomplish something as easily as expected, they typically ask cut bono? (who benefits?) ro discover the obstacle. Some person or group must have caused the failure. Defeat means sabotage. This way of thinking presumes that behind every action there must be an intent,¶ whether conscious or unconscious. Such a view rules out the possibility that mere contingency or friction accounts for the difficulty.¶ flic military theorist Carl von Clauscwitz deemed friction, in this special metaphorical sense, an essential concept in understanding armies. Without using this word, Tolstoy regarded the same phenomenon as pertaining not just to war but to everything social. "If one has never personally experienced war," Clauscwitz explains,¶ one cannot understand in what difficulties constantly mentioned really consist. . . . Everything looks simple; the knowledge required docs not look remarkable, the strategic options are so obvious that by comparison the simplest problem of higher mathematics has an impressive scientific dignity. Once war has actually been seen the difficulties become clear; but it is extremely difficult to describe the unseen, all-pervading element that brings about this change of perspective. Everything in war is very simple, but the simplest thing is difficult. 'Die difficulties accumulate and end by producing a kind of friction that is inconceivable unless one has experienced war. (Clausewitz, 119)¶ The unseen, all-pervading element: For Tolstoy, similar difficulties arise when dealing with bureaucracy, introducing changes in agriculture, and implementing reforms. A Tolstoyan perspective is easily imagined today. Social problems look so simple: people in underdeveloped countries are poor, so give their governments foreign aid; workers arc unemployed, so hire them to perform needed government services; schools do not educate, so raise teachers' salaries; the state regulatory commission keeps energy prices too high, so partially privatize the system: answers seem so obvious, but in practice reforms rarely have the intended effect. They produce unintended consequences, which themselves have consequences; and, as Isaiah Berlin liked to point our, no one can foresee the consequences of consequences of consequences. Experience may teach one to expect certain kinds of difficulties, but some can never be anticipated, lhcrc is always friction: "Countless minor incidents —the kind you can never really foresee—combine to lower the general level of performance, so that one always falls far short of the intended goal" (Clauscwitz, 119).¶ No one is deliberately impeding Levin's efforts for his sister. By the same token, no one is trying to thwart his agricultural reforms. Sabotage is out of the question. "All this happened not because anyone felt ill will toward Levin or his farm; on the contrary, he knew that they [rhe peasants] liked him [and] thought him a simple gentleman (their highest praise)" (340).¶ Friction defeats the reforms. But where does this friction come from and how might one best deal with it?¶ TTic Elemental Force¶ 'Ihe bailiff and peasants recognize in advance when a plan is bound to fail, and at lasr l.evin, instead of growing angry, pays artention to what they say:¶ The bailiff listened attentively, and obviously made an effort to approve of his employer's projects. But still he had that look Levin knew so well that always irritated him, a look of hopelessness and despondency. That look said: " Ihat's all very well, but as God wills." Nothing mortified Levin so much as that tone. But it was common to all the bailiffs he had ever had. They had all taken up that attitude toward his plans, and so now he was not angered by it but mortified, and felr all the more roused ro struggle against this, as it seemed, elemental force continually ranged against him, for which he could find no other expression than "as God wills." (165)¶ Ihe elementalforce: this concept is central to both Tolstoy's great novels. Tolstoy uses a few similar terms for it. In War and Peace, he refers to an elemental force shaping individual lives (W&P, 648) and to "the elemental life of the swarm" constituting the cumulative effect of countless people's small actions governed by no overarching law. In Anna Karentna, he calls the elemental force a "brutal force" when its outcome is cruel. Ihe rough equivalent of friction for Clause-witz, the elemental force applies more widely.¶ Clauscwitz's explanation stops at friction, but Tolstoy takes the elemental force as a starting point for understanding why some plans arc more likely to fail than others.¶ **In order to grasp** the course of **events more easily**, **we** tend to **reduce** the countless infinitesimal forces making up the elemental force to a single cause. After all, it is impossible to enumerate innumerable actions. And **so** historians and **social scientists** naturally **look for some** super-cause that sums up all those small actions. They may presume laws or postulate narrative neatness. Tolstoy relentlessly exposed the **logical fallacies in** both forms of simplification, which, at some point, either assume what is to be proven or proceed as if it were already proven. ¶ Historians, **social theorists**, and biographers favor generalizations or symmetries permitting a clear analysis or simple story. **They find what they seek**, their success demonstrates not that complexity has been adequately explained but that when a discipline demands a certain sort of explanation it is bound to be “discovered.” **In disciplines pretending to be social sciences**, it is repeatedly discovered that things are not as complex as they appear.

## AT Imperialism Stuff

### AT America Imperialist

#### America is not imperial – calling it such methodologically wrecks our ability to critically understand how American power works

Walzer 18 [Michael, Prof Emeritus at the Institute for Advanced Study in Princeton, Fellow of the American Academy of Arts and Sciences, *A Foreign Policy for the Left*, epub]

“Empire” needs extensive qualification if it is to describe anything like what exists, or what is possible, in the world today. Hence the appeal of terms like Michael Ignatieff’s “empire lite.”3 But perhaps there is a better way of thinking about contemporary global politics, drawing on the related idea of “hegemony.” In common use today, “hegemonic” is simply a less vivid way of saying “imperialist,” but it really points to something different: a looser form of rule, less authoritarian than empire is or was and more dependent on the agreement of others. Consider these words from Antonio Gramsci, the foremost theorist of hegemony—who wrote in the context of domestic political struggles: “The fact of hegemony presupposes that one takes into account the interests and tendencies of the groups over which hegemony will be exercised, and it also presupposes a certain equilibrium, that is to say that the hegemonic groups will make some sacrifices of a corporate nature.”4 Hegemony rests in part on force, but it rests also, even more importantly, on ideas and ideologies. If a ruling class has to rely on force alone, it has reached a crisis in its rule. To avoid that crisis, it has to be prepared for compromise. In an essay on Gramsci, Stuart Hall provides a more extended analysis of the “multi-dimensional” character of hegemony (he is still writing about domestic politics): What “leads” in a period of hegemony is no longer described as a “ruling class” in the traditional language, but a historical bloc . . . The “leading” elements in a historical bloc may be only one fraction of the dominant economic class. . . . [A]ssociated with it, within the “bloc,” will be strata of the subaltern and dominated classes who have been won over by specific concessions and compromises and who form part of the social constellation.5 Michael Bérubé comments usefully on this highly abstract passage: “The import is clear: mastery is not simply imposed or dominative in character; consent is not simply manufactured by a ruling class and its monopoly over the means of mental production.”6 The politics of a ruling class is largely internal, a matter of factions and intrigue; politics in a hegemonic system, by contrast, involves the interaction of independent actors, who must be drawn into a “bloc” through argument and concession. So the theory of hegemony provides a view of our political life that comes close to our everyday perception of its complexity. Exactly how a similar analysis would work in international society isn’t entirely clear, but hegemony would certainly require a more complicated understanding than the theory of imperialism allows. I don’t have a fully developed alternative theory, only the beginning of an argument. Nor do I mean to suggest that America’s recent rulers, who began the Iraq war, actually accepted the need for “sacrifices of a corporate nature” or for “concessions and compromises,” even when they made them—as they did with the Turks in 2003 and as the Obama administration, more self-consciously, has done again with the Turks, and also with the Saudis, in the ongoing war against ISIS. President George W. Bush’s unilateralism was a bid for dominance without compromise, which turns out to be impossible. But unilateralism hasn’t been the natural mode of American power. Since World War II we (Americans) have played a major role in shaping international organizations; we have negotiated alliances, and we have generally been willing to consult with our allies in responding to critical events like the Iraqi invasion of Kuwait and in dealing (often reluctantly) with dangerous political or environmental tendencies like nuclear proliferation and global warming. The wish to act alone was an innovation of the second Bush administration—and was short-lived, or so it seemed, until the election of 2016. It was less the product of fear than of arrogance and ideological zeal, and it reflected a view of American power as inaccurate as that held by many of President Bush’s critics. In the contemporary world, imperial rule is an exercise in futility—but a dangerous exercise nonetheless. It is futile in the American case for three reasons. First, Americans don’t have the stomach for old-fashioned imperialism. We are radically unready to pay the economic costs of empire—and empire, when it involves the “microadministrative management of populations,” is expensive: there are profits for corporations like Bechtel and Halliburton, but only burdens for American taxpayers, who won’t be willing to bear them for long. Nor will American mothers and fathers be willing to bear the costs in blood. We don’t have an imperial army made up of “natives” and mercenaries. We have never created an imperial civil service; we don’t even learn the languages or customs of the countries we mean to rule. The American failure to impose law and order across Afghanistan, the deals the Pentagon made with local warlords (and then didn’t enforce), our government’s refusal to invest seriously in state-building outside Kabul: all this points not toward the skill and determination of imperial rule but toward the compromised character of hegemony—and also toward the amateurism of the American effort. Nor did our effort produce a particularly honorable version of hegemonic rule: it was hegemony without responsibility, which quickly came to mean no hegemony at all. Anyone who thought of the American engagement in Afghanistan as an imperialist war must have been surprised at its outcome. The United States lost men and material and gained none of the usual prizes of imperial rule. Nor is it clear that there was ever much to gain once the Cold War engagement with the Soviet Union was over. After 9/11, there were defensive reasons for the war, but imperialist reasons are very hard to find. Ellen Willis argues strongly that the United States could have done good things in Afghanistan after the invasion—and I would add that there was also a debt to pay to the Afghans, given our role in bringing the Taliban to power. Here is Willis’s argument: My frustration . . . is not that we took action in Afghanistan but that we have not done enough. We should have fought the ground war and occupied Kabul; organized an international force to disarm the warlords, protect ordinary citizens, and oversee the distribution of aid; demanded that secularists be included in the negotiations for a new government and that basic women’s rights be built into a new structure of law. If this is “imperialism”—in the promiscuous contemporary usage of that term—I am for it. I believe it is the prerequisite of a stable peace.7 I don’t think Willis is actually advocating an imperialist program here; organizing her international force would have required a diplomacy of concession and compromise, and the gains she was looking for were definitely not material. This is a version of hegemony that the American left could support and should have supported. The actual conduct of the war and the under-resourced state-building that accompanied it required leftist criticism, but calling either of these imperialist didn’t help anyone understand what was wrong with what we were doing. The second reason for the likely futility of an American imperialism is that our public commitment to democracy makes imperial rule very hard to justify or manage. Even when that commitment is obviously hypocritical (for many years we supported non-democratic governments in countries like South Korea and Turkey), we do tend over time to encourage or enable or at least bear with democratic transformations. At the height of the Cold War, indeed, we refused to bear with democratically elected governments in Iran, Guatemala, and Chile. And possibly we will refuse in the future, in countries like Egypt, say, where radical Islamists rather than communists threaten to win elections. But it isn’t easy for us to support dictators, even if they are “our” dictators; it produces a kind of legitimacy crisis for American power—another feature of hegemonic but not imperial rule. The third reason for imperial futility is that under contemporary conditions, governments arise that are capable of opposing the imperialist policies of any aspiring great power. And then the aspiring power will, if it is wise, negotiate and compromise. In the world today, any refusal to do that, any full-scale imperialist project, would encounter such strong opposition from both large and small states, and so strong a sense among people everywhere that opposition was legitimate, that the project would be certain to fail. When Rudyard Kipling called empire the “White Man’s burden,” he was stating, in the ideological idiom of his time, a simple fact: power brings responsibility. But the burdens of hegemony can’t be borne alone; they have to be shared. A rationally governed hegemonic power doesn’t act unilaterally to regulate trade, deal with rogue (or unfriendly) states, repel aggression, stop massacres, or take on the very difficult work of state-building; it seeks allies, it marshals coalitions. These will be coalitions of the willing, obviously, but the willingness has to be won by consultation, persuasion, and compromise. In the early 2000s, the US government sought to avoid any serious version of these necessary processes, as if its leaders wanted to manage the world all by themselves. That ambition is probably a better explanation of the Iraq war than any provided by the theory of imperialism. But America’s leaders can’t manage the world even when they are ready for consultation, persuasion, and compromise—as President Obama discovered. At the end of the Obama years, many of his critics asserted that the United States was no longer hegemonic. We had walked away from our responsibilities in, for example, the Middle East. That was a right-wing critique, but the thought that it might be true should have delighted many leftists. In fact, hegemony is still a useful description of America’s place in the world.

### AT NATO Bad

#### Blanket critique of NATO erases the perspectives of East European left activists – questions about our alliance commitments have to be decided on a case-by-case basis

Walzer 18 [Michael, Prof Emeritus at the Institute for Advanced Study in Princeton, Fellow of the American Academy of Arts and Sciences, *A Foreign Policy for the Left*, epub]

Consider the key question about the international political and military alliances of our country: Which odd bedfellows are too odd or too awful to take to bed? There is no general answer; we have to look at each case, always asking which alliances provide the greatest benefits to the people in greatest need. In answering that question, we see American bedfellows that definitely don’t meet the necessary standard (and some, given the alternatives, that do). The NATO alliance is worth thinking about in this regard. Originally organized to oppose Soviet communism, it was condemned by leftists still struggling, against all the evidence, to defend that murderous regime. After the fall of communism, the NATO powers began a serious debate about extending the alliance into eastern Europe. Many leftists, along with right-wing “realists,” opposed the extension; some of them, like Jeremy Corbyn, a future leader of the British Labour Party, called for their countries’ withdrawal from NATO. It may have been right to oppose the extension or at least set limits to it; it was certainly right to oppose withdrawal. But what was entirely missing from the left side of the debate, most clearly in the politics of people like Corbyn, was any commitment to talk to east European leftists— Poles and Ukrainians, for example—and to consider the views or even the safety and welfare of the people with the most at stake. Surely left internationalists have to engage with our allies abroad before deciding whether to support or oppose our country’s alliances.

### Antimilitarism Bad

#### Leftist foreign policy requires planning for when and how the state can act to promote progressive values – blanket anti-interventionism is indistinguishable from right-wing isolationism

Walzer 18 [Michael, Prof Emeritus at the Institute for Advanced Study in Princeton, Fellow of the American Academy of Arts and Sciences, *A Foreign Policy for the Left*, epub]

The men and women of the left—socialists, social-democrats, and left-leaning liberals, all of us—are most at home in the homeland; our politics is focused on the character of domestic society. Though we claim to be internationalists—and we are, some of the time—we have never gotten a good grip on foreign policy or on security policy. This is, I want to argue, a highly principled failure. We do best with global issues when they are most like domestic issues, as when we oppose inequality, sweated labor, and anti-union practices abroad or work across borders against environmental degradation. Our record is not so good when the issue is the possible use of force. That is something most of us don’t want to think about—or we just want to say no. Bernie Sanders’s Democratic primary campaign of 2016 provides a near-perfect illustration of this position, though not the only one. Like it or not, however, we live together with our fellow citizens in an anarchic society of states where the ability to make wise decisions about the use of force is essential to the safety of our own state, of states with which we have close relations, and sometimes of people far away who are in desperate trouble and need our help. Wise decision-makers opt for peace whenever they can, but sometimes for a cold war, sometimes for the use of force short of war, sometimes for the threat of war, and sometimes for the agony of war itself. Political wisdom isn’t essentially militarist or pacifist (or anything in between). It requires a steady commitment to conciliation and compromise so long as these are possible, and a readiness to fight when fighting is necessary. The two are equally required. That combination has always been a problem for the left. There are leftists, to be sure, who are eager to support revolutionary wars, usually in distant places, and to endorse the violent acts, sometimes even the terrorism, of liberation movements. We are more hesitant when it comes to our own countries’ wars, especially if we live in a great power like the United States. Then our standard argument is critical: anti-imperialist and anti-militarist. Over many years and many occasions, this negative argument is certain to be right some of the time. But when reiterated pretty much all the time, it amounts to a questionable demand for inwardness. Arguing against this imperial aggression or that military adventure, we regularly insist that our country should avoid all engagements abroad and devote its energy and resources to creating a more just society here at home. Leftist conceptions of foreign policy, insofar as we think about foreign policy, lean toward the avoidance of forceful action. A commitment to neutrality in all international conflicts and civil wars is one example of this (think of social-democratic Sweden). Neutrality is a nice way of having and not having a foreign policy at the same time. But there are moments when it represents a critical and positive decision—as in 1917, when American socialists argued against joining the European war. The common man, John Reed claimed at the time, probably wrongly, “has a natural inclination to neutrality.”1 Strong support for the United Nations and the International Criminal Court (ICC) is another example of leftist foreign policy. I remember how, after the 9/11 attacks, many American leftists wanted to turn to these institutions rather than act unilaterally or with close allies against Al Qaeda, even though we knew the United Nations and the ICC would not act at all. Perhaps that was the point. A third, more curious but no less common example of leftism abroad is the claim that everything that goes wrong in the world is America’s fault—and so we (Americans) should refrain from doing anything at all. The denial of agency to other countries suggests a fairly radical version of leftist inwardness; the lack of interest in what would happen if the United States actually disengaged suggests an even more radical version. I will take up leftist arguments about revolutionary wars and liberationist violence, about the possibilities of global government, and about domestic (and foreign) anti-Americanism in the chapters that follow. Here I want to insist that the default position of the left, the position we keep coming back to, is an almost exclusive focus on how we and our fellow citizens live when we are among ourselves. For many of us, the only good foreign policy is a good domestic policy. Americans will be more safe in the world and the world will be better off, leftists have repeatedly argued, if we concentrate on creating a just society at home. This is a very old position. It was first voiced by the Hebrew prophets who claimed that if the ancient Israelites honored the one true God by acting justly toward the men and women created in his image, if they stopped grinding the faces of the poor, he would protect them against Assyrian and Babylonian conquerors. They would live at peace in their land forever, and be a “light unto the nations” (Isaiah 42). All they had to do was sit still and shine. Thus saith the Lord of hosts, the God of Israel. . . . If ye thoroughly amend your ways and your doings; if ye thoroughly execute judgment between a man and his neighbors; if ye oppress not the stranger, the fatherless, and the widow, and shed not innocent blood . . . then will I cause you to dwell in this place . . . for ever and ever. (Jeremiah 7:3–7) Act justly at home and your home will be secure—so says Jeremiah, and Isaiah says that people around the world will admire your light and imitate your justice. In the history of the modern left, it is easy to find activists and militants playing variations on these themes. I will offer just a few examples here; more will come in later chapters. Consider Randolph Bourne’s fierce critique of pro-war intellectuals in 1917. Bourne was “one of the strong and triumphant personalities” of Greenwich Village’s “lyrical left” and also the most brilliant opponent of American engagement in the European war.2 This is what he said about John Dewey, Walter Lippman, and other New Republic writers who supported the war: “Never having felt responsibility for labor wars and oppressed masses and excluded races at home, they had a large fund of idle emotional capital to invest in the oppressed nationalities and ravaged villages of Europe.” This investment, Bourne insisted, was a mistake. So long as “the promise of American life is not yet achieved . . . there is nothing for us but stern and intensive cultivation of our garden.”3 He was probably right in his opposition to American engagement in the European war—though his reasons, I think, were not right. It is an odd leftist position that makes responsibility at home exclude responsibility abroad. This argument has echoed over the years. Writing in the aftermath of the 2003 Iraq invasion, Andrew Bacevich, one of its leading opponents, quoted Bourne’s line about “our garden” and argued that “if we live up to our professed ideals . . . we may yet become, in some small way, a model worthy of emulation”—which is to say, a light unto the nations.4 I believe Bacevich was right about Iraq, but is a bad war sufficient reason for Americans to cultivate their garden—and do nothing more? In addition to Bourne, Bacevich also remembered and celebrated Charles Beard, the radical historian who was, in the lead-up to World War II, one of this country’s most prominent isolationists. Writing in 1940, Beard defended “continental Americanism” and argued that America must concentrate its energy and intelligence on “overcoming the grave economic and social crisis at home.”5 The default position of the left overlaps sometimes, as it did in 1940, with right-wing isolationism, but it is usually very different. Leftists, most of us, are internationalists in spirit even when we fail to be internationalist in policy. We know that we have comrades in foreign countries with whom we should stand in solidarity. Too often, however, we simply stand still; it is hard to figure out, or we don’t try to figure out, what to do to help our comrades. But sometimes the spirit moves us in stronger ways—as when leftists from around the world rushed off to Spain to join the struggle against Franco and the fascists. That was a moment when the left actually had a foreign policy of its own—fight the fascists! The fight was organized and then betrayed by the Comintern, whose leaders were more eager to attack anarchists and Trotskyists than fascist soldiers. Still, this was a brief internationalist moment, when idealistic young leftists fought militarily in Spain while their friends fought politically in Britain, France, and the United States to end the embargo on arms for the Spanish Republic. How could democratic states be neutral, they asked, in a civil war between republicans and fascists? But only a few years later, after the Hitler-Stalin Pact, many leftists here at home were urging American neutrality in the war between Nazi Germany and democratic Britain. In an editorial published in April 1940, the now anti-war New Republic provided a perfect example of the default position: “It is not a mark of barren isolationism to believe with all one’s heart that the best contribution Americans can make to the future of humanity is to fulfill democracy in the United States.”6 At that moment, the New Republic stood shoulder to shoulder with isolationist Charles Lindbergh and the America First movement. The default position is sometimes said to follow from the uncertainties and ambiguities of international politics. Thus Jeff Faux in a debate (with me) about foreign policy: “Because the world is so complicated, the imperial reach so wide, and our access to information and our ability to process it so limited, the minimalist default position still makes the most moral and political sense.”7 Well, yes, it probably is a good idea, when you don’t know what to do, not to do anything. In the years after 2011, President Obama was accused by neo-conservative interventionists of dithering over what to do in Syria. Given the complexities of the Syrian civil wars, dithering probably made sense. But a large portion of the American left wasn’t dithering at all; it simply opposed any American action abroad, any exercise of American power. Leftists produced a long list of the disasters likely to follow from a large-scale US intervention—and then were hardly interested in the disasters that did follow when a very limited (and ineffective) American intervention was overwhelmed by the massive interventions of other states. Complexity wasn’t the issue here, but rather a principled refusal to support an activist American policy in the Middle East, or anywhere else. Surprisingly, perhaps, most US leftists felt little need to stand in solidarity with the Syrian rebels, even those who called themselves secular democrats. Judging by our behavior, we were also only weakly committed to relief for the victims of the war—and not committed at all if relief required the use of force (as the establishment of a safe zone in northern Syria would have done). But later on, all of us supported the reception of Syrian refugees in the United States, and we were ready to take in far more than our government proposed. We argued forcefully against right-wing xenophobia. Once the refugees were here or on their way, solidarity was easier, for the issue now was the character of our own society. As leftists, we were proud to defend ethnic and religious diversity and to reject any curtailment of the rights of new Americans. And we were eager to argue that America, as an immigrant society, could be a light to other nations that had no history of immigration. We fell naturally into the default position. No doubt, this narrow domestic focus makes a lot of sense. Randolph Bourne was right to say that oppressed workers and excluded races in the United States are our first responsibility. And we have a long way to go in the project that Richard Rorty called “achieving our country”—creating a fully inclusive and just society.8 Though we haven’t had many successes in recent years, this is where our voices are strongest and clearest. We stand in opposition to union-busting, racism, misogyny, xenophobia, growing income inequality, the role of money in elections and the advance of plutocracy, the pollution of the environment, homophobia, the attack on the welfare state, and all attempts to undermine the right to vote—I’ve put the list in random order because every group of leftists has its own priorities. But we all know the reach of leftist commitment, and we (mostly) support each other . . . when we are at home. But that can’t be the whole story of the left. So long as we are internationalists in spirit, we can’t escape what Václav Havel, speaking to the Czech parliament in 1993, called “our co-responsibility for the cause of freedom and democracy.”9 In a world beset by wars and civil wars, religious zealotry, terrorist attacks, far right nationalism, tyrannical governments, gross inequalities, and widespread poverty and hunger, that cause requires intelligent leftist attention. Our deepest commitment is solidarity with people in trouble, and some of the worst troubles are being experienced, right now, in the world abroad. So we are going to be engaged again and again in arguments about how we can help people in faraway countries escape poverty and terror and how we can support those among them who are working for freedom and democracy. We will also have to argue about who, exactly, should provide that support, and when. This is a book about those arguments. It is an effort to answer the question What should the left’s foreign policy look like? In the chapters that follow I have tried to join all the recent arguments about leftist engagements abroad. I want to address not only the state policies we should support or oppose but also the policies we should adopt, the actions we should pursue, on our own. We almost always think of foreign policy as state policy, and we certainly ought to take an interest in what our own state is doing in other people’s countries (even if we think it shouldn’t be doing anything). But the left needs its own foreign policy; we need to think about how our parties, unions, and nongovernmental organizations (NGOs) should act in the world. And since speech is action and words are weapons, we also need to think about what we ourselves say about international politics. We should write and argue in support of our friends and comrades in other countries and in opposition to the enemies of democracy and equality, wherever they are.

#### Anti-militarism ignores the necessity of state violence for leftist politics. There are no ideological shortcuts. What should be done has to be decided based on the specific and empirical situation.

Walzer 18 [Michael, Prof Emeritus at the Institute for Advanced Study in Princeton, Fellow of the American Academy of Arts and Sciences, *A Foreign Policy for the Left*, epub]

The defense of the use of force by revolutionaries abroad goes along with opposition to the use of force by one’s own country. A wholesale rejection of militarism (and a reflexive refusal to vote for the military budget) is the most common left position. The pacifist left harbors a deep suspicion of every form of state violence, and almost all leftists are eager to support the peacemakers whenever peace is a real possibility (and sometimes when it isn’t). Hence one standard argument, which is another version of the default position: only militarists and imperialists go to war in other people’s countries. Leftist men and women understand that it is better to keep the “boys” (as all soldiers once were) at home. And if you can’t keep them at home, then, as the Vietnam-era song has it: “Bring ’em back alive.”16 William Appleman Williams, the Wisconsin historian who greatly influenced New Left attitudes toward foreign policy, argued that “the truly essential need is to re-examine our conception of saving other people and societies.” The New Left, he wrote, should pursue a vision “based on self-containment and community.”17 Saving other people too often requires sending the boys abroad or, in more contemporary terms, putting boots on the ground. In a great power like Great Britain in the late nineteenth and early twentieth centuries or the United States from the time of the war with Spain, anti-militarist politics is also anti-imperialist politics. The two go together since empires cannot be sustained without armies. This leftist blend of oppositions has produced some fine moments. One of my favorites is the appearance in 1898 of the Anti-Imperialist League, which campaigned against the American war in the Philippines (and also opposed US policies in Cuba and Puerto Rico). The league’s members included Jane Addams, Ambrose Bierce, John Dewey, Samuel Gompers, Henry and William James, Carl Schurz, and Mark Twain, all of them arguing that democracy at home could not endure alongside empire abroad.18 This might be another example of the default position, except that the American anti-imperialists were not interested only in democracy at home; many were also strong supporters of the Philippine insurgents. Twain and a number of others had initially supported the war against Spain—not an anti-militarist position—thinking it was a war of liberation, a revolutionary war. They turned against it only when they recognized the imperialist program of the American government. Now it was the Philippine insurgents who were fighting a war of liberation. Mark Twain’s pamphlet To the Person Sitting in Darkness, published in 1901 by the Anti-Imperialist League of New York, is a classic left text that ought to be reprinted every time anyone in the United States, or anywhere else, tries by force to bring the light of civilization, or democracy, or socialism to those who sit in darkness. Twain was more than willing to bring, not light, but liberty. The Philippine temptation was too strong, he wrote, and President McKinley had made a bad mistake: he played “the European game.” [But] this was the very time and place to play the American game. . . . Rich winnings were to be gathered in, too, rich and permanent, indestructible; a fortune transmissible forever to the children of the flag. Not land, not money, not dominion—no, something worth many times more than that dross . . . the spectacle of a nation of long harassed and persecuted slaves set free through our influence. Let the Philippine people deal with their domestic questions in their own way, Twain wrote. “I am opposed to having the eagle put its talons on any other land.” As the war dragged on and its cruelties multiplied, he wrote even more strongly. Here he is in 1906, after the Moro massacre: General Wood was present and looking on. His order had been, “Kill or capture those savages.” Apparently our little army considered that the “or” left them authorized to kill or capture according to taste, and that their taste had remained what it had been for eight years in our army out there—the taste of Christian butchers.19 Anti-imperialism also produced the campaign of British radicals against the Boer War, which approximately coincided with the American war in the Philippines. Mark Twain thought these wars were similar and required similar opposition. Indeed, we can find many parallel arguments by British and American anti-imperialists, but there was one significant difference. The British left in 1899 was viciously anti-Semitic, in the style that the German socialist August Bebel called “the socialism of fools.” Leftists from the Social-Democratic Federation and the Independent Labour Party claimed that the war was the work of Jewish capitalists. “The Stock Exchange pulls the string and the British government dances,” wrote the editor of a left newspaper. “But behind the Stock Exchange is the sinister figure of the financial Jew who is gradually enmeshing the world in the toils of the money-web which . . . the great racial free-masonry is spinning in every corner of the globe.”20 There were Jewish capitalists in America by the turn of the twentieth century, but they do not seem to have been blamed for America’s imperial war. The Anti-Imperialist League is an example of principled leftist engagement with the outside world. The same can be said for much of the left’s opposition to US imperialism in Central and South America in the years since the Spanish-American War. US governments have strengthened the hands of local dictators who make deals with American businesses, and they have intervened, in both clandestine and overt ways, in countries where leftists have won elections or seemed about to win them. American support for the Pinochet putsch in Chile is the classic example, but far from the only one. The praiseworthy record of left opposition to all this makes it especially strange that many leftists, after arguing against every US claim to a sphere of influence in the Americas, hurried to defend Russian President Putin’s claim to a similar sphere in eastern Europe. Surely left internationalists who favor self-determination for the people of Chile, Guatemala, and El Salvador should extend the favor to the people of Poland, Lithuania, and Ukraine. I will come back to this issue in chapter 4. The American left’s opposition to our entry into World War I is another exemplary moment, though in this case the left’s weakness may have been the major reason for its excellence. While the large socialist and social-democratic parties in Europe, driven by the patriotism of their base, supported the war, the American party, with a much smaller (and partly new-immigrant) base, held firm to its anti-war position. What was going on in Europe, it maintained, was a struggle between imperial powers, unjust on both sides; the United States should stay out.21 Bourne’s “cultivate our garden” was the line also of many socialists. In a 1916 debate on the question “Must we arm?,” Morris Hillquit concluded for the negative: “Let us center our ambition, our hope and aspiration on making our country the first great peace power in the world.”22 But American socialists were also internationalists who believed in promoting class solidarity across borders and hoped for revolutions abroad. I don’t think they would have favored forceful assistance to those revolutions; they were all anti-militarists, opposed, like Hillquit, to preparing for war as well as to fighting it, but they would have favored political, diplomatic, and (if it were called for) economic support. So they supported the Russian revolution in 1917, but when the Bolsheviks established their dictatorship, many (not all) American socialists decided that internationalismn required political critique. The early New Left opposition to the Vietnam War resembles the old left’s opposition in 1917, but what followed all too quickly—enthusiastic endorsement of Vietcong politics—was neither principled nor useful. It is worth remembering that Students for a Democratic Society, which in 1965 organized the first major anti-war demonstration in Washington, DC, “insisted that there be no expressions of sympathy for the Viet Cong.”23 That was the right position, though it wasn’t held for long. The revolutionary war was destined to end in dictatorship, the murder of thousands, the flight of the “boat people,” and large-scale “re-education.” By the 1960s and ’70s, none of this could possibly have come as a surprise. What those years required was a hard, even paradoxical politics: opposing the American war and also its likely Vietnamese winner. Most leftists didn’t like the paradox. There were good reasons simply to oppose the war—much like the reasons for opposition in the Philippines and World War I. All of these wars, government officials told the world, were waged to save other people or bring them democracy (at great cost to their countries), and in every case the wars’ opponents were right to refuse the mission. But anti-militarism also produced one of the worst moments in left history—the opposition of many, though not all, British, French, and American leftists to rearmament against Nazi Germany in the 1930s. The argument for appeasement was mostly a right-wing argument, but many people on the left supported it because they were (or thought they were) anti-every-war. Clement Atlee, the leader of Britain’s Labour Party, criticized the Munich Agreement in parliamentary debates; allowing Germany to annex parts of Czechoslovakia was, he rightly said, the betrayal of “a gallant, civilised, and democratic people.” But since Atlee’s party had opposed rearmament throughout the 1930s, he could not argue in 1938 for a war on behalf of the Czechs: Britain was grossly unprepared. On the Labour Party left, Sir Stafford Cripps opted for the pure default position, preferring a war against the British ruling class to a war against Nazi Germany. He thought the best defense against the Nazis was a socialist revolution at home. A minority of Labourites were committed pacifists, but most would have supported a war of national defense, as they later did. But they refused on principle to anticipate such a war or to prepare for it.24 Harold Laski, the Labour Party’s leading intellectual, is an interesting exception. He was praised by the American leftist Max Lerner in 1940 as someone who “has had to do his thinking, as also his fighting, on two fronts—facing the enemy of fascism abroad and the enemy of capitalist privilege at home. It is a measure of his humanity that he knows which is the greater enemy.”25 Unfortunately, neither Laski nor Lerner fully grasped the need for another two-front war—against both capitalist privilege and Stalinism. Left internationalists frequently have to fight on two fronts—and sometimes a couple more (see chapter 8). Norman Thomas and Bertram Wolfe’s 1939 book, Keep America Out of War, which called for a “reduction of the size of the military-naval budget,” is a good example of the American left’s position in the lead-up to World War II.26 Of course, the American Communist Party favored whatever policy Stalin thought necessary to Soviet security. American communists were anti-fascist and in favor of rearmament in the 1930s until the Hitler-Stalin Pact brought a quick turn toward neutrality, America First, and the default position, which was followed immediately after the invasion of the Soviet Union in July 1941 by a fierce commitment to a war against Germany. Socialists like Thomas, however, were self-directed, and they chose pretty consistently to fight against the last war. “We were,” Irving Howe wrote years later, “a war behind in our thinking.”27 Thomas repeated the arguments of Eugene Debs without noticing that Hitler’s Germany was nothing like the kaiser’s. How could anyone fail to notice? The oppositional politics that leftists were most accustomed to, aimed always at American militarism (the country was in fact drastically disarmed in the 1930s), blinded many of them to the reality of Nazi militarism. Nor were they ready to acknowledge that fighting against militarism requires a military to do the fighting. Perhaps this is another example of the default position: only an America without an army could be a light unto the nations. Leftist readiness to support disarmament and appeasement has another explanation: what I call the “politics of pretending”—which in 1938 and ’39 took the form of insisting on the reasonableness of people who gave no sign of being reasonable. Paul Berman nicely describes the large numbers of French socialists who supported the Munich Agreement: “They gazed across the Rhine and simply refused to believe that millions of upstanding Germans had enlisted in a political movement whose animating principles were paranoid conspiracy theories [and] blood-curdling hatreds.”28 In the same spirit, later on, many leftists were eager to describe the Chinese communists as “agrarian reformers.” More recently, many were quick to imagine Islamist zealotry as a (strange) form of resistance to Western imperialism. I am fairly sure that in each case, most of the people making these arguments knew, deep down, that they were pretending. Opposition to the use of force is only a common left position, not a consistent one. Think of the International Brigades in the Spanish Civil War. Many leftists were ready to fight against fascism until the Hitler-Stalin Pact forced a large number of them into militant unreadiness. Soon enough, however, leftists recognized a more urgent and forceful militancy. World War II in western Europe was, in its leadership, a right-wing war, run by nationalists (and imperialists) like Winston Churchill and Charles de Gaulle, who had steadily opposed appeasement. Communists and popular front leftists were a major force in underground opposition to the Nazis, though (with a few exceptions) only after Germany invaded Russia. The default position had temporarily lost its appeal. World War II brought one critical issue to the fore: many leftists, especially those influenced by Marxist doctrine, thought that once military force was justified, there were no moral (“bourgeois liberal”) constraints on its use. But anarchists and pacifists, like Dwight Macdonald in his marvelous magazine, Politics, sharply criticized the bombing of German cities and the use of the atomic bomb against Japan.29 Macdonald and his friends had opposed American participation in the war from the beginning, and they maintained their opposition even after they recognized that Nazism was not just one more imperialism. They got the war wrong, but they were right to condemn many incidents in the war’s conduct. On the other hand, those of us leftists who got the war right had little to say about attacks on enemy nations’ civilian populations. Moral arguments would figure in an important way in leftist opposition to the Vietnam War, but they were rarely heard during the “good” war against Nazism and Japanese militarism—which invites a question: Are these arguments relevant to warfare generally, or are they merely useful in our anti-war campaigns? Macdonald applied morality consistently in World War II and afterward, but many leftists did not. Leftists have supported the use of force—even by capitalist countries like the United States—in other instances. Some Marxist militants argue that any war fought by a capitalist country is, by definition, an imperialist war. But the war in Korea, which was fought by an alliance of capitalist countries, was supported by most people on the American and European near-left. A war against aggression, approved by the United Nations, could plausibly be called a just war. Nonetheless, there was left opposition: Michael Harrington, the future leader of Democratic Socialists of America, acting then as a member of the Catholic Worker movement, and David Dellinger, with the War Resisters League, marched against the war; I. F. Stone, bravely and (I think) wrongly, called it unjust.30 The future editors of Dissent magazine, breaking with many of their fellow Trotskyists, supported the war, but critically, which was the right way to do it. The US attack on Afghanistan in 2001 was another just war that nonetheless required sharp criticism. It was necessary then and in the years that followed to distinguish between the decision to fight and the conduct of the fighting. Ellen Willis did exactly that when she wrote in April 2002 that her objections were “from the beginning . . . not to the fact of our war in Afghanistan but to the way we’ve conducted it.”31 Since the Afghan war is commonly cited in leftist argument as a key instance of imperial aggression, I will take it up, and come back to Willis’s commendable critique, in chapter 4. In a history of the American left, Michael Kazin writes that ever since Woodrow Wilson’s administration, “liberals had ardently promoted wars to preserve and advance democracy. The conflict over Vietnam put an end to that tradition for decades to come.”32 But by the 1990s, a more minimalist liberal and left defense of war had emerged—heralded by The Black Book on Bosnia, produced by the editors of the New Republic in 1996 and given full intellectual legitimacy by Samantha Power’s A Problem from Hell in 2002.33 The aim of humanitarian intervention was not to promote democracy but to stop mass murder, rape, and ethnic cleansing. NATO’s Kosovo war of 1999—driven in part by the Srebenica massacre of Bosnian Muslims by Bosnian Serbs—was a just war and also a near-left war: the Labour Party was in power in Britain, the Socialists in France, a coalition of Social Democrats and Greens in Germany, and the Democratic Left in Italy. The Clinton administration represented a weak version of this left politics, but it provided the leadership essential to the war effort. Military intervention in Kosovo was opposed by people on the farther left, who could not credit its humanitarian motive. I remember being told by a “refoundation” communist at the Gramsci Institute in Turin, Italy, in March 1999 that NATO “must be” aiming to seize control of the Black Sea from the Russians. There was no other explanation for the “imperialist” war. Actually, there were other explanations: some leftists thought the war was directed against Slobodan Milošević as the last standing Socialist, in an effort to complete the destruction of “Actually Existing Socialism” in the former Soviet bloc. Amazingly (since Serbia’s “socialism” had little to do with socialism), a group of leftists formed the International Committee to Defend Slobodan Milosevic. Chaired by Michael Parenti, the author of To Kill a Nation: The Attack on Yugoslavia (2000), it included Harold Pinter and former US attorney general Ramsey Clark. The more persuasive far-left critique came later: that left interventionism in Kosovo made the war in Iraq easier to plan and defend. But that can’t be an argument against the use of force for urgent humanitarian reasons. It is instead (and again) an argument for making distinctions. The Iraq war was not a humanitarian intervention; indeed, it left the defense of humanitarianism in “tatters,” as Michael Bérubé writes.34 According to one of its justifications, the aim of the Iraq war was to overthrow a brutal dictator and promote democracy. There were left arguments and precedents for a war of that sort, but there was also a very strong left argument against it—an argument made, perhaps for the first time, by the US Socialist Party in 1917: “Democracy can never be imposed upon any country by a foreign power by force of arms.”35 The Labour Party’s David Miliband was right when he said in 2008 that during the previous decades “the neo-conservative movement seemed more certain about spreading democracy around the world” than the left did. The left, he argued, was “conflicted between the desirability of the goal and its qualms about the use of military means.”36 The qualms are reasonable when it comes to democracy promotion, but not when it comes to stopping a massacre. The campaign for intervention in Darfur, not the invasion of Iraq, was the closest continuation of the near-left’s Kosovo war. I will come back to this issue in chapter 3. Arguments about the use of force for humanitarian or liberationist purposes are complicated; they require close attention to local circumstance and particular histories. We have to think hard about the relation of means to ends. Doing it right will produce judgments that seem radically inconsistent, though they are not: supporting Algerian independence but rejecting FLN terrorism, for instance, or urging American aid to revolutionary Cuba while condemning the growing authoritarianism of the Cuban regime, or opposing the Vietnam War while criticizing Vietcong politics. Ideological shortcuts, created to make the judgments easier, are popular among many leftists and require a left critique. I will just list the shortcuts here; much of this book will be devoted to criticizing them and arguing for a more reflective engagement with world politics. The first shortcut is to pretend that oppression turns men and women into angels and to support the oppressed people of the world no matter what they do. But the oppressed are still frail human beings, and one of the reasons we oppose oppression is because of the pathologies it produces in (some of) its victims and the vicious politics that it (sometimes) promotes. The second shortcut, perhaps more popular than the first, is to stand up always against “imperialism”—or, a shortcut inside the shortcut, always to oppose American policies abroad. Anti-Americanism is a common left politics, which, again, sometimes gets things right and sometimes doesn’t. I believe that it got things right in Vietnam in 1967; it mostly got things right from the beginning to the end of the twentieth century in Central and South America; it got Iran right in 1953, when leftists criticized the anti-Mossadegh coup, and it got Iraq right in 2003. But that’s not enough to make the shortcut a reliable one. The defeat of Nazism and Stalinism, the two most brutal political regimes in world history, was in significant ways American work. Many people on the left supported that work, as we should have. In 1967, Dwight Macdonald wrote to Mary McCarthy that the American war in Vietnam proved “that despite all the good things about our internal political-social-cultural life, we have become an imperialist power, and one that, partly because of these domestic virtues, is a most inept one.”37 We are still inept: in December 2005, with 100,000 American soldiers in Iraq, we organized an election there—and our man came in third. This result may be without precedent in imperial history. (It might suggest that we were less interested in imperial control than in promoting democracy, though the Iraqi politician who came in first wasn’t much of a democrat.) Macdonald’s understanding of US imperialism reflects a political intelligence and a moral balance that are mostly missing in contemporary anti-American writing. Another often used shortcut is to oppose everything Israel does and to blame it for much that it hasn’t done, since it is the “lackey” of American imperialism or, alternatively, the dominant force shaping American foreign policy. The policies of recent Israeli governments require strong criticism—the occupation, the settlements, the refusal to suppress Jewish thugs and terrorists on the West Bank. But much of the left attack on Israel has little to do with its policies and more to do with its existence, which is taken to be the root cause of all evils in the Middle East. This view violates all the requirements of realism—by which I mean simply a readiness to see the world as it really is. The last shortcut is to support every government that calls itself leftist or anti-imperialist and sets itself against American interests. This is different from the old Stalinist shortcut: support the Soviet Union, whatever it does, because it is the first proletarian dictatorship and the first workers’ paradise. That kind of politics is, I think, definitively finished, though it had a brief afterlife focused on China and then, with very few believers, on Albania and North Korea. The more recent version celebrates Maximal Leaders like Gamal Nasser, Fidel Castro, or Hugo Chávez; there are also short-lived infatuations, such as Michel Foucault’s affair with the future Ayatollah Khomeini. Leftist enthusiasm for populist dictatorships is one of our sad stories, which ends when resources run out, the failure to build the economy suddenly becomes undeniable, and the military takes over. But often the Maximal Leader is a military man himself, and the repressive role of the army simply becomes more obvious over time. In Latin America today, the better left is represented by socialists and social-democrats in countries like Chile, Brazil, and Costa Rica who reject demagogic populism and struggle to produce economic growth, greater equality, and a stronger welfare state—and who attract less enthusiasm from American leftists than they deserve.38 There is a lot to be said for the default position. We should work in the place we know best to make things better. The improvement of humanity begins at home. This argument has special force for Americans, who live in an increasingly unequal society that is also a near-hegemonic world power. We need to be wary of adventures abroad that make our work at home more difficult. Still, good leftists can’t avoid internationalism. We will be engaged again and again in arguments about what we should do or what we should urge the United States to do to help people in trouble or comrades abroad. Sometimes there is nothing that the United States can do, at least nothing it is likely to do right. But even when we oppose American action in other countries, we can be active ourselves—providing moral, political, and financial support to men and women fighting in self-defense or in defense of others. There is no magic answer to the question, What should we do? But the ideological shortcuts I’ve just described, lazily adopted and rigidly held, have served us badly in the past and are almost certain to serve us badly in the future. Sticking with them means that we will get things right only by accident. Political intelligence and moral sensitivity work much better than ideology, and they are what should guide our choice of comrades and our decisions about when and how to act abroad. Dictators and terrorists are never our comrades. We should embrace only those men and women who really believe in and practice democracy and equality. We should act abroad only with those who share our commitments and then, only in ways consistent with those commitments. This is the politics that I want to call left internationalism.

#### American military force key to prevent genocidal violence – their reactionary “anti-Imperial” ethics sanction authoritarian intervention and condemn millions to death

Hamid ’16 [Shadi, senior fellow at the Project on U.S. Relations with the Islamic World at the Brookings Institution, “Is a Better World Possible Without U.S. Military Force?,” The Atlantic, October 18, 2016, <https://www.theatlantic.com/international/archive/2016/10/american-intervention-syria/504512/>]

The eight years of the Obama presidency have offered us a natural experiment of sorts. Not all U.S. presidents are similar on foreign policy, and not all (or any) U.S. presidents are quite like Barack Obama. After two terms of George W. Bush’s aggressive militarism, we have had the opportunity to watch whether attitudes toward the U.S.—and U.S. military force—would change, if circumstances changed. President Obama shared at least some of the assumptions of both the hard Left and foreign-policy realists, that the use of direct U.S. military force abroad, even with the best of intentions, often does more harm then good. Better, then, to “do no harm.” This has been Barack Obama’s position on the Syrian Civil War, the key foreign-policy debate of our time. The president’s discomfort with military action against the Syrian regime seems deep and instinctual and oblivious to changing facts on the ground. When the debate over intervention began, around 5,000 Syrians had been killed. Now it’s close to 500,000. Yet, Obama’s basic orientation toward the Syrian dictator Bashar al-Assad has remained unchanged. This suggests that Obama, like many others who oppose U.S. intervention against Assad, is doing so on “principled” or, to put it differently, ideological grounds. Despite President Obama’s very conscious desire to limit America’s role in the Middle East and to minimize the extent to which U.S. military assets are deployed in the region, there is little evidence that the views of the hard Left and other critics of American power have changed as a result. (Yes, the U.S. military is arguably involved in more countries now than when the Obama administration took office, but—compared to Iraq and Afghanistan before him—Obama’s footprint has been decidedly limited, with a reliance on drone strikes and special-operations forces.) As for those who actually live in the Middle East, a less militaristic America has done little to temper anti-Americanism. In the three countries—Egypt, Jordan, and Lebanon—for which Pew has survey data for both Bush’s last year and either 2014 or 2015, favorability toward the U.S. is significantly worse under Obama today than it was in 2008. Why exactly is up for debate, but we can at the very least say that a drastic drawdown of U.S. military personnel—precisely the policy pushed for by Democrats in the wake of Iraq’s failure—does not seem to have bought America much goodwill. Despite the fact that Assad and Russia are responsible for indiscriminate attacks on civilians and civilian infrastructure, including hospitals, many leftists have viewed even the mere mention of the U.S. doing anything in response as “warmongering.” We have had the unfortunate situation of someone as (formerly) well-respected as Jeffrey Sachs arguing that the U.S. should provide “air cover and logistical support” to Bashar al-Assad. We have had Wikileaks’ attacks on the White Helmets, who have risked—and, for at least 140, lost—their lives in the worst conditions to save Syrian lives from the rubble of Syrian and Russian bombardment. Of course, it is not an absurd position to be skeptical of any proposed American escalation against Assad, and many reasonable people across the political spectrum have made that case. But it is something else entirely to apply such skepticism selectively to the U.S. and not to others, especially when the others in question deliberately target civilians as a matter of policy. It can be a slippery slope. While no one would accuse Obama of liking Putin, coordinating with and enabling Russia in Syria is effectively U.S. policy. As the New York Times columnist Roger Cohen noted in February, well before the current disaster in Aleppo: “The troubling thing is that the Putin policy on Syria has become hard to distinguish from the Obama policy.” The Left has always had a utopian bent, believing that life, not just for Americans, but for millions abroad, can be made better through human agency (rather than, say, simply hoping that the market will self-correct). The problem, though, is that the better, more just world that so many hope for is simply impossible without the use of American military force. At first blush, such a claim might seem self-evidently absurd. Haven’t we all seen what happened in Iraq? The 2003 Iraq invasion was one of the worst strategic blunders in the history of U.S. foreign policy. Yet, it’s not clear what exactly this has to do with the Syrian conflict, which is almost the inverse of the Iraq war. In Iraq, civil war happened after the U.S. invasion. In Syria, civil war broke out in the absence of U.S. intervention. What all of this suggests is that attitudes toward the U.S. military, and by extension the United States, are often “inelastic,” meaning that what the U.S. actually does or doesn’t do abroad has limited bearing on perceptions of American power. As a general proposition, many leftists, for example, seem to believe that there is something intrinsically wrong with the use of military force by the United States. In other words, when America does it, it is a bad thing, irrespective of the outcomes it produces, and therefore should be opposed outright. There is rarely any real effort to explain why it’s bad—after all, if it were purely a moral stand against the killing of innocents, the use of Russian or Syrian military force would have to be considered much worse. But, for the use of American power abroad to be intrinsically wrong or immoral, all uses of military force would have to be either immoral or ineffective, or both. However, as a factual matter, this is simply not the case. There was no way to stop mass slaughter and genocide in Bosnia or Kosovo without U.S. military force, buttressed, as it should be, by broad regional or international consensus. In those two cases, a U.S.-led coalition acted. In those cases where the international community did not act, genocide did, in fact, occur, as we witnessed in Rwanda. What became clear then—and what has become clear once again in Syria—is that a world where others than the U.S. take the initiative to stop such slaughter does not exist, and is unlikely to exist at any point in the foreseeable future. While they may be less common, there are also cases where dictators will not only kill their own people but try to forcefully invade and conquer their neighbors. As in the first Gulf War, the gobbling up of Kuwait could not have been prevented without a U.S.-led coalition, again with broad international support. The list goes on. From a moral standpoint, no one should have to suffer under the indignities of ISIS rule. From a strategic standpoint, having an extremist state the size of Indiana in the middle of the Middle East, needless to say, does not suggest the coming of a better, more secure world. While Obama was late to act against the organization and while the anti-ISIS campaign has been deeply flawed, the amount of territory that ISIS controls has been reduced significantly, due in large part to U.S. airstrikes, intelligence, and special-operations forces. No one, not Turkey, Saudi Arabia, or anyone else, was going to seriously confront ISIS without U.S. coordination and leadership, and it’s U.S. coordination and leadership that is facilitating the current battle for the Islamic State’s Iraqi stronghold in Mosul. This is the faulty—and ultimately quite dangerous—premise behind one of the founding assumptions of Obama’s foreign policy: that if the U.S. steps back, others will step in. Even when “others” do step in, the results are often destructive, since America’s allies and adversaries alike do not generally share its values, interests, or objectives. Of course, U.S. military force may be necessary, but it can never be sufficient on its own. This is where the judgment, morality, and strategic vision of politicians and policymakers can make the crucial difference. The United States has not been the “force for good” that many Americans would like to think it’s been. There is a tragic history of intervention abroad that more Americans should be aware of, whether it’s overthrowing democratically elected leaders in Latin America or backing brutal dictators in the Middle East. There is no reason to think the U.S. is necessarily doomed to repeat those mistakes indefinitely. But even if it was, there would still be instances where only U.S. military force could be counted on to stop genocide. The alternative to a proactive and internationalist U.S. policy is to “do no harm,” and this might seem a safe fallback position: Foreign countries and cultures are too complicated to understand, so instead of trying to understand them, let’s at least not make the situation worse. The idea that the U.S. can “do no harm,” however, depends on the fiction that the most powerful nation in the world can ever be truly “neutral” in foreign conflicts, not just when it acts, but also when it doesn’t. Neutrality, or silence, is often complicity, something that was once the moral, urgent claim of the Left. The fiction of neutrality is growing more dangerous, as we enter a period of resurgent authoritarianism, anti-refugee incitement, and routine mass killing. This is the built-in contradiction of what might be called the “anti-imperialist Left.” They are against empire, and there is only one country powerful enough to reasonably be considered “imperial.” (Russia, of course, engages in bloody imperial ventures, but it gets a pass since it is acting against the United States.) But to insist that the fundamental problem in today’s world is American imperialism is to have only the most outdated “principles”—principles that, in the case of Syria, Rwanda, Bosnia, Kosovo, and even Libya, have left, or would have left, the most vulnerable and suffering without any recourse to safety and protection. If the United States announced tomorrow morning that it would no longer use its military for anything but to defend the borders of the homeland, many would instinctively cheer, perhaps not quite realizing what this would mean in practice. But that is the conundrum the Left is now facing. A world without mass slaughter, of the sort of we are seeing every day in Syria, cannot ever come to be without American power. But perhaps this will prove one of the positive legacies of the Obama era: showing that the alternative of American disinterest and disengagement is not necessarily better. For those, though, that care about ideology—holding on to the idea that U.S. military force is somehow inherently bad—more than they care about actual human outcomes, the untenability of their position will persist. That, too, will be a tragedy, since at a time when many on the Right are turning jingoistic or isolationist, there is a need for voices that not just believe in U.S. power, but believe that that power—still, for now, preeminent—can be used for better, more moral ends.

### AT Liberal Warfare

#### “Liberal warfare” and imperialism impacts are so abstract they’re useless - doesn’t provide any accurate method to understand war

Chandler 9 [David, Professor of IR at University of Westminster, "Liberal War and Foucaultian Metaphysics", Review of Dillon and Reid’s The Liberal Way of War: Killing to Make Life Live, www.research.kobe-u.ac.jp/gsics-publication/jics/chandler\_18-1.pdf]

This is a book about the ‘liberal way of war’. But the liberal referred to in the title remains under theorized. On several occasions the authors highlight the distinction between the liberal way of war and the general framing of war in the modern liberal era as a geo-strategic contestation, taking the territorial state as its referent object. For Dillon and Reid, ‘liberalism never fitted this model of modern politics and the modern problematization of war very well’（p.83). They therefore seek to define liberalism and the liberal way of war as distinct from war in the liberal era. The liberal way of war refers not to real wars and conflicts but to an abstract model of conflict, defined as a desire to‘remove war from the life of humanity’which‘derives from the way in which liberalism takes the life of the species as its referent object of politics ─ biopolitics’（p.84）. In this framing, the liberal nature of war very much depends on the self-description of the conflict by its proponents: these range from Gladstone’s occupation of Egypt in the cause of‘suffering humanity’, to US liberal ideological constructions of the cause of‘freedom’in the Cold War struggle against the Soviet Union up to Bush and Blair’s war on Iraq in the cause of humanity（p.6）. As the authors state, of course, wars may be fought on other grounds than universal humanity: ‘liberal states may…also act as geopolitical sovereign actors as well…and may also have geopolitical motives for the wars they wage’（p.84）.¶ It is clear from the beginning that the distinctiveness of ‘the liberal way of war’ which they seek to explore cannot be more than a fool’s quest. They assert that they will critically uncover the paradox of liberal war: why it is that Realist or geostrategic war accepts the necessity of war but attempts to limit it, while liberals wish to end war but, to do so, are willing to fight unlimited wars. Yet, they admit that this starting point is already an ideological dead end ─ the wars of the twentieth century give the lie to the idea that there is some distinction between ‘unending crusades’ and ‘limited jousts between rationally calculative political subjects’: war has its own dynamic（p.7). Nevertheless, Dillon and Reid press on and seek to go beyond a Schmittian critique to ground this paradox in the biopolitical‘driver’of the liberal way of rule ─ biopolitics: wars waged under the banner of the human（against humans）are liberal and, allegedly biopolitical, as human life is declared to be the referent in need of being secured. These wars are alleged to be fought differently to geo-political wars for territory, because the ‘drivers’ of war are not territorialized interests but the biopolitical framings of the needs of the human, how human life can and should be lived. Inevitably there are insuperable methodological hurdles to this Sisyphusian task. Already, there occurs the first fundamental aporia: how do we tell the difference between a liberal and non-liberal war? There appears to be no way of preventing the category of liberal war from becoming a lifeless and descriptive one: wars are liberal and fought biopolitically only if we are told that these are the motives by those fighting them.¶ This separation of liberal ways of war from territorialised framings of geostrategic contestation makes little sense as a framework for understanding either liberal rule or liberal ways of war. In fact, in defining liberal war in this way the connection between liberal rule and war is entirely severed. ‘Liberal war may on occasions also be geopolitical; which is to say that war may be simultaneously geopolitical as well as biopolitically driven since the imperatives behind war are never uniform or simple; but what distinguishes the liberal way of war as liberal are the biopolitical imperatives which have consistently driven its violent peace-making.’（p.85）Liberal rule has also resulted in wars for territory or in defence of territories; nevertheless, a story, of course, could have been told about how views of the human fitted those of struggles to command territory. This is acknowledged, but sits uneasily with the narrow view of liberal war for species life. If the racial doctrines of European empires, up to and including the genocidal racism of the Nazi regime, were also biopolitically driven ─ and the authors, indeed, write of race as part of the‘liberal biopolitics of the seventeenth century’─ then it seems difficult to separate a liberal way of war from allegedly ‘non-liberal’ wars of territorial control.¶ It seems clear that Dillon and Reid do not seek to take the logical step of arguing that the view of the human reflects, and is reflected by, how the human is ruled and how wars are both thought and fought. Why? Because for them there is something suprahistorically unique and distinct about the liberal way of war: a distinctly liberal view which foregrounds the human as the referent of security. Therefore, a second aporia arises: on what basis is this specifically ‘liberal’? It would appear that every form of rule and of war has at least an implicit view of the ‘human’ and through this view of the human the form of rule and the way of war are rationalized. There is not and cannot be anything specifically ‘liberal’ about this. The humanity in need of securing, through war on other humans, could be formed by Alexander the Great’s stoic cosmopolitan vision, or could be‘God’s chosen people’, ‘the master race’, or ‘the gains of the proletarian revolution’: there is little doubt that beliefs of what the human is, or could become, were a vital part of many non-Liberal dispositifs ─ the discourses and practices - of both rule and war. ¶ The key starting assumption, that the liberal way of war can be isolated from any other - and its alleged specific form, of ‘unending violence’, explained by its referent of the human - appears to be a particularly unproductive one. At the level of abstraction at which Dillon and Reid choose to work, there is very little here that would help to distinguish between a liberal and a non-liberal way of war（the asserted purpose of the book）. Of course, what matters is what this view of the human is. Here Dillon and Reid appear to recognise the limits of their essentializing approach: …just as the liberal way of rule is constantly adapting and changing so also is the liberal way of war. There is, in that sense, no one liberal way of rule or one liberal way of war. But there is a fundamental continuity which justifies us referring to the singular…the fact that each takes the properties of species existence as its referent object…finding its expression historically in many changing formations of rule according…to the changing exigencies and understanding of species being…（p.84）¶ Rather than understand our forms of post-political rule and post-territorial war today on their own terms and then consider to what extent this way of rule and war can be theorized, and to what extent, if any, Foucault’s conception of biopolitics may be of assistance, Dillon and Reid start out from the assumption that we live in a liberal world of rule and war and that therefore both can be critiqued through the framework developed by Foucault in his engagement with understanding the rise and transformation of liberal forms of rule. In transposing Foucault’s critical engagement with liberal ways of rule to an understanding of liberal ways of war, Dillon and Reid take a body of historical work about the changing political nature of liberal rule and transpose it into an essentialised and under theorized understanding of liberal war. This is no mean feat; how they manage this accomplishment will be discussed in the next two sections.

## Alternative

### AT Grove

**Grove’s move is totalizing, preemptive, and cedes the present to fascists**

Tallis 20 [Benjamin, Researcher at Institute of International Relations Prague, “Un-cancelling the future,” New Perspectives 1–18, 2020, https://journals.sagepub.com/doi/pdf/10.1177/2336825X20937580]

**Timeless pessimism, hopeless critique** Hope is a Form of Extortion. (Jairus Grove, Savage Ecology, 2019: 25) Both Rutger Bregman (2014) and Franco Berardi (2011) have written extensively on this pessimism. In different ways and with different aims, they argue that **despite the** huge **and** real (**although highly uneven and inequitable**) **progress that we** (in this case, many of us who live in the West) **have made in helping more people live longer, healthier, happier lives, we no longer believe we can** improve further. **We have become** collectively disappointed **by the** failures **of** political **and** technological **vision**; **shocked by the** downsides **of** modernity, **stunned by the** scale **and** complexity **of our challenges** **– and by the** pace **of** change**.** As Jonathan Meades (2014) observed, **change itself has changed: for many in the West, it used to mean change for the better2** **but for too many people that is no longer the case.** This fear of change itself has exacerbated the problem, leading to a stasis of ideas, a lack of daring, deficit of vision and vacuum of purpose. **Even faced with the existential crisis of climate change, our responses have been** piecemeal **and** incremental. Too often even the bolder proposals have been mealy mouthed or, worse, have framed human life itself as the problem (e.g. Sparrow, 2019; Wilkinson, 2020). A pious puritan streak in the environmental movement seems to relish in the idea of a future of less, a restricted and spartan life, purged of joy. It has not been widely embraced. Both Bregman and Berardi note that majorities or significant minorities of people in richer countries have long believed their children will be worse off than they are (see, e.g. Pew, 2019) – but they don’t wish to actively spur this process along. **There has been** **no credible** positive vision **of** radical change **to** countervail **this** negativity **and so we drift,** seemingly helpless **as well as** hopeless **in the** interregnum of ideas. As Bregman puts it: the real crisis of our times, of my generation, is not that we don’t have it good, or even that we might be worse off later on. No, **the real crisis is that we can’t** come up with anything better**.** (Bregman, 2014: 22) He goes on to note that **we have become so** wary **of positive visions of progress that: today we** stamp out dreams of a better world before they can take root. Dreams **have a way of turning into** nightmares, goes the cliche´. Utopias **are a breeding ground for** discord, violence, **even** genocide. Utopias ultimately become dystopias; in fact, a utopia is a dystopia. (Bregman, 2014: 23) **Examples of this way of thinking are plentiful but,** for convenience, **one need to look no further than** Jairus Grove’s scintillatingly pessimistic keynote at the Hamburg Sessions (forthcoming as an essay in NP and based on his 2019 book, **Savage Ecology**).3 **It is not that Grove doesn’t make** compelling **critical arguments** – he does and in brilliant, imaginative ways – **but** that **they** lack balance. And balance matters, whether we are reckoning with horrendous pasts or trying to boldly imaging new futures. **To see, or certainly to** dwell on, only **the** bad **in what we in the West have collectively done** (however, Grove or anyone else defines who we are), **over the entire course of our past and present is** grossly unfair. **It also amounts**, in effect, **to a** counsel of despair, **however much Grove protests to the contrary or** claims to eschew nihilism. In his keynote, **having written off our past and present, Grove also explicitly urged us in Europe and the West** to stop imagining better, progressive futures, **arguing that this has led to precisely the problems he identified**. **Grove’s critique thus not only leaves us** out of time (**without an** avowable **past, present or future) but also leaves us** without space **for** contestingnegative**,** regressive **and** repressive **political trends**. In his book, he laments the ‘debilitating stupor’ in which the work of thinkers like Theodor Adorno and Giorgio Agamben leaves us (Grove, 2019: 238). But **Grove’s own pessimism, if we took it seriously, would leave Europeans** without a political leg to stand on**. It would** **leave us** in just such a stupor – or worse – **with** no solid ground and no lever: **no way to move the world and no platform for positive, progressive change. Why bother, if everything we do only makes things worse? However much harm we** Europeans and **Westerners have done, we** haven’t **done,** don’t **and won’t** only do harm. **The** real **danger of Grove’s type of** timelessly pessimistic **and** literally hopeless **critique is that (**again, if **taken seriously**) **it breeds only** damaging inertia, inaction **and** resentment – **its** hopelessness **makes it a** debilitating critique; **its** timelessness **offers** no possibility of salvage, **let alone** progress. **It** cedes the ground of action **to those** **who many of us** (including Grove) **would** explicitly disagree with – **whether to exponents of ‘**traditional’ approaches **to IR who are more than happy to offer policy advice or, worse, to** authoritarians **and** populists **in practical politics** (as ably described in Johanna Sumuvuori’s essay in this issue). **Critical scholars** too **rarely see it as their task to construct positive visions of better worlds**. **Instead, too often they content themselves** (if no one else) **with** evermore thoroughgoing deconstructive critique – including of other critical academics. Whether totalising or parasitic, even some of its leading proponents admit that **IR’s critical project has**, thus far, **had** insufficient impact **on the world at large** (Austin, 2017, 2019). Few critical scholars will thank me for this comparison, but, in their pessimistic, misanthropic zeal, they echo what French President Emmanuel Macron called the ‘sad passions’ of the author Michel Houellebecq4 (Carre`re, 2017). They may not share Houellebecq’s politics, but many critical scholars certainly share his exhaustive (and exhausting) disenchantment with contemporary (neo)liberal societies, the state of Europe and of the West. Too often they also share his miserabilist outlook on the impossibility of change for the better and the futility or harm of even trying to improve things. **Grove does propose several forms of political action:** micro-kindnesses, **however vague** (e.g. ‘the impossible generosity and affirmation of deconstruction’, 2019: 231); resistant acts **by** brave individuals (**e.g. ‘William ‘‘Fox’’ Fallon, who sacrificed his prestigious position as head of [US Military] Central Command** because he would not go along with the plan to attack Iran’, 2019: 232); **embracing entirely** new ‘forms of life5 ’**; or** welcoming apocalypse as driver of change (2019: 229–248). **Grove** will not be confused with Goldilocks **anytime soon – these forms of action each seem either** too little **or (**much**)** too much. **Few of us would question the** value **of and** need **for** kindness and, indeed, the most hopeful part of Grove’s book is the touching introduction where he details many of the kindnesses he has himself benefitted from, mainly from people in the West where he has spent most of his life. **There is also, clearly, a role for resistance and for the kinds of acts that Grove notes have prevented executions and even nuclear war.** Yet **without a** wider programme, **without a** biggerpositive vision, **kindness and resistance** cannot sufficiently change our world for the better. **Apocalypse, on the contrary,** changes too much, **junks** too much that is good **and is** rarely likely to be an appealing option, **or something we can all get behind. The apocalyptic aspect of Grove’s position**, like that of many critical scholars, **seeks to inflict destructive harm on Western institutions rather than constructively reform them** – something Houellebecq would also relish. Apocalyptic change also smacks of the recklessly callous, negative sides of early 20th-century futurism (Marinetti, 1909), as Grove acknowledges when asking ‘How do we go wild without the cruelty of indifference?’ (2019: 280). Again, a more balanced approach to boldness would help. **To be clear, major change is needed** – that was the whole point of the Hamburg Sessions and the motivation behind giving it the theme of ‘Un-Cancelling the Future’. I’ve argued elsewhere that **the kind of socio-economically regressive, technocratic, defensive liberalisms that have dominated large parts of the last 40 years in the West have a lot to answer fo**r (Tallis, 2018). So too, of course, does the type of narrowly, teleological individually atomising (neo)liberalism that neither saw (Fukuyama, 1992) nor allowed (Fisher, 2009) alternative visions of politics, societies and economies. Mark Fisher (2009), echoing the artist Gerhard Richter (Elger, 2009), called this myopic liberalism ‘Capitalist Realism’. You don’t have to be a Marxist or even a leftist to see that a mandated lack of alternatives and a commensurate narrowing of possibilities and horizons is a bad thing. As noted above, both climate change and sociotechnical upheavals in the ways we work and live need bold visions to address the challenges they pose while also seizing the opportunities they present. **It is, however,** eminently possible **to recognise the** full horrors **of Europe’s (colonial) pasts and presents without** immediately discounting **the** possibility of improvement **coming from the West**, from Europe. **Similarly, one can recognise the myriad problems that Europeans have caused while also** celebrating **the many** positive things **they have also achieved.** Moreover, it is possible to use those achievements as inspirations for better ways of doing things – as catalysts to new, progressive creativity and to positive visions of the future. Just as Kraftwerk did in the **fragile yet fertile Germany of the second half of the 20th century when they acknowledged the abyss yet still sought a better future, including as atonement for that past.** The cancellation of the future William Gibson recently tweeted ‘‘In the 1920s, the phrase ‘the 21st Century’ was already popubiquitous. How often do we see the phrase ‘‘the 22nd Century’’, now?’’. And it’s true – we don’t have these dates anymore. As a boy, as a young man, I had mental pictures of the 21st Century. But I don’t have any sense of 2050 or 2100 – except as a deterioration or a collapse. (Simon Reynolds, Hamburg Sessions 2019, see essay in this issue) I return to Kraftwerk below but first, a little more is needed on the ramifications of contemporary hopelessness. **Rather than striving to create** new **and** compellingpositive, progressive **visions, many thinkers** content themselves with critique (Austin, 2017) while **others**, **like Grove, see** positive**,** progressive **visions and** futures– **especially those coming from Europe or the wider West – as being** necessarily harmful in themselves. This is postmodernism as hangover. **The depressed** – and depressing – **aftermath of the** shortcomings, broken promises **and** unintended consequences **of modernisms of different kinds,** in which strange connections are made and selective, guilty memory runs amok (Fisher, 2014). Forgetting the good, **it fuses the bewitchingly pertinent** **aspects of the post-positivist critical project** (which influenced many of us, myself very much included), **with more zealously** (self-)destructive **and** paralysing tendencies. As Fisher puts it: ‘Deconstruction [is] a kind of pathology of scepticism, which induced hedging, infirmity of purpose and compulsory doubt’ (2014: 16). In this mode, **scholarship** **no longer seeks to** invent the train **but** fixates **on the** train crash **or even** pre-empts **and** precludes the train’s invention **for fear of the** seemingly inescapableimaginedtrain crash to come. **Like Grove’s denunciation of the future, many of the critiques of (popular) modernisms are not so much** wrong **as** imbalanced (although some are wrong of course, others not even). **They take** insufficient account **of modernisms’** multiple **and** meaningfulsuccesses (there’s no time here, but see, e.g. Fisher, 2014: 22; or Meades, 2014, for a flavour). This leaves us in an odd situation where **many** of the **scholars**, commentators and others who criticise neoliberalism, capitalist realism and so on**, find themselves in de facto agreement with its notion that there should be** no alternative. In this view, **we** simply shouldn’t do big vision politics **because our ‘schemes to improve the human condition’ have not only ‘failed’ but will** always**,** inevitably**,** do more harm than good (Scott, 2008). **This approach,** all post and no modern, **will take us** nowhere, even as it fast-forwards the academic careers of its exponents. The future visions that are left, on the left, tend to be Marxist ones (see, e.g. Grove, 2019: 198– 202). Tarred not only by the brush of the communisms that actually existed (and their distinctly less balanced ledger than that of modernism more widely) they understandably fail to inspire mass enthusiasm. Many of their proponents are still really more interested in explaining the failure to bring about the inevitable (full communism) in the past and present than in imagining new futures that go beyond the narrow world view and limiting subjectivity of too many Marxist approaches (see, e.g. Scribner, 2003; Sˇitera, 2015). This has done little to address the crisis of hope or to countervail prevalent contemporary pessimism. **The** loss of the belief **in the** progressive future – **that** tomorrow **can be** better **than yesterday and today – and the related erosion of faith in our ability to** positively shape our own destiny **are** what Berardi (2011: 13) called ‘**the slow cancellation of the future’**. As Simon Reynolds noted in his Hamburg Sessions keynote (included in this issue of NP), the cancellation may have started slowly in the 1970s, but, by the 2000s, it had picked up speed and its effects could start to be seen. The first of these – its more (neo)liberal variant – was the feeling of living in an endless present. For a lot of people in the West, this has been comfortable in many ways (although often unevenly and unfairly) and has had distinct advantages over the past (the extension of rights and opportunities to broader swathes of the population) but without much hope, optimism or greater purpose. Unless it provokes the nostalgic responses outlined below, **this** endless present **can lead to a sense of** ennui, **a** lack of direction **and** loss of momentum. **The second, more overtly** sinister, **variant that** fills the vacuum **left by the** dearth **of** positive, progressive **visions for the future takes the form of** darker re-enchantments **focused on the (**imagined) past(e.g. Campanella and Dassu`, 2019). **Whether ‘**making America great again’, ‘taking back control’ **in the United Kingdom or claiming to offer an ‘**alternative for Germany’, **these movements are fundamentally premised on a** backward-looking politics **of** nostalgia. **The** pessimism about the present **and** worries about the future **on which these movements have each capitalised have given rise to an** increasingly defensive **politics of** closing down **and** protecting, **at the expense of opening up and integrating**. Nativism **and** pessimism tend to go hand in hand: **shrinking pies bring narrowed** **horizons and hasten the circling of wagons around exclusive and chauvinistic visions of national communities**. Too often, this retro-rightism has been met only with retro-leftism or a tired centrism that merely seeks more of the same, to smooth the endless present. But that can change ...