# aff updates– wave 2

# case

## misc

### Cohesion

#### NATO cohesion necessary to maintain stable world order

NATO 20 (Group Appointed by the NATO Secretary General, NATO 2030; United for a New Era, 11/25/2020, <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf>) -LH

In spite of these challenges, NATO remains indispensable. In fact, the fundamental purpose of NATO is more demonstrably clear today than it has been for decades. NATO has weathered stormy times before, surviving the Soviet threat, the Suez Crisis, divisions among Allies over the Vietnam war, dictatorships in its own ranks, the Euromissile debates, disagreements over enlargement, and the Iraq War—just to name a few. Now, as then, Allies have remained bound together by a combination of shared principles, democratic institutions, and the benefit that all Allies derive from collective security. Looking out to 2030, the need for a collective defence Alliance to protect Europe and North America against threats to their physical security and democratic way of life is as strong as ever.

Yet NATO will have to continue to adapt. In a world of systemic challengers and proliferating threats, the Alliance, in complementarity with the comprehensive military adaptation it has undergone, must cement its ability to act as the principal political forum for the strategic and geopolitical challenges facing the transatlantic community. Fulfilling this role will require even greater cohesion than NATO has possessed in recent years. As it has since NATO’s founding, cohesion resides in the ability and will to act collectively against shared threats. This is the lifeblood that ensures the vitality, credibility, and durability of the Alliance; it becomes all the more important in a sharpened competitive environment that requires collaboration and effective networks to deal with growing threats.

In recent years, Allies have strengthened the military component of NATO and should continue to do so. But in parallel, they must move decisively to bolster the political dimension of NATO, including its foundations of shared democratic principles, mechanisms of consultation, processes of decision-making, and political tools for responding to current and emerging threats. If they do so, NATO will be in a strong position to protect the freedom and security of its members and act as an essential pillar of an open and stable international order.

#### Cohesive NATO approach to cyber operations will be critical in dealing with cyber threats

Shea 18 (Jamie Shea, Dr. Jamie Shea is deputy assistant secretary general for emerging security challenges at NATO, “Cyberspace as a Domain of Operations What Is NATO’s Vision and Strategy?” MCU Journal, vol 9, no 2, Fall 2018, <https://apps.dtic.mil/sti/pdfs/AD1068701.pdf)-> LH

In sum, 2016 was the year when the cyberthreat ceased being a concern primarily for individual entities, such as banks, critical infrastructure providers, or hospitals worried about losing data, to become an instrument of hybrid warfare, where the state and society are virtually under permanent attack. The problem with cyber is that, because it is so easy to use, states may decide to attack targets and risk an increase in international tensions that they would probably refrain from doing if they had to use more conventional and overtly aggressive means. So cyber blurs the clear distinction between war and peace and creates a sense that everything a state normally believes it has under control (its administration, election processes, critical infrastructure, key supply chains, and economy) is now being contested or is even under permanent siege.

Given this multiplicity of cyber threats and attack vectors, the concept of what a state needs to defend has shifted. It is now no longer a specific strategic asset, such as an oil refinery or airfield, or a particular invasion route, such as the Fulda Gap in Germany during the Cold War, but it becomes virtually any kind of critical national infrastructure—from undersea internet cables to banks; electricity grids; industrial control systems (ICS); telecommunications; and gas, oil, and water pipelines.13 The scope is almost endless. The state cannot hope to achieve full protection of all these complex and often interdependent networks alone. It has to prioritize and delegate protective responsibilities to the regional or local level or to the private sector that owns and operates much of this critical infrastructure. In terms of basic cybersecurity, it becomes the duty of care and risk calculation of the individual citizen. Cyberspace has rapidly become a domain where everyone is calling upon everyone else to take action. The individual calls on the bank to provide better protection, the bank demands better software from the tech company, the tech company recommends better insurance coverage, while claiming that it is only a platform to post and transmit data and has no particular responsibility for the content. Meanwhile, the state has to decide whether regulation or voluntary effort is the best way to induce companies and individuals to improve their cyber hygiene and restore trust in a cyberspace that is an increasingly important part of economic growth.

For military establishments and an organization such as NATO, fully establishing cyberspace as an operational domain imposes clear cultural shifts and organizational adaptations, with the follow-on impacts for all other operational domains. Cyberspace cannot be a separate silo but has to be integrated with all these other operational domains. Operations in cyberspace need to be designed to support conventional military activity, as a force multiplier, and vice versa. This means that commands must understand, trust, and be prepared to employ all capabilities and determine those situations where the use of a cyber effect would perform a military task more quickly, efficiently, or more cheaply than a conventional weapon. An example is the debate in the Barack H. Obama administration during the Libya conflict in 2011 over whether to use cruise missiles or cyberattacks to take down Muammar Gaddafi’s air defenses.14 This debate revolved around cost-effectiveness, durability of impact, and the international precedent that might be created by the U.S. use of military cyber capabilities. Essentially, it means understanding the characteristics of offensive cyber and what it can and cannot achieve and the risks in terms of cost-benefit analysis. Collateral damage is one such risk as cyber tends to have horizontal rather than vertical effects through the nature of the hyper-connectivity of the internet. When the Stuxnet worm was used in 2010 against the Siemens operating software at the Bushehr nuclear power plant in Iran, it was introduced via a USB stick outside the internet and was designed to infiltrate only one type of software.15 It was seen as preferable to military actions, because it was covert, highly specific, and a way to minimize violence even if hundreds of Iranian centrifuges would be incapacitated. Yet, it ended up on the internet and traces of Stuxnet were found subsequently in 36 countries. Thus, greater transparency will be needed between those allies, such as the United Kingdom, that have publicly announced their willingness to voluntarily contribute national cyber effects to NATO. Additionally, NATO commanders will need to identify which effects are potentially available, what are the targets to which they apply, and how quickly they can be generated in a crisis or conflict scenario, but above all what the actual impact and fallout of such cybereffects are likely to be.

NATO has defined a mechanism for this transfer of cyber effects from the nation to the NATO command structure under the political oversight and control of the alliance. A Cyberspace Operations Centre (CYOC) is being established at Allied Command Operations (formerly SHAPE) in Mons, Belgium, to enhance early warning, carry out strategic and operational planning, factor cyber realistically into NATO training and exercises, and define the scope of joint cyber/conventional operations. Soldiers, sailors, airmen and airwomen, and NATO civilians who operate in other domains must be as ready to support cyberspace operations as those who regularly operate in cyberspace are ready to support any other joint operation. This will without a doubt generate the need for more cyber defense specialists and also more training and education for senior military and civilian leaders across the NATO enterprise in both the military and political ramifications of using cyberspace. For instance, a recent crisis-management exercise organized by Estonia for EU defense ministers (called CYBRID), which simulated a series of cyberattacks against an EU maritime force in the central Mediterranean, revealed several weaknesses. First, one weakness was the reticence of attributing the attacks and the amount of evidence required to attribute them properly. Second, it was difficult to determine whether the characteristic of the attack was simply hostile behavior or actual armed aggression. Third, there was a weakness in the political willingness to assign blame, as well as weaknesses in the usefulness of a number of possible response or retaliatory options (the “toolbox”). This pointed to a need for better coordination from the top.

So, as with the evolution of nuclear deterrence in the 1950s, it makes little sense to develop cyber capabilities and technical expertise if the leadership has a poor grasp of the conditions determining if, when, and how a cyber effect can be used. There is also the possibility that cyber effects are designed foremost for deterrence purposes and signaling rather than for actual battlefield use. This means regular crisis management exercising to synchronize military and political thinking and decision-making cycles is required. Such exercises can help to develop a comprehensive set of crisis response options involving cyber and/or combined cyber and conventional actions. Over time, a basic understanding of attribution methodology needs to be acquired so that what is deemed sufficient at the national level is also adequate for other nations to adhere to and express solidarity through collective action. A good example of this, albeit in the area of 2 chemical weapons, is the attribution by the British government to Russia of the Novichok nerve agent, used against two Russian citizens in Salisbury, United Kingdom, in March 2018.16 Once the UK’s findings were presented to NATO and the EU, the member states simultaneously expelled a significant number of Russian diplomats and agreed to clamp down on Russian intelligence operations in their territories.

As these retaliatory actions become more frequent (e.g., Special Prosecutor Robert Mueller’s grand jury recently indicted 12 Russian Main Intelligence Directorate [GRU] officers for their alleged involvement in hacking into the U.S. election campaign), it will also be important to analyze which of this expanding toolbox of responses below the threshold of an Article 5-type of military response actually has an impact in changing the strategic calculus and behavior of our adversaries.17 Or, in other words, what can be done to change the current calculus of cyber as a low-risk, high-gain operation into one that is high risk and low gain? For instance, do unilateral or collective retaliations work better over time than bilateral agreements, such as the 2013 U.S.-China agreement on restraint in cyberspace?18 What is the practical benefit of international norms and confidence-building measures, such as the two packages endorsed by the Vienna-based Organization for Security and Co-operation in Europe (OSCE)?19 At all events, it is clear that we still have a long way to go before states recognize the essential red lines of effective cyber deterrence and stability; for instance, noninterference in political processes, refraining from attacks on critical national infrastructure, refraining from attacks on the “public core” of the internet, agreeing on common standards for attribution, and agreeing that attacks on nuclear command and control or vital space observation and communication satellites are impermissible. Even if a universal agreement establishing these red lines (i.e., by the United Nations Group of Governmental Experts) still seems a long way off, embedding them in regional or “mini-lateral” frameworks such as the Association of Southeast Asian Nations (ASEAN), the Commonwealth, or the African Union seems possible, and NATO could usefully take them up in its own partnership frameworks. For instance, a mutual agreement on certain norms could be embedded in NATO’s individual cyber cooperation agreements with partner countries, alongside the technical exchanges such agreements usually provide. A memorandum of understanding with Finland has already been concluded and can lead the way to similar agreements with like-minded countries, such as Sweden, Japan, Australia, and New Zealand.

#### Cohesive NATO is Critical for Deterrence of Russia and China

Marcus **Kolga 21**, Marcus Kolga is a senior fellow at the Macdonald-Laurier Institute’s Centre for Advancing Canada’s Interests Abroad., 10-5-2021, accessed 6/28/2022, "Improving NATO’s cohesion is critical to combat Russia and China’s threat: Marcus Kolga for Inside Policy," Macdonald-Laurier Institute, <https://macdonaldlaurier.ca/improving-natos-cohesion-critical-combat-russia-chinas-threat/> //3AM

A united NATO is critically important to projecting credible deterrence. The erosion of domestic trust and confidence in the Alliance among its member states, including Canada, represents a threat to this cohesion. A proposal to withdraw Canada from NATO was tabled at a recent policy conference for one of Canada’s three major political parties. The proposal was defeated, but it represents a fringe anti-NATO narrative within Canada’s illiberal left; if left unaddressed, such a narrative could grow.

If countries like Russia perceive NATO as an atomized collection of states with varied priorities rather than a unified front, the Alliance is exposed to a significant risk of miscalculation in which a foreign adversary might believe they can cross a red line and only face a limited response. Thus, gaps in cohesion within the alliance directly threaten to undermine political and military deterrence. The Alliance and members states must work towards improving communications strategies to foster greater basic general understanding of NATO’s purpose, its missions and its role in protecting its members against external threats.

Similarly, if we see threats as atomized or disparate, we may lack the capacity to adequately respond. Organized GRU terrorist attacks in Czechia, the Salisbury poisonings, transnational repression and censorship, cyberwarfare, disinformation, and overt military posturing all pose threats that are aimed at the same essential goal: undermining and supplanting the power of liberal democracy and advancing authoritarianism. Through this lens, challenges posed by other actors, including China, must also be considered as part of the broader range of shared threats posed to the democratic community as a whole.

If we are to succeed in tackling these shared threats, greater transatlantic cooperation is needed. It cannot remain stagnant, however; it must evolve and expand. The serious nature of the threats, their potential to become kinetic, and the possibility of adversarial coordination (whether formal or informal) means that we must expand our tools to meet these challenges.

In the case of Ukraine, on whose border the Kremlin mobilized over 100,000 troops this past summer, the Alliance should consider extending a Membership Action Plan despite the skepticism of some allies. Ukraine must also be empowered in a similar fashion to frontline NATO states like the Baltic states and Poland. After all, the eFP mission in Latvia not only provides military deterrence, but strengthens interlinkages, develops societal resilience, and provides clear and sustained solidarity.

Finally, the growing threats of foreign interference, information warfare, cyber attacks and emerging threats to Canada’s Arctic requires a coherent long-term strategy and an evolved notion of collective defence, which includes strengthening our partnerships with non-NATO allies in Europe, Asia, and around the world.

Until we impose consequences that force Moscow and Beijing to strategically reconsider their ongoing efforts to probe the extreme boundaries of our threat tolerance, they will continue to test our capacity and political will to confront their aggression. This requires a common understanding and acknowledgement of the threats. It took Russian aggression in 2007 in Estonia, 2008 in Georgia, and the invasion of Ukraine in 2014 to achieve a basic common understanding of the threat posed by Vladimir Putin’s government. Since then, NATO’s eFP missions have thus far deterred Vladimir Putin’s neo-imperialist ambitions in the Baltic Sea region.

We must work towards achieving a similar consensus on the threats posed by Russia and China’s use of information and influence operations, as well as economic, cyber and political warfare against the community of democracies and the developing world at large in order to develop resilience and a common defence against them.

**NATO intelligence sharing key to allied response**

**Maigre 22** (Merle Maigre is a Non-resident Senior Fellow with CEPA's Transatlantic Leadership Program and CEPA's Digital Innovation Initiative, 4/6/22, accessed 6/24/22, “NATO’s Role In Global CyberSecurity”,

<https://www.gmfus.org/news/natos-role-global-cyber-security> (JB)

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 transparency. The growing relevance of attribution is partially due to states becoming better at attributing cyber operations. 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 consequences.** 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 practice. The **best way to implement** the international norms **is by** calling out behavior and having **consequences when these norms are breached**. Attribution 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 cyberattacks? Effective public attribution requires a clear understanding of the attributed cyber operation and the cyber-threat actor, but also the broader geopolitical environment, allied positions and activities, and the legal context. The public attribution framework put forward by Max Smeets and Florian Egloff in March 2021[27](https://www.gmfus.org/news/natos-role-global-cyber-security#footnote27_pukyrym)

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 combination of these four components enables consistent decision-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—information 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 adversary cyber activity? During the Nordic-Baltic foreign ministers meeting in Tallinn in September 2020, a 90-minute tabletop exercise was organized[28](https://www.gmfus.org/news/natos-role-global-cyber-security#footnote28_cpch8u5)

to test the ministers’ ability to respond to and attribute an escalating cyberattack. They answered multiple-choice questions on communication of and possible diplomatic countermeasures to the attack. The ministers 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](https://www.gmfus.org/news/natos-role-global-cyber-security#footnote29_topliia)

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 accurate, timely, and actionable intelligence than what has transpired with Ukraine.[30](https://www.gmfus.org/news/natos-role-global-cyber-security#footnote30_qki9qsu)

**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 alliance behavior according to the threat landscape. This means a sharper focus on future responses to high- and low-end cyberattacks along with concrete deterrence 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-level commander. 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](https://www.gmfus.org/news/natos-role-global-cyber-security#footnote31_9likw2h)

**The alliance should clarify which allies are responsible for offensive cyber operations against certain targets** and the information-sharing and notification requirements.

#### US NATO cohesion key to deterring cyber attacks

**Christian 20** (Christian, Joshua D,, Monterey, CA; Naval Postgraduate School, 2020-06), 6/6/20, accessed 6/24/22, “Russian CYber Operations to Destabilize NATO”, <https://calhoun.nps.edu/handle/10945/62032> (JB)

This thesis uses a case study analysis to better understand the effects of Russian cyber operations. This approach is best to grasp how the cyber operations have become more effective and efficient over time. This has enabled Russia to conduct operations of similar ends against multiple states in order to further its own objectives. Russia views NATO expansion as a direct threat to Russia and reasoning behind this will be analyzed to discover where it fits into Russian grand strategy. **Lack of political cohesion** within the NATO Alliance **creates a vulnerability for Russia to exploit.** Political instability and distrust in the government can be analyzed through the 2016 presidential election, as well as the election tampering in Europe, because both are important case studies to showcase how Russia has adapted the use of cyber and technology to further the effectiveness of its activities. **Civil preparedness and resiliency are key** parts of NATO strength that Russia has attempted to exploit to diminish NATO’s capacity to respond during a crisis. Dragonfly and NotPetya displayed the progression of Russian cyber capabilities against critical infrastructure in a short period of time. The effectiveness and concerns highlighted by these cases are important to analyze in order for NATO states to better prepare to defend against cyber operations of this type. The disruption and damage that can be caused through **critical infrastructure attacks has a global impac**t that far exceeds that of the United States and NATO.

### NATO key

#### Action via NATO takes advantage of the Alliance’s uniquely valuable ability to create foundations of consensus and action beyond the Alliance

Skaluba and Rodihan 22 (Christopher Skaluba and Conor Rodihan, “No consensus? No problem. Why NATO is still effective,” Atlantic Council, 1/18/2022 <https://www.atlanticcouncil.org/blogs/new-atlanticist/no-consensus-no-problem-why-nato-is-still-effective/)-> LH

As the crisis over Ukraine intensifies, key stakeholders are looking to Brussels for signs of Western resolve. At the NATO-Russia Council meeting on January 12, the Alliance delivered: In a vivid expression of solidarity, it categorically (and unanimously) rejected Russian demands to forgo future expansion or withdraw forces from member countries.

Yet as the crisis evolves, decisions about how to support Ukraine will become more difficult, and there’s a limit to how unified NATO can be. While the West might agree on introducing tough new economic sanctions and reinforcing the Alliance’s eastern flank, boosting Kyiv’s military capacity—by supporting an insurgency, for instance, or sending anti-tank weapons—will be impossible to achieve by consensus and is much more likely to come from individual members than under NATO auspices.

This shouldn’t be surprising. Consider Russia’s annexation of Crimea in 2014 and its ongoing support for separatists in Ukraine’s Donbas region: NATO actions in support of Kyiv have been more political than operational, leaving it to individual allies to provide munitions, equipment, and training to Ukrainian forces. And despite a recurrent pledge that Ukraine would one day be welcome to join the Alliance, as well as the sympathy expressed by allies for Ukraine’s plight, there’s been precious little progress on this front.

NATO is primarily concerned about defending its members from Russian aggression—which it is also wary of provoking by supporting the Ukrainian military.

Yet despite its lack of meaningful military support for Ukraine, the crisis has been the animating issue on the Alliance’s agenda since 2014. Russia’s attacks on Ukraine and its support for separatists have driven major NATO initiatives on readiness, defense planning, force posture, intelligence, and technology development, with an eye toward beefing up the Alliance’s northern and eastern flanks and deterring Russia in both the conventional and sub-threshold realms. As an institution established to safeguard Europe, it has successfully geared itself to deter the type of destabilizing Russian belligerence currently on display.

Critics of the alliance (and even some supporters) have interpreted NATO’s unwillingness to militarily support Ukraine—especially during the most significant challenge to the European security order since the Cold War—as an indicator of its declining relevance, timidity, or its divisions. But that overstates the importance of political consensus to NATO’s value and understates its role as an effective and flexible defensive alliance. This is a role with potentially critical benefits for Ukraine.

First, it sets too high a bar for an alliance of thirty members with aligned, but distinct, priorities. Unanimity on every issue is impossible, let alone one as complex as military support to Ukraine. Debate and disagreement, as it should be for any democratic institution, are built-in features of NATO—not bugs. In reality, it’s astounding how often NATO does reach consensus about issues big and small, creating an unrealistic expectation that it always will. The opposite of consensus is not failure. Suggesting otherwise turns any debate that doesn’t end harmoniously into an indictment of NATO, playing straight into Russian propaganda.

Second, a belief that NATO’s value is tied primarily to achieving consensus on every issue misses the more mundane (and important) ways it supports its allies and partners. Its affinity for process—particularly its ability to build a common situational understanding among its members—is an invaluable tool. Habits of consultation and information sharing, buttressed by deep cooperation on operations, intelligence sharing, defense planning, and interoperability, create the foundation upon which any consensus is to be built. Even in the absence of that agreement, the ability to collectively define threats and jointly train to confront them is immensely valuable in its own right.

Third, these habits of cooperation give NATO members the flexibility to act outside of the Alliance’s frameworks. While NATO does much by consensus—such as its missions in the Baltic states—the skills it helps members develop is central to enabling them to form separate coalitions for action. This happened recently with ample success in taking on the Islamic State. Such flexibility should be a point in NATO’s favor, not evidence of its ineptitude.

In the case of military support for Ukraine, policymakers will find more attractive alternatives for dealing with Moscow’s aggression outside of the auspices of the Alliance. Up to and including its recent dialogue with Russia, it has taken a host of consensus actions to support Ukraine—from condemning Kremlin aggression and standing up for Kyiv politically to reaffirming its open-door policy with an expectation that Ukraine will eventually become a member. It might even share intelligence and develop training and advisory programs for the Ukrainian military.

And while it won’t find a consensus to fight, it could provide the foundation for certain allies to support Ukrainian forces in ways consistent with their national priorities outside of NATO. In that case, NATO’s enabling value to its members in complicating Putin’s cost-benefit assessment should be applauded.

Last week’s NATO-Russia Council meeting showcased an Alliance working in lockstep and finding political consensus in responding to preposterous Russian demands. NATO should always strive for this degree of consensus. But if and when this crisis intensifies, and Putin advances further into Ukraine, expectations for NATO assistance will be raised, decisions about how to respond will become more difficult, and consensus will be more elusive.

Despite the rhetoric we might hear in response, this is not evidence of NATO’s ineffectiveness—but rather a reflection of how democratic institutions function. And even absent consensus, NATO can still contribute invaluably to Ukraine’s sovereignty.

#### NATO remains a uniquely valuable institution to the US—influence and capacity to foster coop is unmatched

Skaluba 17 (Christopher Skaluba, Christopher Skaluba served as the principal director for European and NATO policy in the office of the secretary of defense from 2012 to 2015, “IN PRAISE OF NATO’S DYSFUNCTIONAL, BUREAUCRATIC TEDIUM,” Texas National Security Review, 11/7/2017, <https://warontherocks.com/2017/11/praise-natos-dysfunctional-bureaucratic-tedium/>) -LH

A year after Donald Trump’s election to the presidency, the furor around his approach to transatlantic security has predictably calmed. Part of the reason is saturation. Like antibiotics, provocation of one’s allies loses its potency when used excessively. Part of the reason is that the president has found a more willing and compelling foil, in the form of Kim Jong Un, than those buttoned-up European leaders he accuses of freeloading. Certainly, part of the reason includes the administration’s Russia-related scandals and Robert Mueller’s investigation. The president’s hostility toward NATO has always felt more like a sop to Moscow than a matter of principle and thus not a good look with indictments swirling.

But much of it has to do with the nature of the alliance itself. NATO’s bread and butter is cooperation on activities like planning, doctrine, interoperability, and logistics — things which are uninteresting to the general public discourse and largely resistant to the rhetorical or policy whims of even the president of the United States. Cooperation in these areas, while camouflaged to all but the most intense NATO watchers, can move the needle to the benefit of the United States in concrete and practical ways. As Secretary of Defense Jim Mattis heads to Brussels for his third meeting of NATO defense ministers in ten months, it is precisely to ensure such work continues.

Perception Is Not Policy

If it is fair to stipulate, without a hint of irony or partisanship, that the president makes decisions based on a rather shallow understanding of the pertinent facts, then his initial posture towards NATO and Russia makes sense. In fact, as someone who watched an episode or two of The Apprentice, Trump’s embrace of Russia was predictable. Equipped with a disposition that necessarily invites competition between opposing factions, nerdy NATO with its committees and communiques never had a chance against a tiger-hunting former KGB agent who invades countries with impunity and without a shirt. Putin is ready-made television.

Yet, as others have ably pointed out, viewed through the lens of genuine policy, Trump’s complaints about European security and its key players have some basis in fact. And while it is tempting for policy professionals like me to seek some novel, far-reaching meaning from the impolitic veneer of his tweets and applause lines, the most remarkable thing about Trump’s censure of NATO is how quotidian it is as a matter of policy. Questions about NATO’s obsolescence date from at least the 1960s and have been a proverbial albatross for the alliance since the end of the Cold War. That the United States is over-invested in NATO relative to the Europeans and Canada is an acknowledged fact by nearly everyone working transatlantic issues. And while I grimaced at the graceless pluck of invoicing Angela Merkel for Germany’s pedestrian defense spending, if true, it was a gambit rooted in cause.

Even in tone, Trump’s complaints alternately echo Secretary Donald Rumsfeld’s grouchy demonization of “Old Europe” in 2003 and Secretary Robert Gates’ headmasterly admonition of European defense spending in 2011. Similarly, Trump’s flattery of Putin shares policy fingerprints with both President George W. Bush’s plumbing of the Russian leader’s soul and President Barack Obama’s unfulfilling reset, even if the “Pale Moth’s” growing rap sheet since those halcyon times makes the recent spectacle hard to stomach.

What is unique about the Trump era is the juxtaposition of his views on the allies and Russia. The natural correlation is something akin to the Cold War and Obama’s second term: The United States is harmonious with NATO and frosty with Moscow. Disagreements with France and Germany about the 2003 invasion of Iraq occasioned another possibility whereby the United States is at cross-purposes with both sides. Obama’s first term was characterized by a Medvedev-inspired bonhomie with Moscow that was palatable as long as relations with the allies were equally durable. Trump has introduced the final option: threatening estrangement with traditional allies while currying favor with a Russia clearly hostile to U.S. interests. It is this dynamic, among others, that is most responsible for the disconsolation of America’s foreign policy elite.

Yet this unusual state of affairs is more histrionics than a deliberate policy course correction. Even holding out the quixotic possibility that Putin is willing and able to support some of Trump’s foreign policy goals (or, heaven forbid, electoral aspirations), there is no reason this should come at the expense of cordial relations with the Europeans. Unless, the logic goes, that is the price of Russia’s help, or more sinisterly, that Putin can otherwise manipulate Trump’s actions. The former requires malice aforethought inconsistent with most evidence about how the president operates. The chances of the latter, however implausible, are non-zero, and should Mueller find hard evidence to suggest anything of the sort, we would find ourselves in a scandal so serious as to make these matters quaint. In any case, the Congress, a substantial portion of American public, and Trump’s post-Flynn national security officials have all resisted any quid pro quo with Moscow that undercuts our allies. Which leads me to the conclusion that Trump’s enigmatic stance toward NATO and Russia is unlikely to change unqualified American support for the alliance, even when his public actions suggest otherwise. That Mattis and Secretary of State Rex Tillerson have attended regular ministerial meetings, that NATO’s secretary general has visited the White House, and that Trump himself has shuffled off to Brussels like his predecessors before him lends credence to the theory that practical cooperation with the alliance continues apace — in ways often directly in conflict with Russian interests.

Vapid, Vexing, Valuable

As a young Pentagon staffer, I was seconded to Brussels for a few months in 2003 to work at the U.S. Mission to NATO. Naturally excited and looking to make a positive impression, I rushed to backbench a NATO committee meeting at the first opportunity. The topic, I vaguely recall, was related to NATO capability development. I remember the imposing conference room, the translation booths, the flags, and the bevy of well-tailored colleagues from around Europe. I can still conjure the anxious pride of sitting behind the placard stamped “United States” for the first time. This was a dream. About 20 minutes later, it literally became one. I had to repeatedly stab myself in the leg with a pen in order to prod my jet-lagged body into consciousness. I could not have imagined, until that moment, how detailed and dull the daily discourse of NATO often is. And lest you are unconvinced by this reminiscence, I highlight a former secretary of defense’s habit of doing crossword puzzles during NATO meetings or the Weekend at Bernie’s jokes, prominent among senior Obama officials in the Pentagon intended as a metaphor for an alliance seen as moribund.

Moreover, NATO, like any large institution (hello Pentagon!), is raft with dysfunction and internal contradictions. My particular hobby horse is NATO’s requirement for defense spending. Not that, infamously, only a handful of members will ever meet the 2 percent of GDP target, but that in spite of this obvious reality, NATO continues to promote the 2 percent goal as one of its core principles. In high school, I worked summers at a drugstore where the staff would take turns getting lunch for the group. One weekend, I arrived at the chosen spot, order in hand, to be told that because of a delivery issue, the establishment was not serving beef. Incredulous, I proclaimed, “but you’re Burger King.” I likewise imagine a generation of earnest transatlantic scholars staring at their textbooks, perplexed and mumbling, “but you’re the 2 percent people.” To brand your organization with a characteristic that it will never realize takes a chutzpah that Trump can appreciate, but is nonetheless marketing malpractice of the first order. Compounding this folly, Greece, whose military is antiquated, bloated, and oriented toward conflict with another NATO ally, is championed alongside the formidable militaries of the United States and the United Kingdom because it meets the 2 percent threshold. NATO crediting Greece for its military spending is tantamount to House Stark thanking House Frey for hosting the Red Wedding. There are better ideas out there.

Nevertheless, I come here to praise NATO, not to bury it. I detail the aforementioned grievances to assure anyone reading this that those of us experienced in the alliance’s mysterious arts are not ignorant of its problems. Much of our work, over many years, has been dedicated to fixing or mitigating them. And that same experience allows us to appreciate the benefits that NATO membership accrues to the United States. The cynical nature of our times and politics makes it easy to criticize an organization like NATO, whose day-to-day work does not translate readily to the masses. Even so, to have well-founded frustrations with an elaborate and esoteric bureaucracy is one thing. To conclude such an organization is unworthy of American participation or investment is another. Such a posture is at best impetuous and at worst antithetical to the cause of “America First” that NATO naysayers are intent on restoring.

At its core, NATO is a culture of intensive, banal cooperation. It is a swanky headquarters building with Euro-looking conference rooms and passable coffee where mundane meeting after mundane meeting takes place on logistics, standardization, and capability development. It is command centers and watch floors and training areas where alliance militaries practice the monotonous regimens so critical to the science of arms. It is the Alliance Command Transformation — A.K.A. the really boring part of NATO — where the agonizing particulars of interoperability and doctrine are worked out. It is the operational realization of the inane political aspiration to cram soldiers from 14 different nations into a single brigade. It is a collection of customs and habits that dictate how decisions will be made when the balloon goes up. It prescribes where to meet and the rules for discussion. It ensures that you can trust the colleague next to you because you’ve worked with her in such a setting a hundred times before. It structures discourse and operations such that, by ritualizing behaviors and in making a thousand minor decisions, you build the blocks of strategic dexterity that NATO sometimes demonstrates.

The most poignant example I can point to of NATO’s potential is its mission in Afghanistan. Over 15 years, and two distinct American administrations, the United States, through this tool called NATO, coaxed more than a quarter of the world’s countries to participate in a far-flung and elusive mission that had nearly nothing to do with their own national interests. That political feat, however, is rivaled by the operational one, where NATO allies and partners sustained overlapping security, capacity-building, and counter-insurgency missions across an enormous geographical expanse for nearly a decade and a half. The complexity of military operations is often undersold to the public in popular characterizations of war, not to say anything about war by a coalition of militaries measurably different in size, capability, and aptitude. That something the scope, scale, and duration of the International Security Assistance Force (ISAF) was ever realized is rather breathtaking. We could, and should, argue about the strategic success of ISAF, and the costs, and whether it would have been easier operationally had United States gone it alone, but those are different debates. To appreciate ISAF is to recognize the nameless technocrats and servicemen who, through muted craftsmanship, navigated cranky parliaments and inordinate logistical puzzles to achieve a political and operational tour de force. This NATO — obscured to the public and the politicians that charge it with obsolescence — substantiates a faith in the power of process that would make Sam Hinkie smile.

Fashionably Old-Fashioned

Ask some Middle East or Asian security experts about NATO and they inevitably roll their eyes. That old thing. But have a deeper conversation about how they are going about defense cooperation in their regions and you quickly recognize what they want, however impractical, is NATO in all its blessed, bureaucratic glory. Like vegetables to a child, NATO is never what you want, but usually what you need. If you are a purveyor of soft power, NATO should be your thing. Where else can you force common purpose and consensus on scores of dissimilar nations by wont of incessant badgering (i.e., pretty much the job of American officials at NATO)? If you are a hard-power type, I remind you again of ISAF and the fact of 52 militaries operating with solidarity to impose their martial will. In either case, you begin to understand Vladimir Putin’s hostility toward the alliance — of what it is and what it could be should it ever have occasion to turn its withering gaze to Moscow. Is Putin’s disdain not proof itself of NATO’s indomitable relevance and potency?

Ultimately, I suspect Putin’s paranoia is both about the methodical reach of alliance hard power into his perceived sphere of influence as well as the fact that that alliance nations, on the whole, aspire to live in a world defined by classic liberal values. Putin begrudges not only NATO’s endurance and adaptability, but the goody-two-shoes Western order it represents. He certainly delights in Trump’s anti-liberal tendencies and hopes they will weaken NATO, but recognizes they are unlikely to change its deep-rooted puritan culture. To wit, consider again the 2 percent issue. In a world obsessed with image and status, any number of European defense officials fight to maintain the target because it is useful for keeping pressure on their own parliaments and politicians for increased defense spending. That is, the alliance chooses to look impotent in an attempt to do the right thing rather than revise its blueprint to look better. NATO, bless its heart.

So yes, NATO has its problems. The United States pays too much in financial, human, and intellectual resources. On many days, participating in alliance business is an exercise in herding cats, where the United States, for all its trouble, gets to listen to countries with militaries smaller than the office of a Pentagon undersecretary regale everyone with their views on defense planning. Yet, every previous administration has concluded the benefits of NATO for the United States outweigh these costs — that the potential NATO has, and at times, realizes, is too valuable to our security to go without. Recognizing that NATO’s costs are taxpayer funded, Rumsfeld, Gates, and all of us should demand more of alliance members and partners. However, we should not let a sense of grievance confuse our understanding about NATO’s value to U.S. interests — of the benefits that accrue from the yeoman’s work of professionalizing the world’s militaries and security institutions such that they can work competently with Washington to promote American interests. I doubt whether the president can upend this calculus, even if that were his conscious intention. Instead, I imagine the president as a sort of Erlich Bachman whose bravado and opportunism occasionally prove a useful spur to Mattis’ driven and visionary Richard Hendricks and Tillerson’s Big Head. That should be enough for NATO to publicly navigate the Trump era while practical cooperation grinds on systematically beneath the surface.

#### Interconnectivity of cyberspace means NATO cyber response must be from the institution as a whole

Ekstedt, Parkhouse, and Clemente 12 (Victoria Ekstedt, Tom Parkhouse, Dave Clemente, “National Cyber Security Framework Manual,” NATO’s CYBER DIMENSION, 2012, <https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf>) - LH

NATO’S CYBER DIMENSION Digital communications are the backbone of society and, whilst they are a capability that NATO exploits for operational and administrative advantage, it is neither an environment that NATO, nor its Member States, can claim to control. The ability to collect, process and deliver vast amounts of data requires huge increases in military and bureaucratic efficiency. At the same time, all NATO nations need to work with the fact that their dependence on cyberspace, including the internet, is a major vulnerability and, unless invested in, will result in deteriorated overall resilience.571 NATO, the armed forces, International Organisations (IOs) and Non-Governmental Organisations (NGOs) that work with it expose themselves to known and unknown risks while operating in the digital domain. Business as usual for NATO includes the procurement and organisation of military capabilities, engaging in the political processes that support the operation and coherence of the North Atlantic Council, and the administration and control of the NATO command elements and forces assigned to NATO activities. It is a huge undertaking with operational, logistic, economic, political, technical, environmental and reputational risks.

The Alliance is inextricably linked to the digital domain and is faced with many threats that create problems for Member States since cyberspace is international by nature. The interconnectivity makes a weakness of one country a weakness in all, which means that states and organisations cannot deal effectively with cyber threats on their own.

### Active defense good

#### Active defense via OCOs better than current cyber deterrence-- necessary to stop attacks before they happen

Sulmeyer 18 (Michael Sulmeyer, Michael Sulmeyer is Director of the Cyber Security Project at the Harvard Kennedy School's Belfer Center. He previously served as Director for Plans and Operations for Cyber Policy in the Office of the Secretary of Defense, “How the U.S. Can Play Cyber-Offense: Deterrence Isn’t Enough,” https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense)-- LH

The United States has been the victim of repeated cyberattacks by foreign powers, and it seems to have little power to stop them. During the 2016 U.S. presidential campaign, Russian hackers broke into the Democratic National Committee’s e-mail servers and made more general efforts to influence the election’s outcome, as detailed in Special Counsel Robert Mueller’s indictment of 13 Russians and three Russian entities. In February, U.S. intelligence and law enforcement officials warned that the Russian government would again try to use cyber-operations to interfere with midterm elections in November. That same month, the White House publicly blamed Russia for “the most destructive and costly cyberattack in history,” the 2017 NotPetya malware campaign, which crippled the government of Ukraine before spreading to multinational corporations such as FedEx and Maersk, causing billions in damage.

The Russians are not the only ones hacking at the United States’ expense. Chinese hacking groups have stolen U.S. intellectual property from industrial manufacturers and military contractors. In 2015, China weaponized its “Great Firewall” and conducted distributed denial of service attacks against U.S. websites, including GitHub, which Beijing wished to punish for hosting content that the Chinese leadership found undesirable. In 2014, North Korean hackers attacked the U.S. film studio Sony Pictures to block the release of a movie, The Interview, that depicted the attempted assassination of North Korean leader Kim Jong Un. The attack erased the content of thousands of computers, released embarrassing internal e-mails, and intimidated Sony into canceling the movie’s theatrical release. Iran too has lashed out in cyberspace, attacking U.S. financial institutions and a dam in New York.

These threats have led to renewed calls for cyber-deterrence measures that would impose greater costs on would-be hackers while denying them benefits. The administration of President Donald Trump, for instance, has elevated U.S. Cyber Command to a unified combatant command, which it believes will signal greater capability and resolve. Deterrence is also likely behind the Trump administration’s broad declaratory policy in its Nuclear Posture Review, which contemplates the use of nuclear weapons to deter non-nuclear threats. Former President Barack Obama prioritized cyber-deterrence as well, including in his administration’s 2015 Department of Defense Cyber Strategy and in his Justice Department’s efforts to indict Chinese and Iranian hackers.

This focus on cyber-deterrence is understandable but misplaced. Deterrence aims to change the calculations of adversaries by persuading them that the risks of an attack outweigh the rewards or that they will be denied the benefits they seek. But in seeking merely to deter enemies, the United States finds itself constantly on the back foot. Instead, the United States should be pursuing a more active cyberpolicy, one aimed not at deterring enemies but at disrupting their capabilities. In cyberwarfare, Washington should recognize that the best defense is a good offense.

THE PROBLEMS WITH DETERRENCE

There are three main problems with U.S. efforts at cyber-deterrence. The first is that Washington is trying to use a cold war strategy to address a twenty-first-century problem. History teaches that deterrence kept the Cold War cold: the United States and the Soviet Union were each vulnerable to the other’s thousands of nuclear weapons. When it comes to cyberspace, however, the United States has more to lose than its adversaries because it has gone further in embracing innovation and connectivity without security. But although the societies and infrastructure of Washington’s adversaries are less connected and vulnerable than those of the United States, their methods of hacking can still be disrupted.

Second, it is difficult to convince foreign leaders (and foreign hackers) that the costs of hacking really do outweigh the benefits. Deterrence is all about perception: does an actor believe that the threat of punishment is real enough to prevent him from acting? This is as much a question of psychology as one of national security strategy. Many U.S. adversaries are less vulnerable in cyberspace than the United States is, so meaningful punishment would require discerning their priorities (for instance, money or public reputation) and threatening concerted action against them. Yet gaining clarity about foreign leaders’ priorities—and credibly threatening them—is easier said than done: during the Cold War, Soviet leaders often misunderstood signals from their U.S. counterparts, as when they interpreted the NATO military exercise Able Archer 83 as a prelude to war. Not much has changed—National Security Agency Director Admiral Michael Rogers acknowledged during a recent hearing that the Russians “haven’t paid a price . . . that’s sufficient to get them to change their behavior.”

Third, it is virtually impossible to know if deterrence is working. The goal is to prevent attacks. But if no attacks occur, it is hard to determine why—perhaps the would-be attacker was deterred by the threat of punishment; perhaps the attack failed for some other reason. Washington should not base its national cyberpolicy on a strategy whose success, almost by definition, cannot be evaluated, especially if there are good alternatives available.

Today’s fight in cyberspace occurs in the gray zone between war and peace. If the United States hopes to win, it should spend less time trying to persuade its competitors that it is not worth hacking and more time preempting them and degrading their ability to do so. It is time to target capabilities, not calculations.

HACK THE HACKER

How could the United States begin degrading its opponents’ ability to hack? Washington’s actions need not always be aggressive or destructive. In countries where technology companies are willing to cooperate with the U.S. government (or with requests from their own government), a phone call to the right cloud provider or Internet service provider (ISP) could result in getting bad actors kicked off the Internet. This is not a permanent solution, but it will force adversaries to rebuild, which often prompts unforced errors, making them more vulnerable to U.S. surveillance and disruption.

If subtle measures prove insufficient, the United States should be ready to take more offensive action. In situations where the defense of the nation is on the line, U.S. hackers could pursue a campaign of erasing computers at scale, disabling accounts and credentials used by hackers to attack, and cutting off access to services so it is harder to compromise innocent systems to conduct their attacks. Such a campaign would aim to make every aspect of hacking much harder: because hackers often reuse computers, accounts, and infrastructure, targeting these would sabotage their capabilities or render them otherwise useless.

Such actions need not send a message that hacking the United States doesn’t pay. Instead, they should support a more limited but more achievable objective: stop adversaries from hacking the United States. Whether or not foreign leaders perceive that cyberattacks on the United States are worth conducting, Washington can prevent them from doing so in the first place.

Offensive cyber-operations should not be undertaken lightly—the United States must bear in mind its commitments under international law and its relationships with its allies. But excessive caution cannot prevent Washington from defending itself: with the United States’ enemies already attacking it online, the country will need to be more proactive than it has been thus far.

The U.S. government has already undertaken a few asymmetric, or non-cyber, approaches to degrading its adversaries’ abilities to hack targets in the United States. It has sanctioned foreign individuals and companies to limit their access to capital and resources. It has also indicted some hackers from China, Iran, and Russia in the hope that public exposure will make it more difficult for them to hack. These are efforts worth pursuing, but not because they deter. Rather, like offensive cyber-operations, they can degrade attackers’ capabilities, although only in indirect ways because they rely on the cooperation of foreign governments.

DEFENSE AT SCALE

Even as it seeks to upgrade its offensive cyber-capabilities, the United States should also be improving its defense. Best practices for cybersecurity, such as more secure methods to authenticate users, are increasingly well-known and easy to implement. The issue today is how to improve cyberdefenses at scale. The only way to do so is for the government to work with large technology companies to implement security enhancements for everyday Internet use. Examples include rolling out secure connections to websites, known as “https” (as opposed to the unencrypted “http”), for everyone and increasing the use of physical security tokens to improve the security of user credentials. Companies that offer these services need not force every customer to use them, but making greater security the default and allowing users to opt out rather than opt in would go a long way toward increasing protection.

Cyberdefense needs to be a priority for many sectors of the technology industry. Referring to the “private sector” as a monolith conflates the capabilities and interests of different companies. Social media companies are not ISPs, and cloud service providers are not content delivery networks. Different kinds of companies can and should offer different ways to improve the security of their clients. Doing more to prevent malware from reaching U.S. homes and businesses, through measures such as blocking attempted connections to known malicious sites, can improve cybersecurity at scale without individual users needing to take action.

Defense in cyberspace means more than just trying to keep the hackers out of networks. It also means being resilient in the face of successful cyberattacks. Resilience goes beyond backing up data. Companies must also consider how to maintain continuity of their operations (not just websites) in order to survive a cyberattack. North Korea’s destructive attack against Sony Pictures and Russia’s indiscriminate use of the NotPetya malware are harbingers of the future, and both public and private entities should be prepared.

The time for technology companies across the board to improve the security aspects of the products and services they offer is now. Larry Kramer, the president of the Hewlett Foundation, recalled how other industries handled this challenge historically: “If you go back to the early 20th century of Rockefeller and Carnegie and Ford—who made their fortunes in the industrial revolution—the titans of industry actually dedicated their funding to deal with the downsides of what they had wrought.” He continued, “We haven’t had that out of the tech industry here. These are all problems generated by their creations.” Those companies assumed accountability then for their products; today’s technology companies need to assume more accountability for theirs. Steps like these, in combination with the more muscular offensive strategy outlined above, will be far more effective than deterrence at keeping the United States safe in cyberspace.

## AT – NATO Bad

### 2AC – NATO good

NATO strength is an impact filter – extinction

Gallagher and Dueck 19 – (Mike Gallagher and Colin Dueck; "The Conservative Case for NATO"; National Review; https://www.nationalreview.com/2019/01/nato-western-military-alliance-bolsters-american-interests/; 1-30-2019, Accessed 6-25-2022)//ILake-AZ

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.

American presence in NATO is crucial to Chinese and Russian deterrence

Gallagher and Dueck 19 – (Mike Gallagher and Colin Dueck; "The Conservative Case for NATO"; National Review; https://www.nationalreview.com/2019/01/nato-western-military-alliance-bolsters-american-interests/; 1-30-2019, Accessed 6-25-2022)//ILake-AZ

Now consider the alternative. American withdrawal from NATO would be a grave error. Not only would it surrender the above advantages and undo existing progress in Europe. It would also have negative long-term implications globally pertaining to America’s foremost long-term strategic challenge: namely, the People’s Republic of China. As Beijing extends its influence worldwide, U.S. disengagement from NATO would send the signal that the United States is an unreliable friend. America’s allies and partners in the Indo-Pacific would have to rethink the integrated security architecture we have painstakingly built since Eisenhower’s day. This is not to mention the obvious and immediate tactical and operational military advantages that would accrue to Russia in Europe, shifting the balance of power against the United States.

The irony is that the Trump administration actually has a success story to tell about its policies toward NATO and Russia, particularly in Europe. Under this administration, the U.S. has provided lethal aid to Ukraine to fight off Russian-backed insurgents. It has made no concessions to Moscow regarding that conflict. It has increased sanctions against Russia and boosted America’s military presence in Eastern Europe. It has increased funding to the European Defense Initiative, bolstered U.S. defense spending, held Russia accountable for its breach of the INF (Intermediate-Range Nuclear Forces Treaty) Treaty, and explored the place of low-yield nuclear weapons as a necessary component of the American arsenal to deter Russian aggression. At the same time, the president’s calls for increased European defense spending have had some useful effects. Virtually all NATO allies have increased their levels of defense spending over the past two years. As president, Mr. Trump has regularly reiterated his support for NATO. The concomitant emphasis on allied burden-sharing is not unreasonable, as Eisenhower regularly insisted.

In keeping with its treaty powers under the U.S. Constitution, Congress should not be passive on this issue. Last week, a bipartisan group of lawmakers introduced a bill to express continuing congressional support for the NATO alliance. The bill passed by a vote of 357 to 22 in the House of Representatives. The Senate is working on similar legislation.

Public-opinion polls taken over the last three years show that a solid majority of Trump supporters, conservatives, Republicans, and Americans continue to back the NATO alliance. Conservative voters in heartland states such as Wisconsin certainly expect Europeans to do their fair share in defending themselves. But they do not oppose NATO. On the contrary, they support it.

An overarching support for America’s Western alliance has been a key component in the conservative foreign-policy approach since Eisenhower’s time. It remains relevant to this day. As conservative Republicans and other Americans consider the costs and benefits of the U.S. alliance system, recall Ike’s wise recommendation: “Now boys, let’s not make our mistakes in a hurry.”

## Impact scenarios

### China

#### Integrated NATO key to confront Chinese threats to US and European security

Odgaard 4/25 (Liselotte Odgaard, Professor at the Norwegian Institute for Defence Studies and a non-resident Senior Fellow at Hudson Institute. Her work focuses on Chinese foreign, security and defence policy, Indo-Pacific security, and the geopolitics of the Arctic region. She received her Ph.D. in Political Science from Aarhus University in Denmark. “NATO’s China Role: Defending Cyber and Outer Space,” The Washington Quarterly, 4/25/2022, <https://doi.org/10.1080/0163660X.2022.2059145>) -LH

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 cohesion over cyber necessary to confront Russia-China threat

Odgaard 4/25 (Liselotte Odgaard, Professor at the Norwegian Institute for Defence Studies and a non-resident Senior Fellow at Hudson Institute. Her work focuses on Chinese foreign, security and defence policy, Indo-Pacific security, and the geopolitics of the Arctic region. She received her Ph.D. in Political Science from Aarhus University in Denmark. “NATO’s China Role: Defending Cyber and Outer Space,” The Washington Quarterly, 4/25/2022, <https://doi.org/10.1080/0163660X.2022.2059145>) -LH

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.

Even if the balance of forces between the United States and Europe is asymmetrical, the response to Chinese and Russian threats should be joint. In a perfect world, NATO would respond as it did in 1966 when France filed for divorce: redefine the purpose of the alliance by expanding it. In 1967, the Harmel report added to the original purpose of defending member states with the management of European security writ large.21 Ideally, in 2022 a similar exercise would globalize NATO’s purpose to encompass defending the transatlantic member states against threats from China in all domains and across geographic regions.22 However, since 1967, US security interests have moved away from Europe and the post-Soviet sphere and put China and the Indo-Pacific region at the top of the US list of priorities. Washington is not likely to volunteer to spend time and resources renegotiating the fundamental political and military transatlantic relationship. If NATO took on a similar effort, it is likely to produce institutional disintegration and paralysis.23 Instead, NATO must put existing resources and mechanisms to good use to demonstrate its relevance for addressing the China threat in all domains and in the Indo-Pacific. The strategic question for NATO should not be whether, but how?

NATO cannot continue to stand by idly while its member states are redirecting their foreign and defense policies to take into account Chinese encroachments on European security without losing credibility as an adequate guarantor of transatlantic security. It is not only the US that has turned its attention toward the Indo-Pacific; NATO member states such as the UK and France, as well as the EU, are recognized as significant contributors to Indo-Pacific security efforts in the US Indo-Pacific strategy. The US encourages NATO to continue to focus on committing more attention to the Indo-Pacific, an indication that so far the alliance has been largely absent from security initiatives in the region.24 NATO invariably goes unmentioned when deterrence of China is on the security agenda of major powers. Engaging NATO in US and European naval diplomacy would allow NATO visibility on China issues, but it would also meet with insurmountable resistance from significant US partners in the Indo-Pacific, such as France and Germany. If European or US vessels and aircraft were to fly the NATO flag when participating in freedom of navigation operations in the South China Sea to counter China’s claims to historic waters and demands for prior notification of military vessels, Beijing is likely to respond in line with its current position of issuing warnings and pursuing such military vessels.25 The fact that relaxed prospective responses from Beijing seem highly plausible diagnoses the problem: NATO is no longer a cause for concern for China, who does not believe the alliance can agree on a collective transatlantic response to Beijing’s security challenges.

Although NATO visibility may be desirable, it may also not be the best place to start working on increasing the alliance’s role in getting into the game of deterrence of China. French and German resistance toward allowing NATO to play a role in the Indo-Pacific far from the European continent stems from entrapment concerns. Such resistance to the alliance’s involvement indicates that NATO has to prove capable of combining US and European views on how to deal with China threats without increasing the entrapment potential in the eyes of key European allies.

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  
Chinese-Western hybrid war is accelerated by cyber warfare – extinction

Fleming et al. 18 – (T. Casey Fleming, Chairman and Chief Executive Officer of BLACKOPS Partners Corporation, Eric L. Qualkenbush, Board of Directors of BLACKOPS Partners Corporation, and Anthony M. Chapa, Board of Directors of BLACKOPS Partners Corporation; "The New Global Competitive Model Based on Cyber and Asymmetrical Hybrid Warfare"; Army Cyber Institute / Cyber Defense Review; https://smallwarsjournal.com/jrnl/art/new-global-competitive-model-based-cyber-and-asymmetrical-hybrid-warfare; 2-5-2018, Accessed 6-25-2022)//ILake-AZ

Imagine if Pearl Harbor had been attacked and there had been no response from Washington.

This is the actual case today due to a highly sophisticated, mature, and stealth strategy perpetrated against the United States (US) by advanced nation-state military methods leveled at every sector and organization in our society. This includes private sector businesses, all government agencies, the military, and academia - every US organization operating with innovation, intellectual property, or sensitive data. The world is in significant conflict requiring the private sector, US government, and military to deliberately confront this national crisis or become permanently irrelevant. It is no longer “business as usual.”

Over the past three decades, as the US military trained in conventional, nuclear, and counterinsurgency warfare, the Chinese Communist Party (CCP) engaged and perfected over forty methods of warfare intended to permanently destabilize and weaken the US both economically and militarily. At the same time, China rapidly grew its economy and military without the required time or investment in innovation. The result is that the US is hemorrhaging its economic strength and relevance at the rate of $5 trillion in lost total value each year, or one-third of the U.S. Gross Domestic Product (GDP).

General (Ret.) Keith Alexander, former Director of the National Security Agency (NSA) and Commander of US Cyber Command, referred to China’s theft of American innovation and intellectual property as “the greatest transfer of wealth in history.”

Over time, a weakened US economy directly reduces the strength and effectiveness of the US military. Further, when a country is manipulated by an adversary to lose one-third of the value of its economy each year, it is at war. What does this mean for US citizens? A cumulative and shocking permanent reduction in quality of life to those organizations that "don't know what they don't know."

Asymmetrical Hybrid Warfare

Clear and Present Existential Threat

Over the past thirty years, the US government and private sector have advanced their policy of full-cooperation, including substantial financial and technological investment in China, under the belief that they were moving towards a more democratic, free-market society while China played intentional misdirection and deception. In 1986, month number three, the Communist Party of China (CCP) officially declared Asymmetrical Hybrid Warfare (AHW) against the US and its western allies in its nation-state Program 863. This strategy commits all of China with its strict Communist military rule to engage in any and all methods to become on par with, surpass, and dominate the West at any and all cost. China’s ultimate objective is to harvest and perpetuate the Chinese Dream through the extraction and extinguishing of the American Dream, the American way of life and ending Western dominance. The Chinese strategy is that a er 200 years of Western global dominance, it is their destiny to reverse roles with the US and to relegate it to a forced supplier with a much lower quality of life. To underscore this strategy, China refers to the last century as “the century of great humiliation.” It must also be emphasized that AHW strategy is rooted in Unrestricted Warfare or “war without rules.”

Death by a Thousand Cuts

The Modern Battlefield is Everywhere

AHW has been established as the future of modern warfare and business strategy across the globe. It is ultimate warfare that has many forms: economic warfare, transaction warfare, industrial warfare, drug warfare, and propaganda warfare, to name only a few. Each method is characterized by the non-utilization of military or conventional warfare that is typical of aircraft, ships, troops, and weapons. While China continues to aggressively develop and expand its military, it does so with the belief that if it must resort to the use of conventional or nuclear warfare, it has ultimately failed at achieving the enemy’s capitulation through the combined methods of AHW. In the business sector, AHW has become the “New Global Competitive Model” where the “winner takes all.” Soon, China will dictate transactions and pricing based on its market dominance. As businesses rush to move to “digital transformation” and “Big Data,” each must perform a 180° cybersecurity transformation based on sensitive data protection and adversarial motives as a means to survive. Currently, AHW is the primary focus of our adversaries: China is, by far, the most successful at methodically executing all AHW methods, while Russia, North Korea, Iran, and India engage in relatively few methods at present. The strategy is to continuously inflict damage or cuts to every facet of American society just below the pain threshold where we choose not to act. We believe that China has achieved an estimated 750 cuts towards “death by a thousand cuts.” (Sun Tzu)

Definition

AHW is characterized as unconventional, non-military, multi-method strategic warfare based on deception and void of any rules between countries where economic and military power, strategy and tactics differ significantly. The attacking country exploits inherent weaknesses through numerous uneven and seemingly unrelated AHW methods that are designed to destabilize the unwitting target country for ultimate and complete economic and military submission. Extensive use of misinformation and plausible deniability are used to deceive and deflect suspicion of the strategy or its methodical advancement. Hybrid warfare is a military strategy that blends conventional warfare, asymmetric warfare, irregular warfare, offset warfare, non-linear warfare, and cyber warfare. AHW is rooted in unrestricted warfare (war without rules where “everything is fair play”) which is also described as “anything warfare.” Source: BLACKOPS Partners Corporation

Culture Disparity as a Strategic Weapon

It is important to note the striking contrast between the two cultures of the US and Communist China. It is this great divide that has contributed to China’s manipulation and acceleration of AHW against the US. The CCP believes its “legalism” philosophy of supreme law and people are superior to America’s constitutional democracy underpinned by justice, religion, a Creator, and “all men are created equal.” Since 1949, the CCP have controlled all aspects of China’s commerce, military, and daily life where intellectual property is state-owned, all data is controlled, and it is the national duty of all citizens to support the regime, including all aspects of espionage. The Communist culture is further defined not by “winning vs. losing”; rather, “living vs. dying.” It is this extreme belief that underscores China’s support for AHW in its conflict with the US. Another distinction is that the CCP controls every business transaction with US companies. In many cases, the CCP resembles a powerful organized crime faction, through its shell business partnerships and facades. There is no distinction between China’s organized crime, military, or government. This places every US business partnership or transaction with China at extreme risk.

Critical Role of Intelligence

China’s uncompromising commitment to AHW demonstrates a national objective to destroy the US and its Western allies. The critical nucleus that drives the AHW strategy is the complete dependence on stolen innovation, intellectual property (IP), sensitive data, and military secrets - namely intelligence. For over thirty years, China has orchestrated the most impressive and sophisticated strategy with an intricate global network of espionage and industrial the to fuel AHW. In recent years, an emboldened China has demanded the complete surrender of all intellectual property during the process of contracting current international business transactions. Conversely, intelligence plays a critical role for the US to gauge the executional success of AHW, changes in strategy, and individual and cumulative damages.

Cyber Warfare as the Key Accelerator

China has successfully intertwined Cyber warfare as the key AHW accelerator due to its relatively minimal investment and the difficulty of attributing actions to a specific actor. At the same time, cybersecurity remains fundamentally broken in the US and the West due to failed cyber strategies, lack of awareness of AHW, lack of accountability, overconfidence, and over-dependence on inherently fallible cybersecurity products. This is made clear by the “new normal” of the increased trend in number, frequency, and resulting total damages from cyberattacks.

Current estimates place global cyber losses at $6 trillion by 2021, with expectations that this will increase further in the future, according to Cybersecurity Ventures. Cyber warfare and cybersecurity have become a “whole of society” challenge that requires a unified, elevated strategy and 180° approach to combat the morphing threat. As we examine today’s cybersecurity environment, we are looking through the wrong end of the telescope. It is only in the context of AHW that we can begin to fully understand cybersecurity’s critical role for successful defense, protection, and resolution. We have learned to treat cybersecurity first and foremost as a human problem and a senior leadership challenge, not solely an IT issue.

### !! – Space War

Effective OCOs are crucial to defending NATO’s space assets

Rodman 21 – Former Adjunct Senior Fellow within the Military, Veterans, and Society Program at the Center for a New American Security (Maj Lindsay L. Rodman; "Legal Aspects of Space: NATO Perspectives"; NATO Legal Gazette; https://www.act.nato.int/application/files/5716/4032/2170/legal\_gazette\_42.pdf; 12-2021, Accessed 6-27-2022)//ILake-AZ

Having acknowledged outer space as the newest warfighting domain, NATO doctrine helps illuminate the types of capabilities and actions that could require jus ad bellum legal analysis.44 NATO AJP 3.3(A) provides the doctrine for Joint Military Space Operations. Included among the mission areas in space are space control offensive operations and space control defensive operations. An adversary’s space capabilities can be presumed to approximate NATO’s. AJP 3.3(A) describes these as follows: Offensive Operations. Offensive space control operations deny, degrade, disrupt, destroy or deceive an adversary’s space capability or the service provided by a third-party’s space asset(s) to the adversary at a time and place of own choosing through attacks on the space nodes, terrestrial nodes, or the links that comprise a space system. These operations range from dropping ordnance on terrestrial nodes of space systems to jamming enemy satellite uplink or downlink frequencies. Offensive space control operations initiated early in a contingency can result in an immediate advantage in space capabilities and control of the space medium.

#### NATO interoperability enables effective defense of space assets. Otherwise, satellite disruptions undermine NATO operations.

Toscana and Muñoz Mosquera 21 – Borja Montes Toscano is a Legal Assistant at the Supreme Headquarters of Allied Powers Europe. Andrés Muñoz Mosquera is one of the three NATO senior legal advisors ("Legal Aspects of Space: NATO Perspectives"; NATO Legal Gazette; https://www.act.nato.int/application/files/5716/4032/2170/legal\_gazette\_42.pdf; 12-2021, Accessed 6-27-2022)//ILake-AZ

The space domain has recently become a new field full of new opportunities due to the advancements in technology. Nevertheless, vulnerabilities may arise as states and private companies exploit this domain to achieve strategic competitive advantage in different areas (e.g. weather monitoring, transport, environment and agriculture, science, communications, among others), and draw benefits out of them. These realities may pose challenges to the existing rule of law in the space domain leading to legal uncertainty and an apparent governance vacuum. In addition, possible technological disruptions (e.g. satellites’ interferences) may distort information gathered, which is essential for NATO’s operations and missions, including collective defence, crisis response and counter-terrorism.

Hence, these concerns have resulted in NATO’s new space policy, and in this way recognizing space as new operational domain two years ago.4 The 1980s and 1990s bore witness that concluding new binding agreements for outer space matters beyond the existing ones would be extremely difficult. However, the fluid legal regime for the outer space does not entail that customary international law is inapplicable.5 The crystallization of an international customary norm is a lengthy process, as is the development of treaties, and thus the introduction of a Rules-Based International Order (RBIO). Several factors within the space domain cannot be under-estimated by the Alliance such as space-based strike weapons, space support for the Alliance’s operations or dual-use material/devices.

These challenges emphasize the need to complete policy and doctrine to achieve better interoperability and resilience among Allies and contribute to forge a network of reliable soft law. NATO’s inclusion of space as the fifth operational domain represents a step forward in support of the principles of the Charter of the United Nations and on NATO’s pathos of collective self-defence and consultation, as enshrined in articles 4 (consultation) and 5 (collective defence) of the Washington Treaty. Hence, such inclusion is an additional feature of the adaptability of these provisions to armed attacks (including nonconventional tactics).6 Bearing in mind the Alliance’s institutionalized procedures and the behaviours observed over the past years in formal and informal domains, including the space domain, hybrid threats will continue proliferating at the left and the right of article 5.

#### Impact

Boucher 22 – Director of the US Army Space and Missile Defense Command’s Space and High-Altitude Research Center. (Craig Boucher; "On Space War"; Modern War Institute; https://mwi.usma.edu/on-space-war/; 1-6-2022, Accessed 6-27-2022)//ILake-AZ

Over the past few years, there has been a huge uptick in public discourse about the “militarization of space”—a phrase that may sound concerning, but it is also nothing new. Much of this discussion has been driven by the founding of the United States Space Force and reestablishment of the United States Space Command. Regardless of how these moves may look to some, as someone who was a party to the discussions surrounding these decisions, I can confidently say that they were not taken lightly, nor were they aimed at establishing the United States as the aggressor in the space domain. The United States did recently formally recognize space as a new warfighting domain, but in order to understand why this happened it is necessary to examine the history of warfare and human activity in the space domain.

The Theory of War

As Clausewitz would remind us, “War is merely the continuation of policy by other means.” Simply put, war is an extension of politics. When political leaders cannot achieve their objectives through peaceful means, they turn to war as a means to a policy end. James Carafano describes how this plays out across the various domains:

War is a competition between adversaries, a contest of action and counteraction that concludes or changes based on the agency of competitors, and this competition unfolds in the domains accessible to each competitor: land, sea, air, space, and cyberspace. Dominating in war is not about dominating a domain. It is about dominating an enemy.

As technology has evolved over time, so too has our reach into new domains—the surface and subsurface of the seas, the air, and now space and cyberspace. In war, the goal is to force the enemy to accept terms that favor the victor. As Clausewitz puts it, “War is thus an act of force to compel our enemy to do our will”—and advancements in technology have opened up new domains, like space and cyber, to enable us to achieve those aims.

Smart practitioners of warfare seek to achieve victory by attacking their enemy’s perceived weaknesses. As Sun Tzu stated: “So in war, the way is to avoid what is strong and to strike at what is weak.” Clausewitz later introduced the concept of centers of gravity, which are the moral or physical strength of the combatants. Rather than directly attacking this strength, as Dr. Joe Strange and Colonel Richard Iron note, “experienced practitioners of the operational art aim to identify the enemy’s center of gravity and its critical vulnerabilities, then concentrate superior combat power to exploit those critical vulnerabilities, thereby forcing the enemy’s culmination and so achieve decisive success.”

As we look to space and cyber as newly recognized domains of warfare, we must remember these concepts apply to all human conflicts. War is a contest of wills between human competitors, and historically these contests take place wherever humans operate and interact.

The History of the Space Domain

Our modern space capabilities resulted from the evolution of Cold War–era technology and the “space race.” Given the devastating effects of nuclear weapons at the end of World War II and the development of those weapons by both the United States and the Soviet Union as the two remaining superpowers at the end of the war, a competition for technological superiority took shape between the two nations. Out of this competition several arms races resulted to include both a nuclear one and, closely behind, one in space. Enabled by captured German scientists, like Wernher von Braun in the United States, the development of each nation’s rocket technology and, eventually, intercontinental ballistic missiles—which allowed nuclear weapons to be delivered over great distances with little warning—increased the mistrust between the two nations. These technologies not only shaped the Cold War, but were also essential to the development of each nation’s space program. After all, the technology required to place a warhead with precision halfway around the world is foundational to the space program as well, since both cases require rockets to achieve similar altitudes and velocities.

When President Dwight D. Eisenhower developed the United States’ first space policy, he prioritized intelligence gathering to see into the Soviet Union. While this was perhaps initially driven by the “Pearl Harbor mentality” that resulted from senior leaders having experienced the strategic surprise that brought the United States into World War II, this need for intelligence was later underscored when Gary Powers’s U-2 spy plane was shot down—and our ability to monitor the Soviet Union’s nuclear weapons program effectively ended. After the Soviet Union launched its Sputnik satellite and established the first space norm of free overflight in outer space, the United States launched the CORONA program.

In addition to the development of intelligence capabilities, as the United States and Soviet Union competed in the space domain, both nations also attempted to build several space weapon systems. In the 1960s, the United States conducted the first high-altitude nuclear detonation test, Starfish Prime, and the Soviet Union’s fractional orbital bombardment system sought to enable on-orbit nuclear bombing—a concept that China’s recent hypersonic test may be bringing closer to reality. Later, the Soviet Union tested an orbiting aircraft cannon onboard the Salyut-3 space station and the United States experimented with on-orbit missile defense with its Brilliant Pebbles system and launched its first direct-ascent anti-satellite weapon system, the F-15’s ASM-135. Eventually, other countries would build up their space capabilities and follow suit, as China did when it tested an anti-satellite missile by destroying its Fengyun-1C satellite in 2007. While the Outer Space Treaty of 1967 sought to limit the development of these orbital weapon systems, it only specifically bans nations from placing weapons of mass destruction on orbit.

In 1998, the Rumsfeld Commission warned of a “Space Pearl Harbor” and that attacks on the US space infrastructure would be likely during a conflict scenario. In 2015 and 2016, US Strategic Command established the National Space Defense Center (which was then known as the Joint Interagency Combined Space Operations Center), under direction from Deputy Secretary of Defense Robert Work to defend our space architecture. In 2019 came the two moves that garnered the widest attention. First, DoD reestablished US Space Command, reflecting the fact that space had already become a warfighting domain, and that we needed a combatant commander supported by all the services to protect our assets in space. Second, in December 2019, the United States Space Force was established as a separate service under the United States Air Force in recognition of the importance of space as a warfighting domain similar to the land, maritime, and air domains. While at the time, the headlines may have made these moves seem aggressive, they must be viewed through the decades of historical context that preceded them.

The Larger Context

Simply put, the United States has excelled in modern warfare as a direct result of our ability to leverage our space assets as combat multipliers. During Operation Desert Storm, we were effectively able to navigate through open desert thanks to the advent of the Global Positioning System (GPS)—which was not even a fully operational constellation at the time. Later, during Operation Iraqi Freedom we demonstrated how much further we had advanced as we were able to communicate over vast distances and strike targets leveraging precision-guided munitions that were GPS enabled.

As American military forces demonstrated dominance on the modern battlefield, adversaries took note and developed capabilities to take those advantages away and level the playing field. The 2021 Space Threat Assessment provides an overview of the categories of kinetic and nonkinetic weapons being developed globally to reduce that advantage. Because of the nature of warfare, and our demonstrated success on the terrestrial battlefields, our adversaries continue the growth and advancement of these weapon systems.

Given this uncertain world, with persistent and evolving threats from Iran and North Korea and the renewal of great power competition among the United States, Russia, and China, we as a nation must account for the fact that our reliance on space, while in many ways a combat multiplier, may also be perceived as a vulnerability. As we further analyze our adversaries’ objectives, we must be cognizant of those they may be willing to accomplish through force if they are unable to achieve them through peaceful means. We must also account for weapon systems that can be used to create effects to and from each of the domains in which humans operate—including space.

Returning to Clausewitz, however, generating effects (such as the destruction of personnel and equipment) is not the end goal for warfare; it is to achieve political objectives. The effects our enemies choose to create, and where they choose to produce them, are designed to help them efficiently achieve their wartime objectives. Striking the United States where we appear to be weak, in any domain, is a natural element of warfare that we must be prepared for.

Each time humans have ventured off land, first into the sea and later into the air, we’ve brought conflict with us and leveraged those domains to achieve victory. Warfare extends into all domains where humans operate, because war is a contest of wills to achieve policy objectives by force when peaceful methods are no longer considered to be a reasonable means to a political end. Space is no exception, and it began taking shape as a warfighting domain even before humans first managed to reach it.

It is just now getting the recognition it has been lacking in the past due to the recent successful demonstration of destructive space technologies that have been in development from the very beginning of our foray into the space domain. Given that recognition, we must prepare to defend our vital national interests in this domain and develop our thinking and communication about warfare as it applies to space. That begins with the fundamental principles that define warfare in all domains and an understanding of the history behind space as warfighting domain.

### !! – Iran

Cohesion of NATO deters Iran – Otherwise, NATO-Iran conflict goes nuclear

Black and Lynch 21 – James Black is a research leader on Defence, Security and Infrastructure for RAND Europe, Alice Lynch is a Former Security and Defence Analyst for RAND Europe ("Cyber Threats to NATO from a Multi-Domain Perspective"; NATO CCD COE; https://ccdcoe.org/uploads/2020/12/7-Cyber\_Threats\_NATO\_Multidomain\_Perspective\_ebook.pdf; 1/12/2021, Accessed 6-28-2022)//ILake-AZ

3) OtherPotential Adversaries

While their concepts and capabilities are less well-developed, smaller nations such as Iran and the DPRK are also investing heavily in cyberspace and exploring the effects on other domains. There is limited evidence of explicit multi-domain thinking within the current doctrine or activities of either country; however, both are seeking to enhance the use of cyber capabilities within their own joint operations. Iran’s concepts of ‘Retaliatory Deterrence’ and ‘Mosaic Warfare’ increasingly seek to exploit the cyber domain and encourage more deeply integrated joint operations, primarily aimed at deterring US-led intervention. Capitalising on opportunities presented by new technologies, Teheran is investing in cyber forces and capabilities to extend the reach of its deterrence strategy in conjunction with long-range ballistic and cruise missiles (McInnis, 2017; DIA, 2019). The DPRK is also pursuing an apparent shift towards warfighting beyond the traditional domains, viewing cross-domain integration and coordination of effects as a ‘force multiplier’ (Paul et al., 2018). This includes leveraging cyberspace and the EMS to defeat a militarily superior adversary by targeting vulnerabilities or dependencies within C2 networks to undermine cohesion within or between allied adversaries and erode their will to fight (Paul et al., 2018; Tasic, 2019).

3. IMPLICATIONS FOR NATO

Ongoing initiatives by Allies and adversaries alike emphasise the need to consider future threats in cyberspace and the EMS not in isolation but rather in terms of convergence with operations and vulnerabilities in other domains. At the Alliance level, these complex interlinkages present both opportunities and challenges for NATO. Novel technologies and concepts associated with cyberspace, space and information operations or activities in the EMS potentially offer new ways and means to understand, influence, deter and ultimately defeat adversaries through MDO. There are, however, considerable gaps between future ambitions and present realities. Addressing known shortfalls in cyber capabilities and MDO at the national level represents a significant, long-term and resource-intensive challenge. Integrating and cohering initiatives across an Alliance of 30 nations only increases the complexity of transformation ‘exponentially’ (Sharpy, 2020).

To address growing external threats posed by adversaries employing cyber-attacks as part of cross-domain manoeuvre, NATO must first understand its internal barriers, limitations and vulnerabilities regarding MDO. Only then can Allies agree a common approach to developing the future concepts, policies and permissions, C2, capabilities and innovation ecosystem required to compete in such a contested operational environment. The following sections address each of these themes in turn.

A. Conceptual Difficulties

NATO’s challenges start with language (Heren, 2020; Reilly, 2020). There is no single definition of MDO employed consistently across the US services, let alone NATO (Donnelly & Farley, 2019; Smagh, 2020). According to Jeff Reilly of the US Air Command and Staff College, the ongoing revolution in the technology and threat environment ‘mandates a greater investment of intellectual energy in the concept before it will be accepted by the military and defence communities within NATO’ (Reilly, 2020: p. 2). This includes wargaming, modelling and simulation and experimentation to socialise, stress-test and refine MDO concepts (Zadalis, 2018).

Though arguably most mature in its thinking, the US is still working to build a common understanding of domains and of MDO, including why it is necessary, how it is novel or different from joint operations, and how to translate it into practice; including through a new Joint Warfighting Concept and related initiatives such as Joint All-Domain Command and Control (JADC2) capabilities (Grispen-Gelens, 2020). NATO remains even earlier in development: explicit MDO terminology such as convergence is largely absent from NATO doctrine, and has only recently begun featuring in national documents among European Allies such as France, Norway and the UK (Watling & Roper, 2019).

Whether ‘multi-domain’ is an enduring concept or simply the latest ‘buzzword’ in military thinking also remains to be seen. If the latter, there is a chance that US thinking may shift away from MDO before NATO has even begun to fully mature its own concept (Spirtas, 2018). As with many buzzwords, there is potential for conceptual confusion or for misappropriation of the latest fashionable concept to provide political and intellectual cover for enduring competition among individual service branches for new funding and responsibilities in emerging domains such as cyberspace and space (Grest & Heren, 2019).

NATO is evolving its understanding of multi-domain synergies while doctrine, policies, plans, C2 structures and capabilities for the cyber and space domains remain immature. The Allies approved a high-level Military Vision and Strategy on Cyberspace as a Domain of Operations in June 2018 (NATO, 2020b) and NATO only recently published the first edition of AJP- 3.20 Allied Joint Doctrine for Cyberspace Operations covering cyberspace operations in January 2020. Reservations lodged by Allies include US concerns about how NATO defines and understands domains and the information environment (NATO, 2020c). NATO is also busy operationalising the Military Strategy adopted in 2019, implementing readiness initiatives, developing theatre-wide strategies, and graduated response plans, and working up both the NWCC and a new Concept for the Deterrence and Defence of the Euro-Atlantic Area (NATO, 2019a; NATO, 2020f). With so many competing priorities already on the Alliance’s agenda, finding the political, institutional and intellectual bandwidth needed to agree a common lexicon and concept of MDO—and cyberspace’s role therein—is a challenge.

NATO faces another difficulty not shared by adversaries. While Russia and China can focus conceptual, force and capability development efforts on a specific foe (the US and NATO) and region (their near abroad), NATO must plan and prepare for wide-reaching scenarios. A multi-domain concept and set of forces configured to address Russia in northern and eastern Europe might be ill-suited to operating in the Mediterranean, countering Iran in the Gulf, or deterring China in the Indo-Pacific. One potential risk is a divergence between US efforts to design MDO and JADC2 networks primarily to address China and any NATO system-of-systems for MDO oriented towards Russia (Grispen-Gelens, 2020).

B. Policy Tensions

Policy differences exacerbate conceptual ones. Allies differ in their policy and legal constraints, strategic cultures, threat perception, resources, planning and budgetary cycles and forces (Sondhaus, 2006). While solidarity ultimately remains NATO’s strongest asset, these differences create seams that adversaries can exploit. This is especially so with cyberspace, where there is more sensitivity and less commonality to emerging national approaches than in more established domains, and to MDO, which is inherently predicated on integration and interoperability (Sharpy, 2020).

Information sharing is especially problematic for the cyber dimension of MDO, with Allies reticent to share details of their capabilities across NATO given security concerns and political sensitivities. The issue of permissions is also a ‘significant challenge in the development of cyber capabilities’, especially where reconnaissance on Allied soil and networks is required to detect hostile cyber activity (Watling & Roper, 2019). Nations also have differing policy, legal and ethical stances on key technologies on which MDO relies. This includes the use of offensive cyber capabilities or basing of hypersonic missiles or longrange penetrating fires in Europe, which some fear could be destabilising and escalatory (Quintin & Vanholme, 2020). NATO similarly lacks a common approach to governance and use of AI, autonomy and automation, all envisaged as essential enablers for JADC2 (Williams, 2020). This affects the levels of autonomy (with the human in, on or out of the loop) used for sensor data fusion and decision-making, or to deliver effects using uncrewed platforms, automated cyber systems and human-machine teaming (Scharre, 2018).

In considering cooperation and burden-sharing, Allies face several dilemmas depending on their ambitions and resources for both cyberspace and MDO. The US must overcome domestic inter-service rivalries and decide how to integrate partners, including whether it can accept a multinational vision of MDO that is not imposed on smaller allies—or excludes them entirely, at NATO’s expense—but rather is genuinely collaborative (Watling & Roper, 2019). Larger European nations face the dilemma of whether to buy into a US-led architecture and system-of-systems with implications for freedom of action, data-sharing and procurement choices, or shoulder the costs of sovereign or multinational alternatives.11 They also face choices over how best to contribute to multinational MDO: whether to aspire to full-spectrum capabilities to allow sovereign action and offer redundancy to Allies’ capabilities or to specialise in certain domains (e.g. cyber) to offer niche capability and buy leverage with the US and NATO by making themselves indispensable. Smaller nations must decide how to influence larger Allies and NATO, and what to do if they lack cyber capabilities (or others deemed central to MDO, e.g. long-range fires) or their forces are too small to operate or gain MDO experience at echelons above brigade (Watling & Roper, 2019).

The economic fallout of COVID-19 also raises renewed questions about affordability and the extent to which Allies are willing and able to invest in new cyber capabilities—though some may see these as cost-efficient alternatives to land, air or maritime forces—and how they time investments in ambitious transformation programmes such as MDO (Clark, 2020). Timing presents both threats and opportunities from a cyber perspective. Rapid, hasty transformation risks undermining NATO cohesion and interoperability or creating vulnerabilities in JADC2 systems with immature cyber defences (Donaldson & Sciarini, 2019b). Conversely, overly cautious change risks ceding ground to adversaries such as Russia and China which are investing heavily in asymmetric means, including offensive cyber capabilities, to gain an information advantage over NATO (Kilcullen, 2020).

The most likely outcome may be a variegated approach, with some Allies (including the US) taking the lead on conceptual and capability development for MDO, creating national or mini-lateral networks for JADC2, and then building up a looser degree of interoperability at NATO level (Watling & Roper, 2019).

C. Capability and Force Development Priorities

Assuming NATO can overcome conceptual and policy hurdles, significant effort will still be required to develop the necessary forces and capabilities across all domains, but perhaps especially for cyberspace.

Operationalising MDO demands a ‘calibrated force posture’ with multi-domain formations strategically positioned, held at readiness and able to de ploy over large distances, trained and equipped to operate across multiple contested domains (Grispen-Gelens, 2020). The vision is for different sensors and shooters to share and fuse data, build a common operating picture, inform rapid decision-making and deliver effects at a time and place of the commander’s choosing and to do so agnostic of domains, nation, service or platform (Niewood, Grant & Lewis, 2019). Forces must operate at pace and against an adversary contesting all domains. This tempo necessitates moving beyond NATO’s past focus on synchronisation of pre-planned effects in individual domains towards more agile targeting and more resilience against hostile attempts at ‘disorganisation’ or ‘systems attack’ (Thomas, 2019; Engstrom, 2018).

Linking all this together demands novel approaches to C4ISR, as reflected in investments in JADC2 (Harrigian, 2020). This US initiative leverages advances in information and communication technologies such as mesh networks, cloud and edge computing, open architectures, data analytics, AI and machine learning, autonomy and automation, software-defined systems, robotics, satellite communications and sophisticated cyber and EMS capabilities (Hitchens, 2019). Future JADC2 networks must be secure, robust, resilient, agile and more decentralised, with enough bandwidth to share data in a timely and secure manner despite cyber attacks, jamming, spoofing or physical destruction of communication nodes (Goldfein, 2017). Trust is also essential, handling data from different sources and at multiple security levels without making controls so arduous that users and devices cannot access the network (Donaldson & Sciarini, 2019a).

Reliance on connectivity makes cyberspace, space and the EMS the ‘centre of gravity’ for MDO (Hess et al., 2019). JADC2 introduces obvious challenges from a cyber threat perspective, both in terms of the attack surface for different threat vectors and the cascading effects from hostile cyber activity—though, of course, existing centralised C2 hubs also have their own vulnerabilities to cyber or physical attack (Hess et al., 2019). Improved cyber capabilities are not only needed to secure and enable operations in other domains (Reilly, 2020). Investments by Russia and China to contest cyberspace and the EMS may also limit the ability of NATO commanders to employ offensive cyber capabilities at a time and place that will ‘converge’ with effects through other domains. Securing networks against disruption is critical at the operational and strategic levels given requirements for reach-back to headquarters, especially constraining organisations responsible for delivering offensive cyber effects, since these are likely to be physically located in the homeland (Watling & Roper, 2019; Nettis, 2020)

Impact ??/iran has intent to go to war w nato

Jordet 12 – (Nils Jordet; "Explaining the Long-term Hostility between the United States and Iran: A Historical, Theoretical and Methodological Framework"; No Publication; https://www.nato.int/acad/fellow/98-00/jordet.pdf; 11-22-2012, Accessed 6-27-2022)//ILake-AZ

Iran fiercely opposes several of NATO’s current long-term objectives. The Iranian theocracy promotes a system of governance that fundamentally contradicts the core interests and values upon which the NATO alliance was founded. This is particularly true in the realm of basic human rights, such as the systematic use of torture and executions, freedom of speech and freedom of religion, and more generally the adherence to the principles of peaceful coexistence in the international system. In fact, Iran is perhaps second only to Russia in the threat it poses to the to the long-term objectives of the NATO alliance. It is therefore not surprising that there have been a warming of ties between these two historical enemies in the 1990s. If NATO wants to continue to be successful in its second fifty years, it must seek to influence and accommodate Tehran.

Iran will continue to challenge core NATO objectives in the future for several important reasons. First, it is clearly in the interest of the NATO alliance to reach a comprehensive peace settlement between Israel and its Arab neighbors. Iran has made no secret of its strong opposition to the U.S.-sponsored Middle East Peace Process. Since the Iranian Revolution in 1978-79, Iran has actively sought to obstruct any accommodation by the Muslim World of the State of Israel, which it perceives as a continuation of the painful legacy of Western imperialism.

Second, Iran is the only remaining nation with a common border with a NATO that has explicitly and repeatedly declared its hostile intentions against at least one of members of the alliance. During the Cold War, Norway and Turkey were the only two members of the alliance with a shared physical border with the Soviet Union. While the commitment to defend the northern NATO flank in North Norway was a symbolic goal rather than a militarily realistic objective against the largest military complex in the world at that time on the Kola Peninsula. Yet, it sent a powerful message that the alliance was committed to defending its territory. The most realistic territorial threat against NATO in the future will come from Turkey’s eastern neighbors. With the possible integration of Turkey into the European Union, the Kurdish problem in the east will most likely become a more serious source of instability than in the past since the traditional harsh methods of suppression will not be available to the central Turkish government. In addition, the ongoing dispute over access to scarce water resources — now predominantly controlled by Turkey — will become increasingly contentious as the regional consumption of water is dramatically increased due to extreme high rates of population growth, rapid urbanization, and improved standards of living. Water scarcity issues suggest that by the year 2010, NATO will now have to make a commitment to stabilize its southeastern flank against external pressure. Iran has tremendous leverage over any lasting settlement of ties between Turkey and the larger NATO alliance, and states in the Middle East and Central Asia. In short, it is clearly in NATO’s interest to reach a comprehensive and lasting accommodation with the government in Tehran over transborder issues involving Turkey.

Third, Iran is one of the key players in an emerging regional and international nuclear arms race, not so much for its capabilities as for its perceived hostile intentions. Publicly, the United States quotes missile attack from “rogue states,” such as Iran and North Korea, as the justification for developing and deploying a missile defense system. However, many analysts believe that the system is intended to counter the missile threat from China since Iran’s and North Korea’s overall offensive capabilities are disproportionate to the planned U.S. defensive capacity. Moreover, many analysts believe that such a system will have the unintended effect of provoking a large-scale missile build-up. The real question is not whether Iran has the intention or technical will to acquire nuclear weapons or not; it is which strategic variables factor into the Iranian regime’s threat-response and cost-benefit analyses. It has surely not escaped the decision-makers in Tehran that deployment of nuclear missiles will almost certainly trigger a regional and international arms race. If NATO intends to prevent a serious build-up of weapons of mass destruction capabilities on its southeastern border, it must influence Iran’s ever more rational decision-makers by acknowledging Iran’s legitimate security concerns.

Fourth, the conflict with Iran will in the future test the internal unity of NATO. The United States perceives the conflicts in the Middle East in the context of terrorism, weapons of mass destruction, and the flow of oil to the world market. The European Union is increasingly concerned with the influx of refugees from the Middle East and North Africa to Western Europe. Illegal immigration is challenging the core values of all liberal democracies in the Europe. Over the last two decades, the far right in nearly every European country has seen a tremendous increase in support by exploiting dark xenophobic undercurrents in the population at large. Newly arrived immigrants in Western Europe have not assimilated over time in the same way as massive immigration has in the United States. European politicians increasingly see illegal immigration as a serious challenge to the social fabric of Europe, and there is building consensus that future immigration must be seriously curtailed. Iran is a vital important player in Europe’s immigration woes. Iran has for many years given shelter to the largest refugee population in the world, and has the power to control several regional conflicts that can create massive refugee problems, which will eventually spill over to Europe. Rather than deal solely at home with the difficult issues surrounding immigration, Europe and the NATO alliance will be forced to deal with political and economic conditions which give rise to immigration at the source. Iran’s partnership in this process will be critical to its success.

Finally, Iran has for a long time been the most effective barrier against drug trafficking from Afghanistan and Pakistan. Governments in most countries in the West now list the threat from international organized crime as a threat to national security. A change in policy within Iran would effectively undermine the effort to stop the flow of narcotics to the markets in Western Europe.

For the above reasons, and due to the fact that differences between U.S. and European approaches to dealing with the Iranian clergy have a potential to weaken the NATO alliance, overcoming long-term hostility between Washington and Tehran is a central component in NATO’s future. Yet, the true nature of U.S.-Iranian hostility remains elusive and poorly understood. The following sections outline the problem. The paper is divided into five sections. Section II defines long-term hostility by describing the contemporary and historical background for the conflict and by distinguishing between different categories of the phenomenon. Section III evaluates alternative approaches for explaining long-term hostility. Section IV looks at how improvements in research methodology will yield more reliable and valid findings. Finally, I propose in Section V a different contextual approach for understanding the conflict.

Iran war goes nuclear

Hussain 21 – (Murtaza Hussain; "The Iran War That Obama Tried to Avoid Is Now Around the Corner"; Intercept; https://theintercept.com/2021/12/07/iran-war-nuclear-weapons-biden-trump/; 12-7-2021, Accessed 6-28-2022)//ILake-AZ

THE UNITED STATES is going to war with Iran.

That conclusion seems unavoidable watching President Joe Biden fail to revive the Iran nuclear deal from which the Trump administration unilaterally withdrew in 2018. The Iranian side has demanded the removal of sanctions imposed by former President Donald Trump, as well as a guarantee that a future U.S. administration will not once again abruptly pull out of the nuclear deal, which is known as the JCPOA. While Iran has continued to abide by the minimum terms of the deal in order to preserve the possibility of bringing it back to life, Biden’s unwillingness or inability to meet its terms has left observers now warning of a “worst-case” scenario in which Iran proceeds to weaponize its nuclear program and the two countries come to a full-blown armed conflict.

It is worth reflecting on how both sides came to this point. The nuclear deal negotiated by the Obama administration was a means of averting war by placing Iran’s nuclear program under international monitoring in exchange for economic integration with the West. That agreement was abruptly torn up by Trump, seemingly in a fit of personal pique at President Barack Obama, with the encouragement of hawkish advisers and former Israeli Prime Minister Benjamin Netanyahu. In place of a diplomatic arrangement, the Trump administration waged a campaign of economic pressure, sabotage, and assassinations targeting Iranian leadership.

Those efforts did great harm to innocent Iranians as well as to U.S. diplomatic standing. They have not done what the diplomatic agreement did: actually curb Iran’s nuclear program. Iran today remains under U.S. sanctions that have severely harmed its economy and sent its people into desperation. Its nuclear program, however, has continued to advance. The Biden administration’s failure or incapacity to do the minimum of reversing Trump’s economic sanctions has likely put an end to the old agreement. Absent the 2015 nuclear deal, the only two options left on the table are the international community accepting an Iran with nuclear weapons capability or going to war to stop it.

The truly depressing thing is that even if Biden wasn’t dragging his feet, it is unclear whether the original deal was even revivable after Trump showed that the U.S. could turn against it without notice. Western companies that had expressed an interest in investing in the Iranian market when the deal was first negotiated have been scared off, likely for good. “Even if the JCPOA was restored, no Western company would dare invest a cent in Iran, no Western bank would finance any deal in Iran with the threat of the return of US sanctions in 2025. Once was enough. The Iranians know it,” former French diplomat Gérard Araud observed in a tweet.

In addition to its unwillingness to lift the Trump-era sanctions and its inability to make executive promises that bind future administrations, the Biden administration probably lacks the majority votes it would need in the U.S. Senate to ratify the deal as a treaty. That means the odds of another rug-pulling in 2025 are high if a Republican administration comes to office. Absent the ability to guarantee the not-unreasonable demand that a signed deal be adhered to, the U.S. faces the prospect of being structurally unable to carry out the type of complex diplomacy necessary to avert war or nuclear proliferation.

Regional powers are already sending strong signals that they are preparing for a major conflict over the issue.

In recent days, top-ranking Israeli military officials have visited the headquarters of the U.S. military’s Central Command for meetings said to be about the deteriorating situation with Iran. The Israeli defense establishment has been divided in its views on the Iranian nuclear issue, with some officials contradicting the position held by Netanyahu that the deal is an unacceptable threat to Israeli security. But even Israeli officials who have said that Iran is not close to making a bomb have begun to signal that airstrikes are now on the table, particularly as it appears that the nuclear program may soon be freed of the oversight imposed by the original deal. In addition to discussing strikes against nuclear targets in Iran, Israeli news reports this week have claimed that officials are even pushing their U.S. counterparts to carry out strikes against Iranian targets elsewhere in the Middle East.

In the big picture, Iran is not completely free of blame for this predicament. Its decision to make Israel its primary villain in its public rhetoric despite the absence of any concrete territorial dispute between the two countries has mired it in a serious conflict that it may otherwise have avoided. But the fact remains that the 2015 nuclear deal, which Iranian diplomats at the time characterized as a first step toward broader conversations on areas of disagreement with the U.S., was being upheld on their side at the moment that Trump decided to tear it up and that the Biden administration has failed to reverse the steps that Trump took. The response to the question “What now?” has no easy or comforting answers.

The sclerotic nature of foreign policy debate means that if and when a major war with Iran comes, including airstrikes, naval conflict, and possible ground operations involving U.S. troops, most Americans will have forgotten the precipitating events that brought the two countries to this point, as well as the people responsible for destroying a diplomatic agreement intended to prevent bloodshed. After 20 years of conflict in the Middle East and Central Asia, Americans are clearly fatigued and eager to avoid new wars in the region. Despite how tired they may be of confrontation, their leaders seem bent on having one more — perhaps the biggest of all.

### !! – Russia

\*\* vs security – achieving consensus on threats is good, tolerating Russia increases aggression

A unified NATO is key to project credible deterrence against Russia – tolerating Russia only incites further aggression

Kolga 21 – Senior fellow at the Macdonald-Laurier Institute’s Centre for Advancing Canada’s Interests Abroad. (Marcus Kolga; "Improving NATO’s cohesion is critical to combat Russia and China’s threat: Marcus Kolga for Inside Policy"; ; https://macdonaldlaurier.ca/improving-natos-cohesion-critical-combat-russia-chinas-threat/; 10-5-2021, Accessed 6-28-2022)//ILake-AZ

Following his election victory, Prime Minister Trudeau and his new government urgently need to address the multiple security and foreign policy challenges facing Canada and our allies. These include the persistent and growing threats of foreign interference and cyber operations targeting Canada, and the danger of Russia and China’s transnational repression, human rights violations and aggression in Europe, Asia and beyond.

Of particular concern to Canada and its Northern allies is the Kremlin’s rapid militarization of the Arctic and Russia’s recent claim to all the resources under the entire Arctic Sea – right up to Canada’s 200-mile Exclusive Economic Zone. This, coupled with China’s expanding interest in the region, represents a potential future challenge to Canada’s sovereignty and mobility in the High North.

Canada’s allies on NATO’s Eastern flank continue to face various forms of aggression from Russia and Belarus, including information warfare and other forms of grey-zone hybrid aggression. Most recently, the Lukashenka regime in Belarus has weaponized thousands of innocent migrants who have been lured to Belarus from Iraq and elsewhere, and then forced to cross into Lithuania, Latvia and Poland by Belarusian authorities. The migrants are used to destabilize border regions and incite domestic political conflict.

Many of these issues were discussed during a high-level dialogue on Canadian and Baltic Sea region security and cooperation, hosted by the Macdonald-Laurier Institute. The dialogue highlighted the strengths of some of the approaches Canada has taken, lead among them being the Canadian-led NATO enhanced Forward Presence (eFP) mission in Latvia and Operation Unifier in Ukraine.

Canada’s leadership of the eFP in Latvia helps strengthen the transatlantic relationship beyond the obvious security considerations. Through it, Canada can raise its diplomatic profile and develop significant and lasting linkages between government officials, diplomats, and experts in the Baltic Sea region. Thus, when Canada faces challenging issues such as the arbitrary detention of Michael Kovrig and Michael Spavor by China, NATO members can be counted on to support us.

Most importantly, the eFP represents clear, meaningful, and targeted deterrence. It imposes significant cost if the Russian government engages in hostile action against the Baltic states or Poland. It draws a definitive red line, which if violated will result in significant consequences. However, NATO’s deterrence operations remain largely limited to conventional warfare and do not yet fully cover evolving hybrid and grey-zone threats – including information warfare and other forms of interference operations.

The Canadian Armed Forces have endeavoured to address the threat of disinformation, but those efforts have been hindered by a series of unfortunate missteps and domestic misinformation about them. Conversely, Canada’s Baltic allies have developed robust strategies to build broad social and political resilience against foreign disinformation and influence operations. Canada should be working with them and NATO to form a common strategy to deter non-linear types of warfare and aggression, which threaten our democratic processes, institutions and social cohesion.

Cautious engagement with our adversaries should remain one tool within our broader diplomatic tool kit. Yet Canada should learn from the experiences of our allies and recognize that states like Russia and China are not constrained by the same respect for transparency, democratic values, or the rule of law. The Canadian government should be aware that foreign regimes may engage in the theatre of diplomacy to distract from their true intentions and actions.

There is also concern that tolerating Russian aggression and advocating for greater engagement and integration may only further encourage bad behaviour. In the case of Nord Stream 2, for example, some NATO members have knowingly increased European dependence on Russian energy resources despite the Kremlin’s well documented use of energy as a political tool.

A united NATO is critically important to projecting credible deterrence. The erosion of domestic trust and confidence in the Alliance among its member states, including Canada, represents a threat to this cohesion. A proposal to withdraw Canada from NATO was tabled at a recent policy conference for one of Canada’s three major political parties. The proposal was defeated, but it represents a fringe anti-NATO narrative within Canada’s illiberal left; if left unaddressed, such a narrative could grow.

If countries like Russia perceive NATO as an atomized collection of states with varied priorities rather than a unified front, the Alliance is exposed to a significant risk of miscalculation in which a foreign adversary might believe they can cross a red line and only face a limited response. Thus, gaps in cohesion within the alliance directly threaten to undermine political and military deterrence. The Alliance and members states must work towards improving communications strategies to foster greater basic general understanding of NATO’s purpose, its missions and its role in protecting its members against external threats.

Similarly, if we see threats as atomized or disparate, we may lack the capacity to adequately respond. Organized GRU terrorist attacks in Czechia, the Salisbury poisonings, transnational repression and censorship, cyberwarfare, disinformation, and overt military posturing all pose threats that are aimed at the same essential goal: undermining and supplanting the power of liberal democracy and advancing authoritarianism. Through this lens, challenges posed by other actors, including China, must also be considered as part of the broader range of shared threats posed to the democratic community as a whole.

If we are to succeed in tackling these shared threats, greater transatlantic cooperation is needed. It cannot remain stagnant, however; it must evolve and expand. The serious nature of the threats, their potential to become kinetic, and the possibility of adversarial coordination (whether formal or informal) means that we must expand our tools to meet these challenges.

In the case of Ukraine, on whose border the Kremlin mobilized over 100,000 troops this past summer, the Alliance should consider extending a Membership Action Plan despite the skepticism of some allies. Ukraine must also be empowered in a similar fashion to frontline NATO states like the Baltic states and Poland. After all, the eFP mission in Latvia not only provides military deterrence, but strengthens interlinkages, develops societal resilience, and provides clear and sustained solidarity.

Finally, the growing threats of foreign interference, information warfare, cyber attacks and emerging threats to Canada’s Arctic requires a coherent long-term strategy and an evolved notion of collective defence, which includes strengthening our partnerships with non-NATO allies in Europe, Asia, and around the world.

Until we impose consequences that force Moscow and Beijing to strategically reconsider their ongoing efforts to probe the extreme boundaries of our threat tolerance, they will continue to test our capacity and political will to confront their aggression. This requires a common understanding and acknowledgement of the threats. It took Russian aggression in 2007 in Estonia, 2008 in Georgia, and the invasion of Ukraine in 2014 to achieve a basic common understanding of the threat posed by Vladimir Putin’s government. Since then, NATO’s eFP missions have thus far deterred Vladimir Putin’s neo-imperialist ambitions in the Baltic Sea region.

We must work towards achieving a similar consensus on the threats posed by Russia and China’s use of information and influence operations, as well as economic, cyber and political warfare against the community of democracies and the developing world at large in order to develop resilience and a common defence against them.

### Nuke escalation

#### Cyber deterrence failure guarantees rapid nuclear escalation

Cimbala 22 (Stephen J. Cimbala, Stephen J. Cimbala is Distinguished Professor of Political Science, Penn State Brandywine, an American Studies faculty member, “Nuclear-Crisis Management and Cyber War—A Dangerous Crossroads,” Naval War College Review, Winter 2022, <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8246&context=nwc-review)-> LH

Cyber weapons should appeal to those who prefer a nonnuclear, or even a postnuclear, military-technical arc of development. War in the digital domain offers, at least in theory, a possible means of crippling or disabling enemy assets without the need for kinetic attack, or at least while minimizing physical destruction.4 Nuclear weapons, on the other hand, are the very epitome of “mass” destruction, such that their use for deterrence—the avoidance of war by the manipulation of risk—is preferred to the actual firing of same. Unfortunately, neither nuclear deterrence nor cyber war will be able to live in a distinct policy universe for the near or distant future.

Nuclear weapons, whether held back for deterrence or fired in anger, are incorporated into systems for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). The weapons and their C4ISR systems must be protected from attacks both kinetic and digital in nature. In addition, the decision makers who must manage nuclear forces during a crisis ideally should have the best possible information about the status of their own nuclear and cyber forces and command systems, about the forces and C4ISR of possible attackers, and about the probable intentions and risk acceptance of possible opponents. In short, the task of managing a nuclear crisis demands good information and clear thinking. But the employment of cyber weapons in the early stages of a crisis could impede clear assessments by creating confusion in networks and the action channels that depend on those networks.5 The temptation to take preemptive cyber action—for example, intrusive cyber reconnaissance of commandand-control (C2) systems—might “succeed” to the point at which nuclear-crisis management becomes weaker instead of stronger. Related to this, one challenge of the second nuclear age is that conventional war is more likely to take place within a nuclear context. Paul Bracken has noted the following:

Cyber’s effect on conventional operations has barely been considered in the current nuclear debate. Cyber could cripple U.S. command and control. Space war is also overlooked. Disruptions, from cyber, ASAT [antisatellite], and hacks to our reconnaissance system[,] make good sense from the enemy point of view, to blind our reconnaissance targeting. This would turn our precision strike force into blunt carpet bombing, and likely [result in] a vast increase in collateral damage. Obviously this has political implications. It could lead to a U.S. reluctance to act. This may well be the real intent of such a move on the part of the enemy, to create a kind of nuclear digital brinkmanship that forces the United States to back off in a crisis.6

IT systems provide invaluable intelligence during a crisis, using databases, big data, visualization, geographic-information-systems mapping, artificial intelligence (AI), image recognition, and other means. If the confidentiality, integrity, or availability of these systems is doubtful, leaders will feel that they have lost control and are left groping for options.

Ironically, the downsizing of U.S. and post-Soviet Russian strategic nuclear arsenals since the end of the Cold War, while a positive development from the perspectives of nuclear arms control and nonproliferation, makes the confluence of cyber- and nuclear-attack capabilities more alarming. The overkill deployments of missiles and bombers and expansive numbers of weapons that the Cold War Americans and Soviets deployed had at least one virtue; those arsenals provided so much redundancy against first-strike vulnerability that relatively linear systems for nuclear-attack warning, C2, and responsive launch, under or after attack, sufficed. At the same time, Cold War tools for military cyber action were primitive compared with those available now. In addition, countries and their armed forces were less dependent on the fidelity of their information systems for national security. Thus, the reduction of U.S., Russian, and possibly other forces to the size of “minimum deterrents” might compromise nuclear flexibility and resilience in the face of kinetic attacks preceded or accompanied by cyber war.7 In addition, although the mathematics of minimum deterrence would shrink the size of attackers’ as well as defenders’ arsenals, defenders with smaller-size forces might have greater fears of absolute, compared with relative, losses, and therefore might be more prone to preemption-dependent strategies than defenders with larger forces would be. One of the reasons for Cold War force redundancy was that superpowers lacked confidence in the reliability or availability of some of their nuclear systems.

Offensive and defensive information warfare (infowar), as well as other cyberrelated activities, is obviously very much on the minds of U.S. military leaders and others in the American and allied national-security establishments.8 Russia also has been explicit about its cyber-related concerns. In early July 2013, President Vladimir V. Putin urged the Russian Security Council to improve state security against cyber attacks.9 Russian security expert Vladimir I. Batyuk, commenting favorably on a June 2013 U.S.-Russian agreement for the protection, control, and accounting of nuclear materials (a successor to the then recently expired NunnLugar agreement on nuclear risk reduction), warned that pledges by Presidents Putin and Barack H. Obama of cooperation on cybersecurity were even more important: “Nuclear weapons are a legacy of the 20th century. The challenge of the 21st century is cybersecurity.”10 On the other hand, arms control for cyber is apt to run into daunting security and technical issues, even assuming a successful navigation of political trust for matters as sensitive as these. Of special significance is whether cyber armscontrol negotiators can certify that hackers operating within their own states are sufficiently under control for cyber verification and transparency. There is extensive evidence that Russia, China, and other states use civilian hackers to support national goals. For example, some sources attributed Russia’s hacking into the e-mail account of the Democratic National Committee in 2016 to “Guccifer 2.0”—an homage to the original Romanian hacker using that name. Some forensic evidence supports the hypothesis that Guccifer 2.0 was run by the Russian FSB (the country’s principal security agency), with some involvement by Russian military intelligence.11 Another uncertainty is the potential role of hacktivists who routinely join in conflicts even without state sanction. If a country is in a state-versus-state crisis, then finds itself on the receiving end of an effective, widespread cyber attack that affects “the man on the street,” pressure on the government for a kinetic (i.e., military) response may become overwhelming. Technically minded, determined individuals or small groups of hacktivists now have the potential to shake the world through cyber warfare.

The cyber domain cuts across the other geostrategic domains for warfare as well: land, sea, air, and space. On the other hand, the cyber domain, compared with the others, suffers from a lack of historical perspective; it “has been created in a short time and has not had the same level of scrutiny as other battle domains,” as one author has argued.12 What this might mean for the cyber-nuclear intersection is far from obvious.

CRISIS MANAGEMENT Definitions and Parameters Crisis management, including nuclear-crisis management, is both a competitive and a cooperative endeavor between military adversaries. A crisis is, by definition, a time of great tension and uncertainty.13 Threats are in the air, and time pressure on policy makers seems intense. Each side has objectives that it wants to attain and values that it deems important to protect. During a crisis, state behaviors are especially interactive and interdependent with those of another state. It would not be too farfetched to refer to this interdependent stream of interstate crisis behaviors as a system, provided the term system is not understood as referring to something completely separate from the state or individual behaviors that make it up. The system aspect implies reciprocal causation of the crisis behaviors of A by B and vice versa.

One aspect of crisis management is this deceptively simple question: What defines a crisis as such? When does the latent capacity of the international order for violence or hostile threat assessment cross over into the terrain of actual crisis behavior? A breakdown of general deterrence in the system raises threat perceptions among various actors, but it does not guarantee that any particular relationship will deteriorate into specific deterrent or compellent threats. In defining the onset of a crisis, Patrick M. Morgan offers the useful concept of immediate deterrence failure: specific sources of hostile intent have been identified by one state with reference to another, threats have been exchanged, and responses now must be decided on.14 The passage into a crisis is equivalent to the shift from a Hobbesian world of omnipresent potential violence to the actual movement of troops and exchanges of diplomatic démarches.

All crises are characterized to some extent by a high degree of threat; a short time for decision; and a “fog of crisis”—reminiscent of Clausewitz’s “fog of war”—that confuses crisis participants about what is happening. Before modern scholars ever invented the discipline of crisis management, historians had captured the rush-to-judgment character of much crisis decision-making among great powers.15 The influence of nuclear weapons on crisis decision-making is not easy to measure or document, because the avoidance of war can be ascribed to many causes. The presence of nuclear forces obviously influences the degree of destruction that can be inflicted should crisis management fail. Short of that catastrophe, the greater interest of scholars is in how the presence of nuclear weapons might affect the decision-making process itself in a crisis. The problem is conceptually elusive; there are so many potentially important causal factors relevant to a decision on war versus peace. History is full of dependent variables in search of competing explanations.

Crisis Management: The Requirements The first requirement of successful crisis management is communications transparency. Transparency includes clear signaling and undistorted communications. Signaling refers to the requirement that each side must send its estimate of the situation to the other. It is not necessary for the two sides to have identical or even initially complementary interests, but a sufficient number of correctly sent and received signals is a prerequisite for the effective communication of goals and objectives from one side to the other. If signals are sent poorly or misunderstood, steps taken by the sender or receiver may lead to unintended consequences, including miscalculated escalation.

Communications transparency also includes high-fidelity communication between adversaries and within the respective decision-making structures of each side. High-fidelity communication in a crisis can be distorted by everything that might interfere physically, mechanically, or behaviorally with accurate transmission. Electromagnetic pulses that disrupt communication circuitry and physical destruction of communication networks are obvious examples of impediments to high-fidelity communication. Cultural differences that prevent accurate understanding of shared meanings between states can confound deterrence as practiced according to one side’s theory. As Keith B. Payne notes with regard to the potential for deterrence failure in the post–Cold War period, “Unfortunately, our expectations of opponents’ behavior frequently are unmet, not because our opponents necessarily are irrational but because we do not understand them—their individual values, goals, determination, and commitments—in the context of the engagement, and therefore we are surprised when their ‘unreasonable’ behavior differs from our expectations.”16

#### Cyberwar uniquely likely to escalate—credible deterrence is a must-have

Cimbala 22 (Stephen J. Cimbala, Stephen J. Cimbala is Distinguished Professor of Political Science, Penn State Brandywine, an American Studies faculty member, “Nuclear-Crisis Management and Cyber War—A Dangerous Crossroads,” Naval War College Review, Winter 2022, <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8246&context=nwc-review)-> LH

POTENTIAL DISRUPTERS Information or cyber warfare has the potential to attack or to disrupt successful crisis management with regard to each of the preceding attributes.24 First, infowar can muddy the signals being sent from one side to the other in a crisis. This can be done deliberately or inadvertently. Suppose one side plants a virus or worm in the other’s communications networks.25 The virus or worm becomes activated during the crisis and destroys or alters information. The missing or altered information may make it more difficult for the cyber victim to arrange a military attack; however, destroyed or altered information also may mislead either side into thinking that its signal has been interpreted correctly when it has not. Thus, side A may intend to signal “resolve” instead of “yield” to its opponent on a particular issue; side B, misperceiving what it has received as a “yield” message, may decide to continue its aggression, but then meets unexpected resistance, causing a much more dangerous situation to develop. There is also the possibility of cyber-enabled preemption to disable enemy nuclear missiles before they reach the launchpad or during the launch itself. Apparently, the United States has used such “left-of-launch” techniques against North Korea.26 During a nuclear crisis, would such a move be accepted by the attacked party as one of intimidation and deterrence or, to the contrary, would offensive cyber war against missile launches prompt a nuclear first use or first strike by the defender for fear of losing its retaliatory capability?

Infowar also can destroy or disrupt communication channels necessary for successful crisis management. One way it can do this is by disrupting communication links between policy makers and military commanders during a period of high threat and severe time pressure. Unanticipated problems, from the standpoint of civil-military relations, may arise under these conditions. For example, political leaders may have predelegated limited authority for nuclear release or launch under restrictive conditions; only when these few conditions obtain, according to the protocols of predelegation, would military commanders be authorized to employ nuclear weapons distributed within their commands.27 Clogged, destroyed, or disrupted communications could prevent top leaders from knowing that military commanders perceive a situation to be far more desperate, and thus permissive of nuclear initiative, than it really is. For example, during the Cold War, disrupted communications between the U.S. national command authority and ballistic-missile submarines, once the latter came under attack, could have resulted in a joint decision by submarine officers and crew, in the absence of contrary instructions, to launch.

Second, infowar during a crisis almost certainly will increase the time pressure under which political leaders operate. It may do this literally, or it may affect the perceived timelines within which the policy-making process yields its decisions. Once either side sees parts of its command, control, and communications (C3) system being subverted by phony information or extraneous cyber noise, its sense of panic at the possible loss of military options will be enormous. In the case of American Cold War nuclear war plans, for example, disruption of even portions of the strategic C3 system could have prevented competent execution of parts of the Single Integrated Operational Plan (SIOP), the nation’s strategic nuclear war plan. The Cold War SIOP depended on finely orchestrated time-on-target estimates and precise damage expectancies against various classes of targets.28 Partly misinformed or disinformed networks and communications centers would have led to redundant attacks against the same target sets and, quite possibly, unplanned attacks on friendly military or civilian installations. Even in the post–Cold War world of flexible nuclear-response plans, the potential slide toward preemption, on the basis of mistaken or exaggerated fears of C2 vulnerability, casts a shadow over deterrence stability. As Blair has warned, “There are no widely accepted methods for calculating command and control performance under wartime conditions, and empirical validation of such an assessment cannot be done. Compared with the tight and tidy standard calculations of force vulnerability, any objective assessment of command and control systems would raise more questions than it answered.”29

A third potentially disruptive effect of infowar on nuclear-crisis management is that it may reduce the search for available alternatives to the few and desperate. Policy makers seeking escapes from crisis denouements need flexible options and creative problem-solving. Victims of infowar may have a diminished ability to solve problems routinely, let alone creatively, once information networks are filled with flotsam and jetsam. Questions to operators will be posed poorly, and responses (if available at all) will be driven toward the least common denominator of previously programmed SOPs. Retaliatory systems that depend on launchon-warning dynamics instead of survival after riding out an attack are especially vulnerable to reduced time cycles and restricted alternatives. “A well-designed warning system cannot save commanders from misjudging the situation under the constraints of time and information imposed by a posture of launch on warning. Such a posture truncates the decision process too early for iterative estimates to converge on reality. Rapid reaction is inherently unstable because it cuts short the learning time needed to match perception with reality.”3

The propensity to search for the first available alternative that meets minimum satisfactory conditions of goal attainment is strong enough under normal conditions in nonmilitary bureaucratic organizations.31 In civil-military C2 systems under the stress of nuclear-crisis decision-making, the first available alternative quite literally may be the last—or so policy makers and their military advisers may persuade themselves. Accordingly, the bias toward prompt and adequate solutions is strong. During the Cuban missile crisis, for example, a number of members of the presidential advisory group continued to propound an air strike and invasion of Cuba during the entire thirteen days of crisis deliberation. Had less time been available for debate and had President Kennedy not deliberately structured the discussion in a way that forced alternatives to the surface, the air strike and invasion might well have been the chosen course of action.32 Paul K. Davis and coauthors have noted the following:

Usual discussions of crisis stability assume that leaders are in control of their nuclear capabilities. Again, history is sobering. President Kennedy became worried in 1961 about possible unilateral actions by military leaders to prepare a preemptive strike against the Soviet Union. He instigated efforts to tighten the President’s personal control. Soviet leadership worried about survivability of its forces and developed capability for launch on warning and automatic response. Such systems could be the source of accidental war.33

Fourth and finally on the issue of crisis management, infowar can cause flawed images of each side’s intentions and capabilities to be conveyed to the other, with potentially disastrous results. Another example from the Cuban missile crisis demonstrates the possible side effects on U.S. crisis management of simple misunderstanding and noncommunication. At the most tense period of the crisis, a U-2 reconnaissance aircraft got off course and strayed into Soviet airspace. U.S. and Soviet fighters scrambled, and a possible Arctic confrontation of air forces loomed. Khrushchev later told Kennedy that Soviet air defenses might have interpreted the U-2 flight as a prestrike reconnaissance mission or as a bomber, calling for a compensatory response by Moscow.34 Fortunately, Moscow chose to give Washington the benefit of the doubt in this instance and to permit U.S. fighters to escort the wayward U-2 back to Alaska. Why this scheduled U-2 mission was not aborted once the crisis began never has been revealed fully; the answer may be as simple as bureaucratic inertia compounded by noncommunication down the chain of command by policy makers who failed to appreciate the risk of “normal” reconnaissance under these extraordinary conditions.

The significance of the preceding discussion and examples is underscored by the assessment of expert analyst Martin C. Libicki about the relationship between cyber war and crisis management.

To generalize, a situation in which there is little pressure to respond quickly, in which a temporary disadvantage or loss is tolerable, and in which there are grounds for giving the other side some benefit of the doubt is one in which there is time for crisis management to work. Conversely, if the failure to respond quickly causes a state’s position to erode, a temporary disadvantage or degree of loss is intolerable, and there are no grounds for disputing what happened, who did it, and why—then states may conclude that they must bring matters to a head quickly.35

#### Cyber attacks on NATO allies escalate to nuclear conflict

Richard **Walker 21** (Distinguished University Professor), 6/15/21, accessed 6/24/22, “Biden-Putin Summit: Experts Warn of Cyber Nuclear Nightmare”, <https://www.dw.com/en/biden-putin-summit-experts-warn-of-cyber-nuclear-nightmare/a-57906147> (JB)

The allies signed off on a new "Comprehensive Cyber Defense Policy," affirming that, if serious enough, **a cyberattack could lead to the invocation of NATO's core Article 5**: that an attack on one member is considered an attack on all.

Recent targets have included [various parts of the US government](https://www.dw.com/en/us-expels-russian-diplomats-and-issues-sanctions-over-solarwinds-hacking-attack/a-57215141), the  [German parliament](https://www.dw.com/en/russia-backed-hackers-target-german-legislators-report/a-57018097) and election campaigning in France. Ever more corporations have been held up by ransomware, with their systems blocked in an attempt to extort money.

And these are just the attacks we know about.

One of the most serious intrusions in recent years hit Ukraine's electricity grid, cutting power to more than 200,000 people in the winter of 2015. It showed how cyberattacks could bring societies to their knees.

Kyiv and Washington [blamed the Russian government](https://www.dw.com/en/us-charges-6-russian-military-intelligence-officers-over-cyberattacks/a-55329146), with the US even singling out a member of the GRU military intelligence agency in late 2020.

"These were the first reported destructive malware attacks against the control systems of civilian critical infrastructure," said John Demers, the US assistant attorney general at the time, announcing the charges.

"No country has weaponized its cyber capabilities as maliciously and irresponsibly as Russia."

[Cyberattacks on civilian infrastructure](https://www.dw.com/en/us-states-declare-emergency-over-gas-shortage-fears-following-cyberattack/a-57501414) have triggered broad public concern, and debate on how to protect against them.

But **cyberwar could also hit the world of nuclear weapons** — an even more serious prospect. And only a small group of experts have been speaking out about this risk.

"This is an issue that is enormously important — and exceptionally difficult to discuss," said James Acton, co-director of the Nuclear Policy Program at the Carnegie Endowment for International Peace in Washington. "Because it is so heavily classified."

Acton's concerns center on cyber intrusions not against nuclear weapons themselves, but the command and control systems surrounding them. "Nuclear command and control is everything apart from the physical weapons themselves that are needed to make those weapons work," he explained.

This is perhaps the most sensitive infrastructure in the world. It's so sensitive that **the US explicitly said** in its latest "Nuclear Posture Review" that if it comes under attack, **it could respond with a nuclear strike.**

#### Nuke war could cause human extinction and destroy biosphere

**Lynas 22** British author and journalist who has written multiple books on the environment and climate change, Mark Lynas, 03/10/2022, “What Science Says: Could Humans Survive a Nuclear War Between NATO and Russia?”, <https://allianceforscience.cornell.edu/blog/2022/03/what-the-science-says-could-humans-survive-a-nuclear-war-between-nato-and-russia/> (JB)

If global nuclear famine could result from just 100 nuclear detonations, what might be the result of a fuller exchange of the several thousand warheads held in current inventories by the US and Russia?

[One 2008 study](https://doi.org/10.1063/1.3047679) looked at a Russia-US nuclear war scenario, where Russia would target 2,200 weapons on Western countries and the US would target 1,100 weapons each on China and Russia. In total, therefore, 4,400 warheads detonate, equivalent to roughly half the current inventories held each by Russia and the US.

Nuclear weapons held by other states were not used in this scenario, which has a 440-Mt explosive yield, equivalent to about 150 times all the bombs detonated in World War II. This full-scale nuclear war was estimated to cause **770 million direct deaths and generate 180 Tg of soot** from burning cities and forests. In the US, about half the population would be within 5km of a ground zero, and a fifth of the country’s citizens would be killed outright.

A [subsequent study](https://agupubs.onlinelibrary.wiley.com/doi/10.1029/2019JD030509), published in 2019, looked at a comparable but slightly lower 150 Tg atmospheric soot injection following an equivalent scale nuclear war. The devastation causes so much smoke that **only 30-40 percent of sunlight reaches the Earth’s surface for the subsequent six months**.

A massive drop in temperature follows, with the weather staying below freezing throughout the subsequent Northern Hemisphere summer. In Iowa, for example, the **model shows temperatures staying below 0°C for 730 days straight**. There is no growing season. This is a true nuclear winter.

Nor is it just a short blip. Temperatures still drop below freezing in summer for several years thereafter, and global precipitation falls by half by years three and four. It takes over a decade for anything like climatic normality to return to the planet.

By this time, most of Earth’s human population will be long dead. The **world’s food production would crash by more than 90 percent**, causing [global famine](https://doi.org/10.21203/rs.3.rs-830419/v1) that **would kill billions** by starvation. In most countries less than a quarter of the population survives by the end of year two in this scenario. Global fish stocks [are decimated](https://www.pnas.org/cgi/doi/10.1073/pnas.2008256117) and the [ozone layer collapses](https://agupubs.onlinelibrary.wiley.com/doi/10.1029/2021JD035079).

The models are [eerily specific](https://assets.researchsquare.com/files/rs-830419/v1/7c33234ad24f7e3c3e83b9ec.pdf). In the 4,400 warhead/150 Tg soot nuclear war scenario, averaged over the subsequent five years, China sees a reduction in food calories of 97.2 percent, France by 97.5 percent, Russia by 99.7 percent, the UK by 99.5 percent and the US by 98.9 percent. In all these countries, virtually **everyone who survived** the initial blasts **would** subsequently **starve**.

### democracy

#### NATO key to democracy—especially important in supporting fledgling democracies

Poast and Chinchilla 20 (Paul Poast & Alexandra Chinchilla, Paul Poast is Associate Professor in the Department of Political Science at the University of Chicago. Chinchilla is a Rosenwald Fellow in U.S. Foreign Policy and International Security and Niehaus Postdoctoral Fellow at The John Sloan Dickey Center for International Understanding at Dartmouth College. She received her Ph.D. in Political Science at the University of Chicago, “Good for democracy? Evidence from the 2004 NATO expansion,” International Politics, 04/30/2020, <https://link.springer.com/article/10.1057/s41311-020-00236-6)-> LH

In what way should one expect NATO to enhance democratic development? After all, as highlighted above, democracy is a core principle of the institution. Much of the existing work on NATO and democratic development points to several avenues of possible influence: socialization, guidance from NATO about how to create and implement reforms, NATO pressure to implement reforms, and legitimizing new democracies by helping them provide the public good of security through NATO membership. It is important to note that each of these mechanisms for how NATO could prompt reform should begin operating before full NATO membership is achieved. Once prospective members are given a promise of membership in the form of the MAP, they will be brought into close contact with NATO members and therefore exposed to the socialization mechanism. If domestic reform is a necessary condition for NATO membership, prospective members participating in the MAP should begin reforming so that they can reap the benefits of membership. Finally, if democratic reforms made to gain NATO membership persist, NATO membership should also be associated with higher levels of democracy in new member states. Below we discuss each of these means for NATO influence proposed in the literature.

First, NATO may have a subtle impact on future member states by socializing military and civilian leaders from states seeking membership to respect democratic norms. Democracy is dependent not only on the formal institutions of a country, but also on whether elites are willing to abide by democratic constraints on their power rather than undermine or dismantle them. The example of Poland’s recent democratic backsliding despite the former presence of formal democratic institutions illustrates this point. Even when democratic reforms preceded NATO involvement, NATO could still have a democratizing influence by socializing military and civilian elites to respect democratic reforms—particularly civilian control of the military. NATO created the conditions for regular, institutionalized interaction between elites from partner states and longtime member states within the institutional framework of the alliance and the Partnership for Peace (PfP), making socialization possible. NATO taught military officers and civilian defense policymakers who had served most of their professional lives under a communist system about the norms of a democracy and their role in it (Gheciu 2005b). This socialization logic outlined by Alexandra Gheciu and others is not in conflict with our argument, as we measure changes in democratic institutions rather than changes in elite attitudes. However, recent democratic backsliding in some NATO countries indicates that either the right elites were not socialized by NATO or the main effect of NATO socialization was teaching elites to value civilian control of the military and continued engagement with NATO.

Elite socialization began well before NATO membership, with collective briefings, individualized MAPs for each prospective member state, NATO-led workshops, military advisers from NATO member states, and professional education programs (Gheciu 2005b). NATO used these cooperative activities to teach the goals and norms of the alliance and assess the commitment of PfP countries to them (Gheciu 2005a). Joint military exercises, in addition to augmenting the capability aggregation of the alliance, allowed military elites from NATO states and prospective member states to interact. Military education programs—such as the NATO Defence College and programs through partner states such as the year-long International Fellows program at the US National Defense University—played a similar role in building military capability while creating space for socialization through military-to-military interactions.

Second, even when countries intended to make democratic reforms on their own initiative, they often lacked institutional knowledge about how to reform. NATO stepped in to provide assistance and advice to prospective members regarding how to enact democratic reforms. Democracy advising was provided through the NATO Parliamentary Assembly and the associated Rose-Roth seminars. According to Trine Flockhart (2004), the NATO Parliamentary Assembly and Rose-Roth seminars brought together parliamentarians from NATO and partner states to ‘familiarize legislators with key security issues and debates, to promote the development of appropriate civil–military relations, and to facilitate the sharing of expertise and experience in parliamentary practice and procedures.’ These seminars also played a ‘very important social function’ as policymakers from NATO and partner countries built professional networks with one another (Flockhart 2004). Civilian defense policymakers and military officers from NATO partner countries were also able to participate in the NATO-adjacent George C. Marshall Center, which has over 13,300 alumni. Courses at the Marshall Center include discussion of international law, democracy, rule of law, and human rights alongside more traditional security topics (Marshall Center 2019).

Third, NATO provided pressure for specific reforms through direct communication with a country’s NATO liaisons and naming and shaming countries slacking on reforms. For example, a US Congressional Research Service report released in 1995 raised concerns that Poland was not ready for NATO membership. The report stated: ‘Initiation into NATO nevertheless may hinge even more on publication of a democratic Constitution and the legal basis for civilian control. Meanwhile, the Minister of Defense and many senior officers who set policy and shape opinions have become mired in political wrangling over control of the armed forces’ (quoted in Epstein 2005, 254–285). As Rachel Epstein notes, this report was widely publicized in the Polish media with the effect of shaming Polish officials into complying, given that NATO membership was by this time an established national foreign policy goal. When the chief of the Polish General Staff, General Tadeusz Wilecki, opposed increased civilian control of the military, an unflattering New York Times article put sufficient pressure on Polish president Aleksander Kwasniewski that he removed Wilecki (Epstein 2006, 280–281).

By utilizing naming and shaming tactics and building alliances with pro-reform domestic politicians, NATO successfully shepherded a select group of partner states through enacting civilian control of the military and more internationalized defense policies (Epstein 2005). Although Poland joined NATO in the 1999 wave of enlargement, one could argue that the logic of pressure for reforms was still relevant for the countries that joined NATO in 2004. The smaller reforms of hiring personnel supportive of democratic norms and building political coalitions in support of democracy that Epstein highlights are consistent with what we find in our quantitative analysis. Some states that rapidly enacted democratic reforms after transition to democracy in the early 1990s made small improvements under NATO tutelage, even though their average democracy scores after reaching NATO applicant status and membership remained similar to what they had been before. Other NATO-induced changes, such as the firing of Wilecki in Poland, may have been crucial for continued progress even though our quantitative data do not measure them. NATO’s value, then, may be in encouraging states already democratizing to persist in maintaining democracy despite challenges from domestic elites. However, any democratizing effect of NATO would be concentrated on the premembership period, as democracy is in practice not a condition for remaining a NATO member.

Finally, NATO can assist in providing the public good of security, which can be critical for the legitimacy of some new democracies. Poast and Urpelainen (2018) argue that leaders in transitional democracies use, and often must create, international organizations to consolidate democratic rule and improve their ability to distribute public goods to the populations under their rule. Public goods are broadly defined as policies that benefit large constituencies in society. Examples of public goods include internal and external security (Loader and Walker 2007; Bueno de Mesquita et al. 1999), public infrastructure that increases investment (Henisz 2002), free and fair elections (Donno 2010), reduction of corruption (Banerjee 1997), and environmental protection (VanDeveer and Dabelko 2001). Providing such goods is critical to the survival of leaders in democratizing states. But because autocratic developing countries have little need or capacity to improve the provision of public goods (Bueno de Mesquita et al. 2003; Wintrobe 1998), democratization leaves leaders in newly democratic regimes with a unique challenge; they face high expectations for public good provision, yet their administrative apparatus has little experience providing public goods (Haggard and Kaufman 1997). Therefore, newly democratic governments can benefit from outside expertise on public goods provision, namely that offered by international organizations (IOs). IOs can assist democratizing states in the provision of public goods. IOs provide a venue through which members can pool limited resources or coordinate on policy reforms even with limited institutional capacity. IOs assist in highly technical tasks, including advising on governance capacity, monitoring elections, and facilitating learning about democratic institutions. IOs can help governments of transitional democracies govern effectively and acquire the resources to supply public goods to the newly expanded electorate.

### Hybrid war

#### Hybrid War happening now and will escalate

**Polyakova & Boulègue** (Alina Polyakova President and CEO of CEPA, Mathieu Boulègue Senior Research Fellow Russia & Eurasia Programme at Chatham House), 1/29/21, accessed 6/24/22, “THe Evolution of Russian Hybrid Warfare: Executive Summary”, <https://cepa.org/the-evolution-of-russian-hybrid-warfare-introduction/> (JB)

Russia’s military interventions in Syria, Venezuela, and, more recently, Libya raise the question whether the Kremlin is still being opportunistic or whether it has revised its military strategy to better project force around the globe based on a single playbook. These interventions have taken advantage of preexisting chaos and weakness that Russia did not directly cause. Together with its growing conventional power, Russia is now far more confident about **using hard power in the hybrid mix.**

The aforementioned changes in Russian military thinking reflect a reinvigorated confidence in the efficacy of chaos as a competitive strategy. If anything, the **Kremlin leadership feels vindicated about the usefulness of hard power options**, while categorizing nonmilitary means as a tool to prepare conflict environments and make the use of force more effective.[19](https://cepa.org/the-evolution-of-russian-hybrid-warfare-introduction/#footnote_18_7492) This is best exemplified by Kalev Stoicescu’s chapter on Estonia, where the threat of Russia’s military action cannot be dissociated from hybrid tools aimed at testing the country’s resolve below the threshold of Article V of NATO’s founding treaty, which commits the Alliance to collective defense.

Among the drivers of change in Russian thinking, disappointment and unexpected outcomes have been some of the most powerful. As Kateryna Zarembo and Sergiy Solodkyy show, this is most notably the case with low-intensity military operations in Ukraine: difficulty in upholding a degree of “plausible deniability” of direct military intervention; war fatigue; issues with managing proxy groups and local militia; the failure of “Novorossiya” and other ideological products in Ukraine;[20](https://cepa.org/the-evolution-of-russian-hybrid-warfare-introduction/#footnote_19_7492) the absence of an exit strategy in the Donbas, etc. Russia has now altered its originally ambitious aim (to control Crimea and the Donbas) in favor of perpetuating a persistent, low-scale conflict that will impede Ukraine’s integration into Western security structures.[21](https://cepa.org/the-evolution-of-russian-hybrid-warfare-introduction/#footnote_20_7492)

Further afield, in the United Kingdom, Precious Chatterje-Doody explores how **Russian hybrid operations** — mainly information operations — have been **adapting** in order **to infiltrate networks, destabilize internal norms,** and ultimately create an environment conducive to Russian interests. Oscar Jonsson outlines Russian tactical adaptations in the EU and NATO, where Russian **hybrid tools are used to increase political polarization** and challenge institutional cohesion.

Chaos strategy through hybrid, multi-vector warfare is here to stay. The consequences of this are many and unwanted, and notably include the **potential for miscalculation with the West**. To avoid such a situation, **U.S. experts and leaders can learn** much **from** the knowledge and experiences of **allies and partner states in Europe** — countries and institutions which have long been contending with the most aggressive forms of Russia’s hybrid warfare.

#### NATO key to prevent Hybrid War, but must shift methods of response

**Underwood et. al. 22** (Major Andrew Underwood, USA, is Executive Assistant to the Deputy Director for Strategy, Plans, and Policy (J5), Europe, NATO, Russia. Colonel Andrew Emery, USAF, is the Space and Missile Defense Planner in the U.S. Military Delegation to the NATO Military Committee (JCS) at NATO Headquarters, Brussels, Belgium. Lieutenant Colonel Paul Haynsworth, USA, is currently serving in the Commander’s Action Group in the NATO Special Operations Headquarters at Supreme Headquarters Allied Powers Europe, Mons, Belgium. Commander Jennifer Barnes, USN, most recently served in the Commander’s Action Group at U.S. Africa Command Headquarters in Stuttgart, Germany), 4/14/22, accessed 6/24/22, “All Quiet in the Eastern Front: NATO Civil-Military Deterrence of Russian Hybrid Warfare”, <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2999367/all-quiet-on-the-eastern-front-nato-civil-military-deterrence-of-russian-hybrid/> (JB)

As **Russia has evolved to increasingly rely on hybrid warfare** as a major component of its strategy, NATO must adapt accordingly. **NATO’s model must shift** from a reliance on traditional military deterrence and expand to incorporate political, economic, and social spheres to counter aggression below the level of armed conflict. Since NATO’s structure does not readily support innovation or active (versus passive) deterrence measures, new ideas and emphases are needed to address these challenges.

Pursuing activities to deter hybrid warfare certainly poses risks and challenges to NATO and its member states and partners. Activities in these spheres might risk further blurring lines between military and nonmilitary responsibilities. Individual member laws and EU regulations might complicate these efforts. Civil institutions could be at risk of being identified as military targets in the event of a linear war.

Consequently, **Allies and partners must update their methods** to better deter Russian aggression by reducing Russia’s strategic options and increasing their own ability to impose costs. Imposition of costs via Allies’ domains of diplomatic, information, military, and economic levers are central to changing Russia’s cost-benefit assessment regarding hybrid warfare and enabling deterrence. Doing this could be achieved through such concepts as comprehensive defense, **improved IO, and expanded allied member and partner collaboration**. While the overall goal of maintaining Alliance unity and solidarity remains the same, the means and ways through which Allies and partners achieve that goal should change. This includes embracing the diversity of members’ strengths and capabilities and exploring increased partnerships with non-NATO members to leverage and learn from their experience with Russian hybrid warfare aggression.

### EU Grid Collapse

#### Cyber-attacks on EU grid increasing

**Nelson, Romero 22** (Jonathan Nelson is the director of institutional relations at Constella Intelligence. Alejandro Romero is an ECFR council member and the chief operations officer of Constella Intelligence.), 3/7/22, accessed 6/27/22, “Why Europe’s energy industry is vulnerable to cyber-attacks”, <https://ecfr.eu/article/why-europes-energy-industry-is-vulnerable-to-cyber-attacks/> (JB)

Russia’s war on Ukraine has created widespread concern that European **energy supplies and infrastructure will come under intensifying cyber-attacks**. The Putin regime, which has long used such disruptive tactics, may retaliate against Western economic sanctions with cyber-warfare. European states and energy companies should reflect on the laundry list of such attacks that have occurred in recent years to recognise and respond to the risks they face in this area.

On 7 May 2021, the US Colonial Pipeline suffered a critical ransomware cyber-attack [resulting from a single leaked password](https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/) – the largest cyber-attack on infrastructure in US history. This prompted the authorities to declare a state of emergency in 17 US states along the east coast and in Washington, and resulted in major fuel shortages and long queues at gas stations throughout affected sectors. By early February 2022, a **slew of subsequent** [**cyber-attacks**](https://www.bbc.com/news/technology-60250956) had struck oil and gas facilities across Europe, disrupting the operations of multiple oil transport and storage companies in Germany, Belgium, and the Netherlands, and threatening production and distribution in the sector.

Such attacks are possible due to three unique vulnerabilities of the global energy ecosystem.

Firstly, this ecosystem relies on inherently complex infrastructure. **Utility companies are exposed to relatively high risks** because their networks of both physical infrastructure and cyber-infrastructure – including distributors, suppliers, storage facilities, and other assets – often overlap and are spread across many countries.

Secondly, the digital infrastructure that supports the global energy sector operates around the clock, with virtually no downtime.

Thirdly, the vulnerability of the global energy sector is **rooted in the many motivations for attacks against it**. As noted in a recent assessment by the [Canadian Centre for Cyber Security](https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-canadas-electricity-sector), these include attacks carried out by states trying to achieve geopolitical goals, by criminals attempting to extort money from desperate companies, and by activists seeking to publicise their agendas or oppose particular projects

Therefore, given the frequency with which these structures come under attack and how vital they are to the economy, **the energy sector is a key geopolitical battleground**. The vulnerabilities of Europe’s digital security and global energy interconnections could have a significant impact on citizens’ lives. The World Economic Forum [highlighted](https://www.weforum.org/whitepapers/cyber-resilience-in-the-oil-and-gas-industry-playbook-for-boards-and-corporate-officers) this in 2021, arguing that: “as one of the world’s most sophisticated and complex industries makes a multifaceted transition – from analogue to digital, from centralized to distributed and from fossil-based to low-carbon – managing cyber risk and preventing cyberthreats are quickly becoming **critical** to company value chains.”

#### France is expanding its nuclear power arsenal now

Alderman 22 (Liz Alderman is the Paris-based chief European business correspondent for The New York Times, covering economic and inequality challenges around Europe.), 2/10/22, accessed 6/28/22, “France Announces Major Nuclear Power Buildup”, <https://www.nytimes.com/2022/02/10/world/europe/france-macron-nuclear-power.html> (JB)

President Emmanuel Macron announced a major buildup of France’s huge nuclear power program on Thursday, **pledging to construct up to 14 new-generation reactors** and a fleet of smaller nuclear plants as the country seeks to slash planet-warming emissions and cut its reliance on foreign energy.

The announcement represented an about-face for Mr. Macron, who had previously pledged to reduce France’s reliance on nuclear power but has pivoted to burnishing an image as a pronuclear president battling climate change as he faces a tough re-election bid in April.

“What our country needs is the rebirth of France’s nuclear industry,” Mr. Macron said at a nuclear turbine factory in the industrial city of Belfort in eastern France as throngs of workers and political officials gathered around. “The time has come for a nuclear renaissance,” he added.

Mr. Macron’s move is seen as a pivotal moment in a growing debate over nuclear power in Europe. The divide has [taken on new dimensions](https://www.nytimes.com/2021/11/29/business/nuclear-power-europe-climate.html?searchResultPosition=1) as leaders [pledge to avert a climate catastrophe](https://www.nytimes.com/2021/07/14/world/europe/climate-change-carbon-green-new-deal.html) and grapple with an energy crisis that has sent prices for natural gas and electricity surging to record highs — in part because nuclear energy production has fallen.

Mr. Macron has been leading a coalition of like-minded countries in backing nuclear energy to speed up the push to net-zero emissions and energy independence. That has opened a rift with a group of nations led by Germany, which is wary of nuclear proliferation and [will close its last atomic power plants this year](https://www.nytimes.com/2011/05/31/world/europe/31germany.html?searchResultPosition=9), following a 2011 policy set by former Chancellor Angela Merkel after the [nuclear disaster](https://www.nytimes.com/interactive/2016/world/asia/japan-fukushima-anniversary.html?searchResultPosition=4) in Fukushima, Japan.

The French plan is aimed at cementing the country’s position as **Europe’s** [**biggest atomic power producer**](https://cnpp.iaea.org/countryprofiles/France/France.htm) and positioning Électricité de France, or EDF, the troubled state-backed operator, to compete more aggressively against Chinese and American companies in the growing global market for nuclear energy.

#### A lack of nuclear power creates a shift back to fossil-fuels

**Alderman 22** (Liz Alderman is the Paris-based chief European business correspondent for The New York Times, covering economic and inequality challenges around Europe.), 2/10/22, accessed 6/28/22, “France Announces Major Nuclear Power Buildup”, <https://www.nytimes.com/2022/02/10/world/europe/france-macron-nuclear-power.html> (JB)

Climate change and the nuclear industry’s potential role in it have become a central issue in France’s coming presidential election. Most candidates, with the exception of France’s Greens party, have said nuclear power is needed to meet climate goals.

The nuclear industry is a national priority in France, creating about 200,000 jobs directly and indirectly.

France relies on an aging fleet of 56 nuclear reactors — the most after the United States, with 93 — to generate 70 percent of its electricity and to export energy to other countries. But France has fallen from dominance as EDF, which has grappled with a series of longstanding setbacks, faces a full-blown crisis just as Europe struggles with an [energy crunch](https://www.nytimes.com/2021/12/22/business/europe-natural-gas-prices.html?searchResultPosition=2).

The company warned this week that its nuclear energy output would slump to the lowest levels since the 1990s because of problems at some sites, sending European energy prices to fresh highs. The company has temporarily closed 10 reactors, down from 17 in December, for maintenance, including to fix cracks found in pipes at some plants.

The energy shortfall has left France in the awkward position this winter of leaning more heavily on its coal-fired power stations, tapping coal-generated electricity from Germany and relying on natural gas imports as prices spike amid the conflict between [Russia](https://www.nytimes.com/2022/01/25/business/energy-environment/russia-europe-natural-gas-ukraine.html?searchResultPosition=28) and Ukraine.

#### Nuclear power plays an important role in the fight against climate change

**NEA 21** (The Nuclear Energy Agency is an intergovernmental agency that is organized under the Organisation for Economic Co-operation and Development.), 12/13/21, accessed 6/28/22, “The role of nuclear energy in mitigating climate change”, <https://www.oecd-nea.org/jcms/pl_62806/the-role-of-nuclear-energy-in-mitigating-climate-change#:~:text=Nuclear%20energy%20already%20displaces%201.6,emissions%20between%202020%20and%202050>. (JB)

One key advantage that the nuclear sector has is that it is an established industry with proven technologies and supply chains. Nuclear energy already displaces **1.6 gigatonnes of carbon dioxide emissions annually**. Through refurbishments and [long-term operation of existing reactors](https://www.oecd-nea.org/jcms/pl_60310), the nuclear sector can continue displacing carbon dioxide for decades to come: up to 50 gigatonnes of cumulative carbon emissions between 2020 and 2050.

There is also significant potential for new builds of large-scale nuclear energy reactors, which could displace 23 gigatonnes of emissions between 2020 and 2050 by replacing fossil power generation. This includes replacing coal power, which is among the most intensive emitters of carbon dioxide but is particularly widespread in developing countries, where demand for energy is forecast to grow quickly as more parts of their economies link up to the electricity grid. Currently, non-OECD countries China and India account for the biggest shares of such new projects.

As a key pillar of global decarbonisation strategies, nuclear energy would also save money: meeting the Paris targets without nuclear energy would cost the world an estimated USD 1.6 trillion more, [according to the International Energy Agency](https://www.iea.org/reports/nuclear-power-in-a-clean-energy-system).

But the nuclear sector can also play a much larger role. As countries ramp up other types of carbon-free energy production, such as solar or wind, nuclear power can serve as baseload that backs up renewables and [guarantees electricity supply](https://www.oecd-nea.org/jcms/pl_34670) is constant, reliable and dispatchable. The importance of this has become obvious from the recent experience of some countries that have suffered power outages or surges in energy prices. Where nuclear facilities are being phased out, governments have had to resort to restarting fossil fuel-powered plants—including coal—to ensure a constant electricity supply, taking a direct step backwards in the fight to reduce carbon emissions and pollution.

#### Major grid collapse spills over to other industries, impacting the world as a whole

**Gray 19** (Editor Richard Gray leads BBC Future's editorial and commercial strategy), 8/24/19, accessed 6/28/22, “ What Would Happen in an Apocalyptic Blackout”, <https://www.bbc.com/future/article/20191023-what-would-happen-in-an-apocalyptic-blackout> (JB)

She is right. While the term “black sky” events illustrates perhaps the most visible impact of widespread power failures, it fails to convey the scale of the impact these can have. In our modern world, **almost everything**, from our financial systems to our communication networks, are **utterly reliant upon electricity**. Other critical infrastructure like water supplies and our sewer systems rely upon electric powered pumps to keep them running. With no power, fuel pumps at petrol stations stop working, road signs, traffic lights and train systems go dead. Transport networks grind to a halt.

Our complex food supply chains quickly fall apart without computers to coordinate where produce needs to be, or the fuel to transport it or refrigeration to preserve it. Air conditioning, gas boilers and heating systems also rely upon electricity to work.

A little over 100 years ago, our cities ran on human and animal muscle power to ferry goods and waste around. Modern infrastructure is now utterly reliant upon electricity.

“In today’s world, our systems are highly interdependent and it is very hard to find many systems that are not fundamentally reliant upon power,” says Mian. “**A black sky scenario will affect everyone**.”

The causes of a black sky event are many. They vary from natural disasters like hurricanes or earthquakes to [geomagnetic storms triggered by enormous flares from the Sun](https://www.swpc.noaa.gov/impacts), or coronal mass ejections, that send a barrage of electrically charged particles racing across the Solar System and [can overload electrical grids](https://www.sciencedirect.com/science/article/pii/S2352146516306433). One intense geomagnetic disturbance caused [a nine-hour outage across large areas of Canada in 1989](https://www.nasa.gov/topics/earth/features/sun_darkness.html).

The Electric Infrastructure Security Council, an international body that reviews threats to power grids, also [lists a number of human threats that can trigger a mass black out](https://www.eiscouncil.org/BlackSky.aspx). These include cyberterrorism attacks or coordinated physical assaults on energy infrastructure such as power stations, and electromagnetic pulses that can disable electricity grids.

“Our national power grids are tremendous feats of engineering and operations that have supported rapid economic growth around the world,” say Melissa Lott, a research fellow at the Center on Global Energy Policy at Columbia University in New York. “But more investment is needed if electric power grids are going to keep up with rapid technology shifts and increasingly extreme weather events.”

She says that while true black sky events are mercifully rare, the deep impact they have on businesses and people means more needs to not only update grid technology and management, but also improve infrastructure so it can be more resilient against physical threats like flooding.

“In the summer of 2012, blackouts in India cut power to more than 600 million people over two days. In Puerto Rico, Hurricane Maria crippled infrastructure across the island, leaving people in the dark and triggering a humanitarian crisis. In 2018, an earthquake on Japan’s Hokkaido island left more than 5 million people without power. In order to keep these events from becoming more common and to minimise their impact, we need to invest in our grids.”

Putting measures in place to counter all of these potential threats is difficult and expensive. Critical systems can be guarded from human attacks and they can be shielded from electromagnetic pulses with enough money being spent on them. Building new systems for [protecting transformers from coronal mass ejections](https://www.sciencedirect.com/science/article/pii/S2352146516306433) can also help to keep systems safe.

But there are some events that cannot be planned for and the complex, interconnected nature of our electricity grids are remarkably vulnerable. Take what happened in September 2003 when a fallen tree brought down a power line in Switzerland’s Lukmanier Pass over the Alps into Italy and 24 minutes later another tree came down onto a line in the nearby Great St Bernard pass. The sudden failure of these two key lines caused other connections to Europe’s electricity network to trip, which triggered [power plants across Italy to shut down](http://www.rae.gr/old/cases/C13/italy/UCTE_rept.pdf). **The whole of Italy was left without power because of two fallen trees starting a cascade of events.**

Modern electricity grids are increasingly interconnected and complicated, making failures like this difficult to predict. Most of Europe now runs off [a massive interconnected power grid](https://www.entsoe.eu/data/map/) – probably the largest in the world – that supplies more than 400 million customers in 24 countries. The USA is made up of five different grids.

But there are some that are seeking ways of anticipating potential power failures and are enlisting the help of artificial intelligence to help them grapple with this highly complex problem.

When a power plant goes down, for example, it causes an abrupt spike in load on others on the network, which in turn slows down the generators at these plants and causes the frequency held on the grid to decrease. This risks destabilising the delicate balance that electricity grids are held in, and **operators have to deploy countermeasures rapidly – often within milliseconds** – to prevent sections of the grid being cut off.

# AT: T

## t- cybersecurity

### interps

#### 1. We meet: DoD cybersecurity strategy includes defense through OCOs

Erica D. **Lonergan 20,** Assistant Professor in the Army Cyber Institute, PhD in Political Science from Columbia University, “Operationalizing Defend Forward”, Lawfare, 03/12/2020, accessed 6/24/2022, https://www.lawfareblog.com/operationalizing-defend-forward-how-concept-works-change-adversary-behavior.

Defend forward is a crucial component of the Cyberspace Solarium Commission’s strategic concept of layered cyber deterrence, particularly in terms of defend forward’s role in creating costs for adversaries conducting malicious behavior in cyberspace. The commission reimagines defend forward, originally articulated in the 2018 Department of Defense Cyber Strategy, as a whole-of-nation concept. That said, here I will focus on the logic of defend forward in its military application and detail how the concept should be operationalized. Defend forward, as defined by the commission, entails the proactive observing, pursuing, and countering of adversary operations and imposing costs in day-to-day competition to disrupt and defeat ongoing malicious adversary cyber campaigns, deter future campaigns, and reinforce favorable international norms of behavior, using all the instruments of national power. This piece traces the emergence of the logic of defend forward and describes how the commission built on existing concepts to more fully articulate defend forward’s theory of victory and how defend forward seeks to accomplish desired end states.

Defend forward, as a strategic concept, grew out of a number of related realizations about the strategic environment in cyberspace. First, Defense Department entities governed under Title 10 of the U.S. Code have to be able to more routinely operate outside of the department’s own networks, known as the Department of Defense Information Network. Adversary operations span global cyberspace because the environment is not defined by geographic boundaries or even shared understandings about how sovereignty applies in this domain. If the Defense Department’s ability to operate outside of its own networks was more limited and circumscribed, as envisioned in the 2015 Department of Defense Cyber Strategy, the department would be giving free reign to adversary actors that traverse global networks constrained only by capabilities.

Second, intelligence collection in cyberspace against an adversary cannot be conducted solely through static, passive collection. Observing adversaries as they maneuver—and understanding their evolving organizations, capabilities, techniques and personas—requires the U.S., or its allies and partners, to gain access to netwo­­­rks and systems where adversaries operate. The challenge is that this infrastructure is owned by some entity, whether by the U.S. government, private companies or individuals, allied and partner governments, or the adversary. In other words, unlike in other domains, there are no “high seas” or “international waters” in cyberspace. It is important to acknowledge this reality and be transparent about its implications for how the U.S. can and should operate to achieve defensive strategic objectives consistent with international law.

Third, to rapidly generate effects in cyberspace at the desired time, forces and capabilities have to routinely operate where the adversary is. In cyberspace, a decision-maker cannot simply call for fires and reliably anticipate that the desired effect will be delivered against the intended target at the right time. Cyber operations and campaigns demand operational preparation of the environment; prior intelligence collection and operations to identify vulnerabilities and exploits; the development or procurement of tools to deliver the intended effects; and the ability to hold targets at risk over time to deliver the appropriate effect on a decision-maker’s request. Relatedly, capabilities are dynamic—today’s tools may be irrelevant tomorrow—and opportunities are fleeting—today’s access may be gone by tomorrow. Therefore, maintaining cyber capabilities and forces in reserve cedes the initiative to adversaries.

The above understanding coalesced into a new Defense Department strategy anchored in the defend forward concept. Its operationalization, as demonstrated by U.S. efforts to counter Russian interference in the 2018 U.S. midterm elections, was enhanced by further changes to policymaking processes, the delegation of authorities and law. But the Cyberspace Solarium Commission recognized that further work remained to be done to parse the strategic logic of defend forward, identify its desired end states, and trace the causal processes that link its implementation with those objectives.

The commission addresses a central question posed by defend forward: How can the U.S. positively change adversary behavior in cyberspace short of war to produce a more favorable status quo in the short to medium term, while cultivating stability in the international system over the long term?

This question implies a number of desired end states. The first is to change the status quo for activities below the level of war, in which adversaries operate in and through cyberspace to contest U.S. interests on a routine basis. Specifically, defend forward seeks to reduce the magnitude and effects of malicious adversary behavior, recognizing it is impossible to stop or prevent all unwanted activities. The second is to maintain the status quo regarding managing within- and cross-domain escalation dynamics. The U.S. should be able to preserve deterrence of cyberattacks of significant consequence, while being able to employ cyber capabilities below the level of armed attack without triggering significant adversary retaliation or escalation. Third, over the long term, defend forward aims to contribute to the establishment and enforcement of favorable international norms of behavior. Norms do exist in cyberspace, but not all are consistent with U.S. interests and values.

#### 2. Counter Interpretation: Cybersecurity includes forms of deterrence

James E. **Cartwright 10,** General, USMC Vice Chairman of the Joint Chiefs of Staff; “Joint Terminology for Cyberspace Operations"; The Department of Defense Vice Chairman of the Joint Chiefs of Staff; published November 2010; accessed 6/28/2022; <https://publicintelligence.net/dod-joint-cyber-terms/> ;//3AM

Cyber-Security: All organizational actions required to ensure freedom from danger and risk to the security of information in all its forms (electronic, physical), and the security of the systems and networks where information is stored, accessed, processed, and transmitted, including precautions taken to guard against crime, attack, sabotage, espionage, accidents, and failures. Cybersecurity risks may include those that damage stakeholder trust and confidence, affect customer retention and growth, violate customer and partner identity and privacy protections, disrupt the ability to conduct or fulfill business transactions, adversely affect health and cause loss of life, and adversely affect the operations of national critical infrastructures

#### 3. Counter Interpretation: Cybersecurity includes everything that deters attacks on networks

**NICCS no date**, “Explore Terms: A Glossary of Common Cybersecurity Words and Phrases”, CISA National Initiative for Cybersecurity Careers and Studies, No Date, accessed 6/28/2022, <https://niccs.cisa.gov/cybersecurity-career-resources/glossary> //3AM

cybersecurity

Definition: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Extended Definition: Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

Cyber-Security: All organizational actions required to ensure freedom from danger and risk to the security of information in all its forms (electronic, physical), and the security of the systems and networks where information is stored, accessed, processed, and transmitted, including precautions taken to guard against crime, attack, sabotage, espionage, accidents, and failures. Cybersecurity risks may include those that damage stakeholder trust and confidence, affect customer retention and growth, violate customer and partner identity and privacy protections, disrupt the ability to conduct or fulfill business transactions, adversely affect health and cause loss of life, and adversely affect the operations of national critical infrastructures.

#### 4. Offensive capabilities are key to deterrence.

**Mazanec & Thayer 15** – Director in GAO’s Defense Capabilities and Management team; Professor, Faculty of Political Science, University of Iceland

Brian M. Mazanec, Bradley A. Thayer, “Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace,” Palgrave McMillan, 2015, https://link.springer.com/book/10.1057/9781137476180

Deterrence-in-kind: developing offensive cyber capabilities

In addition to a declaratory policy, **developing credible options** for **deterrence-in-kind**, for example, **offensive cyber capabilities**, will be **key** to **bolstering credibility** of such a policy as some actors **will not believe** the United States would respond to a cyber attack with anything but cyber weapons. Peter Singer and Allan Friedman identified this deterrence-in-kind as well as the prospect of mixed ‘cyber- and real-world retaliatory force’ as one avenue to pursue to bolster the deterrence of cyber attacks.13 US Cyber Command’s ambitious plan to field over 100 cyber teams by late 2015 is a **positive step** in this direction.14 Evidence leaked in August 2013 that the United States conducted **231 offensive cyber operations** in 2011 also helps **demonstrate advanced cyber capability**.15 These developments could help ensure any **clear US threat** of **retaliatory cyber attack** in response to a **major cyber attack** was **credible**, in spite of the **challenges** of **weapon** and **target unpredictability**. Some analysts, such as Franz-Stefan Gady, have pointed out that a ‘systematic public display of nation states’ cyber-war capabilities ... . can have a **greater deterrence effect**’ on some actors because they will **better understand adversary capabilities** and **signaling** through behaviors and actions.16

### Prefer our Definition

#### 1. Many measures are taken to ensure DOD definitions are credible

DoD 22, “Standardization of Military and Associated Terminology”; Department of Defense Office of the Director of Administration and Management; effective 1/21/2022; accessed 6/28/2022; https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/502512p.pdf?ver=32dYCHVMwDjYiBxZT9MLXQ%3D%3D; //3AM

3.3. APPROVAL CRITERIA.

Terminology will be approved for inclusion in the DoD Dictionary when it is:

a. Directed by the Secretary of Defense, Deputy Secretary of Defense, or the Chairman of the Joint Chiefs of Staff.

b. Nominated for inclusion in the DoD Dictionary by the OSD or DoD Component heads, coordinated with OSD, the Office of the Chairman of the Joint Chiefs of Staff, and the Military Departments at a minimum, and approved according to the provisions of this issuance and Chairman of the Joint Chiefs of Staff Instruction 5705.01.

c. Nominated for inclusion in the DoD Dictionary in an appropriate source document (e.g., joint doctrine publications, DoD issuances, Chairman of the Joint Chiefs of Staff issuances) consistent with Chairman of the Joint Chiefs of Staff Instruction 5705.01, and coordinated by the sponsoring DoD Component with OSD, the Office of the Chairman of the Joint Chiefs of Staff, and the Military Departments, at a minimum.

#### 2. This definition is used everywhere by everyone related to the military

**Joint Chiefs of Staff 18**, “DoD Dictionary of Military and Associated Terms”; United States Joint Chiefs of Staff; published June 2018; accessed 6/28/2022; <https://www.hsdl.org/?view&did=813130> ; //3AM

1. Scope

The DOD Dictionary of Military and Associated Terms (DOD Dictionary) sets forth standard US military and associated terminology to encompass the joint activity of the Armed Forces of the United States. These military and associated terms, together with their definitions, constitute approved Department of Defense (DOD) terminology for general use by all DOD components.

2. Purpose

This publication supplements standard English-language dictionaries and standardizes military and associated terminology to improve communication and mutual understanding within DOD with other US Government departments and agencies and among the United States and its allies.

3. Application

This publication applies to the Office of the Secretary of Defense, the Services, the Joint Staff, combatant commands, DOD agencies, and all other DOD components. It is the primary terminology source when preparing correspondence, to include policy, strategy, doctrine, and planning documents. Criteria for inclusion of terminology in the DOD Dictionary is enumerated in Department of Defense Instruction (DODI) 5025.12, Standardization of Military and Associated Terminology, and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5705.01, Standardization of Military and Associated Terminology.

#### 3. Any time any military or ex-military author talks about cybersecurity, they will use our definition, means predictability which outweighs all else

# AT: Tradeoff DA

### UQ/thumpers

#### NATO already announced climate initiatives at Madrid Summit in the face of other priorities

The National News 6/28 (Thomas Harding, “Climate change to shape Nato's security policy after Madrid summit,” The National News US, 6/28/2022, <https://www.thenationalnews.com/world/europe/2022/06/28/climate-change-will-shape-natos-security-policy-at-madrid-summit/>) -LH

NATO has responded to pressure to meet the challenge presented by climate change to world security by pledging to cut its civilian and military greenhouse gas emissions by at least 45 per cent by 2030.

Secretary General Jens Stoltenberg on Tuesday said alliance operations would be carbon neutral by 2050, as he announced the first emissions targets for the organisation.

"It will not be easy but it can be done," he said at the Nato summit in Madrid. "All allies are committed to reducing their greenhouse gas emissions as part of the Paris agreement. Adapting their militaries will contribute to this, including more green tech, such as renewables, climate-friendly synthetic fuels and more energy efficient solutions."

A report from a British think tank said it was “imperative” that the summit addressed Nato’s role in providing climate solutions, especially as rising temperatures across in the Middle East and North Africa would have ramifications for security in Europe.

“The Mena region risks being particularly impacted and is in Europe’s neighbourhood,” Chatham House said.

“Although recent Nato interventions in the region have been limited to operations in Libya, Afghanistan and Iraq, further instability due to climate change on Nato’s southern flank could be the tipping point to develop a much-needed coherent strategy for supporting stabilisation and peacebuilding efforts in the Sahel and beyond.”

Madrid summit discussions were due to open on Tuesday with an address on climate change and alliance security from Iceland’s Prime Minister Katrin Jakobsdottir.

The Chatham House paper urged Nato to prioritise climate change because it can become a “threat multiplier” with increased mass migration, weakening governments and food and water scarcity.

“It is imperative the summit and the new Strategic Concept [statement of the alliance's values] lay the groundwork for Nato’s sustained role in tackling climate change-induced security challenges,” it said.

Climate change threatens strategic interests by exacerbating problems, which can “ultimately contribute to conflict”.

As Nato prepares to issue its first Climate Change and Security Progress Report in Madrid, it was “crucial this maintains the same level of determination to prepare the alliance for climate-related instability”, Chatham House said.

Another report, by the International Military Council on Climate and Security, highlighted the “high operational costs” of fossil fuel use by militaries.

It recommended that Nato states procure and develop equipment with low carbon emissions.

“We have passed the point of debating whether or not climate change is also a matter of national security,” said Gen Tom Middendorp, chairman of IMCCS and former chief of defence for the Netherlands.

“It is time to develop solutions. The security sector has a role to play in forecasting the security effects of climate change and in the areas of mitigation and adaptation.”

Last year, Nato figures suggested the carbon emissions from a 60-tonne US Abrams main battle tank were the equivalent of 10 Mercedes-Benz cars.

Mr Stoltenberg has urged militaries to look at how they can power tanks and jets with alternative energy sources, such as solar panels, to reduce its carbon emissions.

“Nato should do its part to look into how we can reduce emissions from military operations,” he told a Chatham House event in 2021.

“We know that heavy battle tanks or fighter jets and naval ships consume a lot of fossil fuel and emit greenhouse gases and therefore we have to look into how we can reduce those emissions by alternative fuels, solar panels or other ways of running our missions.”

Reducing dependence on fossil fuels would help to eliminate a vulnerability common to many operations, where long supply lines are used take fuel to the front line, Mr Stoltenberg said.

#### Security already top priority for NATO at Madrid Summit— means climate focus is either resilient or inevitably doomed

NATO 6/23 (NATO, “INTRODUCTION: A NEW SECURITY REALITY – A UNITED ALLIANCE,” On the Agenda Madrid Summit, 29-30 June 2022, 6/23/2022, https://www.nato.int/cps/en/natohq/news\_196910.htm)-LH

NATO Leaders are meeting in Madrid at a pivotal time for our security. Russia's war against Ukraine has shattered peace in Europe, caused far-reaching energy and food crises, and shaken the rules-based international order. NATO's response has been swift and united.

More than ever, NATO is the indispensable platform for transatlantic consultations and cooperation on security and defence. At the Madrid Summit, Allies will continue to adapt, taking decisions to keep NATO strong and ready in a more dangerous world. Heads of State and Government will agree to strengthen deterrence and defence, and support Ukraine for the longer term. They will agree the 2022 Strategic Concept, which will be a roadmap for the Alliance in the years to come. Allies will also boost cooperation with partners, enhance resilience and sharpen NATO's technological edge – all underpinned by the necessary investments in our collective defence.

#### Litany of issues on the agenda for the Madrid Summit besides climate— proves climate agenda is either doomed or resilient

Erlanger 6/27 (Steven Erlanger, Steven Erlanger is the chief diplomatic correspondent in Europe, based in Brussels. He previously reported from London, Paris, Jerusalem, Berlin, Prague, Moscow and Bangkok. Mr. Erlanger graduated from the Taft School in Watertown, Conn., and received an A.B. degree, magna cum laude, Phi Beta Kappa, from Harvard College in 1974. He majored in political philosophy in the government department. He also studied Russian as a senior fellow at St. Antony’s College, Oxford. “Spotting the Fault Lines in NATO’s United Front,” New York Times, 6/27/2022, https://www.nytimes.com/2022/06/27/world/europe/nato-summit-madrid-ukraine.html)-LH

BRUSSELS — After the collapse of the Soviet Union, some asked whether NATO had any real reason to exist. But Russia’s invasion of Ukraine gave new urgency to NATO as a defensive alliance aimed at deterring Moscow.

Now, at its annual summit meeting this week in Madrid, leaders of the 30 members of NATO are set to agree on the most significant overhaul of the alliance’s defenses since the Cold War.

There will be a large increase in the number of troops assigned to defend NATO’s eastern flank, closest to Russia and Belarus, with a major commitment to position heavy military equipment there, like tanks and artillery, that would bolster an allied response to any Russian threat or aggression.

There will also be statements of unity on Ukraine, despite internal debates within the alliance on how long the war will take, how it will end and its mounting costs to NATO and European allies.

“The summit will show western solidarity as we go into a period of high gas prices and food scarcity, with Russia willing now to use both as weapons of war,” said Kori Schake, director of foreign and defense policy studies at the American Enterprise Institute. “So we know that and can still hang together.”

At the same time, she said, debates about the future are rumbling among member countries. “The lesson the U.S. is tempted to take away from Ukraine is the incapacity of the Russian military, suggesting that Europe should be able to handle the burden of European security,” Ms. Schake said. “But the European lesson is that unless the U.S. is at the center of the Western response, there will be no Western response, so they’re trying to lock in American involvement.”

In Madrid, the alliance will also approve its first updated mission statement in 12 years, portraying a world of new perils, with threats not just from Russia but also China, an American priority, and from new forms of warfare ranging from cyber and artificial intelligence to disinformation and restrictions on energy, food and rare minerals.

The mission statement, known as the strategic concept, frames defense planning, spending and resource allocation throughout the alliance. It sounds arcane but has been hotly debated, with France and Germany insisting on describing a rising China as a “challenge” to the trans-Atlantic security order, not as a “threat,” as Russia has clearly become.

There will also be discussion on how to convince Recep Tayyip Erdogan, the president of Turkey, to remove his effective veto over the applications of Sweden and Finland to join NATO, a matter that inevitably will have to involve President Biden.

One of the other key debates during the summit, which runs from Tuesday evening through Thursday, will be the issue of new NATO troops along the eastern flank — how many, how they are deployed, and how permanent they will be.

As the war in Ukraine has proceeded, NATO has established four more multinational battalion-sized groups in Romania, Bulgaria, Hungary and Slovakia, to add to the ones already established in 2017 — following Russia’s annexation of Crimea in 2014 — in Estonia, Latvia, Lithuania and Poland.

The Baltic nations of Estonia, Latvia and Lithuania are pressing for larger permanent deployments, to move from the current “tripwire” defense — the roughly 1,500 rotating NATO troops in each country — to “deterrence by denial,” which would involve more permanent deployments of up to a division of American troops, as Estonia has been demanding.

They want the larger deployments to better defend all NATO territory from any conflict at its very start, fearing that they would be quickly overrun by Russian forces otherwise.

The secretary-general of NATO, Jens Stoltenberg, said recently that allies could agree “to strengthen battle groups in the east up to brigade level,” which would bring them to between 3,000 and 5,000 troops.

A permanent American division is not in the cards. Mr. Biden is expected to announce new deployments of another one or two brigade combat teams to bring the assigned level of American troops in Europe to about 100,000, up from some 70,000 before the Russian invasion, NATO officials said.

But they are likely to be kept in Germany and Poland, ready to move in times of threat or conflict to pre-assigned countries where they will also train with pre-positioned equipment.

Other NATO allies are increasing their deployments, too, with Germany announcing the addition of 500 troops to its forces in the multinational battlegroup it leads in Lithuania, plus the pre-assignment of some 3,000 more troops in case of trouble.

There has been criticism from the Baltic nations that those troops will be stationed in Germany. But the German government and other allies argue that it is too expensive to build permanent barracks and schools to house troops and their families in other countries when they can arrive quickly to the battlefield from established bases in places like Germany.

“They argue that you need large forces in the country like a Maginot line to prevent them from being overrun early in a conflict,” said Ivo Daalder, a former U.S. ambassador to NATO and head of the Chicago Council on Global Affairs, referring to the Baltic countries. “But that’s not the best way to defend them, because these countries are too small for real, regular training, which you can do in Poland or Germany. Better to have them there and constantly train them and rotate them regularly.”

The issue is now more sensitive, with Moscow accusing Lithuania of blocking its rail shipments to its heavily armed enclave of Kaliningrad in line with E.U. sanctions against Russia, and threatening reprisals. Lithuanian and European officials say there is no blockade against the enclave, which is on the Baltic Sea, sandwiched between Poland and Lithuania. But the narrow strip of some 60 miles between Belarus and Kaliningrad, known as the Suwalki Gap, is considered vulnerable.

The anxiety among the Baltic countries is justified, said Ms. Schake. “I would want more NATO deployments too if I were them, because they live exposed,” she said. “For smaller countries, proximity to a Russia that would negate Ukraine is scary.”

Since the start of the war, NATO has activated its “response force,” now 40,000 troops, under NATO command. Mr. Stoltenberg said on Monday that the force would be expanded to 300,000. It is expected to be rebranded as the Allied Response Force, and will include more troops based in their home countries but pre-assigned to the eastern flank if needed.

Mr. Daalder sees another fault line in the different perceptions of the Russian threat among NATO members. Some, especially in former Soviet-bloc nations, believe that “Russia has fundamentally changed everything and we’re back to a Cold War alliance, and we have to hold the line from the Barents Sea to the Black Sea,” he said, referring to NATO’s northern and southern reaches.

And there are other members of the alliance, including the United States, Italy and Spain, which say there are other important threats too — from terrorism, climate change and mass migration. And then there is China’s inexorable rise as a technically advanced rival seeking global influence.

There is also the question of how big NATO should be — not just in light of the potential addition of Finland and Sweden, but also its 2008 promise that Ukraine and Georgia would one day be full members, Mr. Daalder said. Both the European Union and NATO have now promised Ukraine paths to membership, but have been vague about that commitment. “I don’t think NATO can just walk away from it in Madrid, as some would like,” he said.

And as ever, there will be debates about increases in military spending, about NATO’s own budget and about burden-sharing, not only between the United States and its allies but between the European Union and NATO.

Christopher Skaluba, a security expert at the Scowcroft Center for Strategy and Security of the Atlantic Council, said that “following the money at NATO is always a smart idea.” NATO allies make commitments, “but they’re easier to say than do, and inflation makes everything more expensive,” he said.

“The cost of failing to deter Russia from going into Ukraine is very high, and we’re all paying the price for it, the Ukrainians most of all,” Mr. Skaluba said. The pressure to walk back from the alliance’s commitments, he said, “will be real, too.”

#### Variety of agenda items plus climate goals for upcoming Madrid summit proves NATO can focus on many things at once

Anadolu Agency 6/27 (Beyza Binnur Donmez, “What to expect from NATO's Madrid summit,” Anadolu Agecy, 6/27/2022, <https://www.aa.com.tr/en/politics/what-to-expect-from-natos-madrid-summit/2623259)-> LH

MADRID Leaders of NATO's member countries and key partners are set to meet in Madrid to discuss issues facing the alliance during a three-day summit beginning on Tuesday.

Russia's war against Ukraine has shattered peace in Europe as it caused far-reaching energy and food crises by shaking the rules of the international order since it began on Feb. 24.

As NATO became a more indispensable platform for transatlantic cooperation on security and defense, allies will continue to make decisions to keep the alliance ready against any threat at the summit.

Strengthening NATO's long-term deterrence and defense, sustaining support for Ukraine, launching NATO's 2022 Strategic Concept, reinforcing partnerships and maintaining an open door, adapting to threats and challenges from any direction, and transatlantic unity and alliance solidarity will be on the agenda for the member states to discuss.

Some "important" topics to be discussed by members and partners include how has Russia's military operation in Ukraine and the new security reality in Europe affected the alliance's approach to deterrence and defense; what is NATO doing to address challenges like China's growing influence or security consequences of climate change and what to include in the next Strategic Concept.

To protect and defend allied territory amid the current security reality, NATO has more than 40,000 troops under direct command, backed by air and naval assets.

The alliance also doubled the number of battlegroups to eight, extending from the Baltic Sea in the north to the Black Sea in the south.

NATO leaders will "significantly strengthen the Alliance's posture for the long term, with more presence, capabilities and readiness," according to the alliance, which will require adequate resources and continued investment in defense.

Support for Ukraine Noting that allies "significantly stepped up with billions of euros' worth" of additional lethal and non-lethal aid to help Ukraine after Russia launched its war in February, NATO said it builds on the years of NATO training and assistance since Moscow's illegal annexation of Crimea in 2014.

Leaders of member countries will meet with Ukraine to agree to step up and sustain support for the "longer-term" at the summit.

2022 Strategic Concept Serving as a blueprint for future adaption, strategic concepts give the alliance the ability to respond to current security challenges and guide political and military developments for the challenges of tomorrow.

In Madrid, leaders will endorse a 2022 Strategic Concept, which will set out NATO's joint positions, including on Russia and emerging challenges, and will address China for the first time.

"The Madrid Strategic Concept will reflect the new security environment, recommit to our values, and reaffirm our unity, ensuring that our Alliance is fit for the future," NATO Secretary-General Jens Stoltenberg said of the new concept.

The concept has been reviewed and updated approximately every 10 years since the end of the Cold War. The last one was adopted at the Lisbon Summit in 2010.

Reinforcing partnerships, maintaining an open door

Finland and Sweden's NATO bids will belong to the main agenda points of the summit as part of the alliance's Open Door policy.

Sweden and Finland formally applied to join the alliance last month, a decision spurred by Russia's war on Ukraine.

But Türkiye, a longstanding member of the alliance, has voiced objections to the membership bids, criticizing the countries for tolerating and even supporting terrorist groups.

Stoltenberg has constantly said that Türkiye has "legitimate concerns related to their fight against the PKK a group and other organizations," and that the PKK is considered a terror organization by NATO, the EU, Finland, and Sweden.

However, Spanish Foreign Minister Jose Manuel Albares recently said the host country hopes to sign with Finland and Sweden at the summit as parties could get closer in talks during the one-week window.

In its more than 35-year terror campaign against Türkiye, the PKK has been responsible for the deaths of more than 40,000 people.

NATO will step up support to Georgia and other partners to build their capabilities and strengthen their resilience during the summit.

The leaders of four Asia-Pacific partners -- Australia, Japan, the Republic of Korea and New Zealand will be part of a NATO summit for the first time.

Adapting to threats, challenges Member countries are set to make decisions to maintain NATO's technological edge, "including through the new Defence Innovation Accelerator for the North Atlantic and a billion euro Innovation Fund, to support start-ups and develop cutting-edge solutions to security challenges," according to the alliance.

Terrorism, cyberattacks, China's "coercive" policies, disruptive technologies and the security impact of climate change are among the topics that the alliance will focus under threats and challenges title.

Regarding climate change, leaders will agree on a new methodology to map military greenhouse gas emissions and a target to help NATO contribute to the goal of net-zero emissions.

As NATO faces "the most serious security situation in decades," the decisions leaders make in Madrid will ensure that NATO continues to preserve "peace, prevent conflict and protect our people and our values," according to the alliance.

The summit has special importance for Spain as the country is hosting on the 40th anniversary of Madrid's accession to NATO.

# AT: PTX DA

### 2AC – NUQ

#### Bill won’t pass – Extensive big tech lobbying and competing priorities effectively deter lawmakers

Zakrzewski et al. 6/27/22 – Cat Zakrzewski, Will Oremus, Gerrit De Vynck and Cristiano Lima ("With clock ticking, battle over tech regulation intensifies"; Washington Post; https://www.washingtonpost.com/technology/2022/06/27/antitrust-tech-battle-congress/; 6-27-2022, Accessed 6-28-2022)//ILake-AZ

The left-leaning advocacy group Fight for the Future watched as tech companies blanketed the airwaves with ads urging millions to tell their senators to block major antitrust bills winding their way through Congress. Trying to make the most of its significantly smaller budget for counter messaging, the advocacy group decided to target one person: Senate Majority Leader Charles E. Schumer.

Over the weekend, the group drove billboard trucks with 12-foot-wide screens to Schumer’s homes in New York and Washington, blaring a video of comedian John Oliver urging Congress to pass the legislation.

The decision to target Schumer was a simple one, said Evan Greer, Fight for the Future’s director: “He is the key. … This was a way to get creative and put this right in his face.”

Friends and foes alike of the landmark legislation, two bills that seek to rein in the business practices of the country’s largest tech companies, have their eyes on Schumer, who will decide whether the legislation will make it to the Senate floor for a vote.

In recent days, it’s not just proponents of the bills who have sought to sway Schumer. The leaders of Google and Amazon have personally called the Senate majority leader. His office said he tells anyone who calls him to discuss the legislation the same message: “Senator Schumer supports the legislation and is working with Senator [Amy] Klobuchar and others to get the necessary votes to pass it,” said Schumer spokesman Justin Goodman.

It’s a wonky yet momentous political battle that has united an unlikely alliance of would-be trustbusters from left and right against some of the wealthiest corporations in world history. With time running out for this Congress to pass them, those corporations are putting up the political fight of their lives.

Facebook quietly bankrolled small, grass-roots groups to fight its battles in Washington

Three years in the making, the legislation would prohibit the largest online platforms from tilting the playing field toward their own goods and services, its proponents say. But the tech companies say it would do far more than that, squelching innovation and giving a leg up to their rivals in China. They aren’t shy about claiming a national security threat.

The titans of the industry have mobilized like never before to combat it. Google CEO Sundar Pichai personally called Schumer during a visit to Washington last week. Amazon CEO Andy Jassy has been making personal calls to Schumer and other lawmakers, Politico first reported earlier this month. And Apple CEO Tim Cook made his own trip to Capitol Hill earlier this month.

Meanwhile, industry-backed groups have been pouring tens of millions of dollars into an anti-regulation campaign, blasting ads on TVs and social media feeds across the country that warn Americans the tech bills will break popular services like Amazon Prime and Google Maps. The groups have already spent $72 million on ads this year, according to an analysis from the ad tracking firm AdImpact. Nearly half of that money was spent in June alone.

“Spending $72 million is a drop in the bucket,” said Rep. David N. Cicilline (D-R.I.), who authored the House legislation and led a bipartisan investigation into the companies. “These companies have billions and billions of reasons to oppose the legislation and maintain the status quo.”

The focus on Schumer has intensified after the segment on Oliver’s show, which is known for bringing mainstream attention to complex policy issues. In the segment, Oliver zeroed in on Schumer particularly, noting that he has not yet brought the bills for a floor vote. He also mentions previous media reports that show that 17 members of Congress have children who work or recently have worked at large tech companies, including Schumer’s daughters who work as a marketing manager at Meta and a registered lobbyist for Amazon.

Yet there are key holdouts in both parties. Though two key tech antitrust bills passed through committee earlier this year with strong bipartisan support, members of both parties indicated they had outstanding concerns that would need to be addressed before a floor vote. Schumer’s resolve to pass them is in question amid a bevy of competing priorities.

Senate advances antitrust legislation, despite reservations from California Democrats

The clock is ticking. The legislation has support from the left, right and center, a rare alliance that will likely dissolve after the midterm elections, said William E. Kovacic, former Republican chair of the Federal Trade Commission and a professor at George Washington University Law School who studies antitrust and competition.

“Simply put, this may be the best chance the advocates of new legislation ever get to realize their aims for reform,” Kovacic said.

For more than three years, through a pandemic, two impeachments and an insurrection, lawmakers and their staffs have systematically collected evidence that Amazon, Apple, Google and Facebook engaged in anticompetitive tactics to solidify their dominance across the internet. They’ve hosted high-profile hearings with the companies’ CEOs, and pushed bills through House and Senate committees with bipartisan votes. And they heard from the CEOs of smaller tech firms, including Sonos, Spotify and Tile, who testified that the giants had leveraged the power of their platforms to give their own apps and products unfair advantages over independent rivals.

The congressional probe found that the four companies control essential portals to the digital economy — and increasingly use those platforms to offer their own products and features, competing with the same businesses that rely on them. Critics say that’s a glaring conflict of interest; the tech giants say it’s for their customers’ own good.

Breaking up the companies isn’t on the table in the current antitrust package, which focuses on regulating tech companies’ treatment of rivals. Still, the bills mark the closest Washington has yet come to comprehensive regulation of a U.S. tech industry that includes four of the world’s five most valuable publicly traded companies.

The key bills — the American Innovation and Choice Online Act and the Open App Markets Act — have been languishing in Congress for months, and their chances of becoming law grow dimmer the closer Congress gets to the midterms, when lawmakers’ attention will turn to campaigning. Democrats risk losing control of Congress in that election, and significant tech antitrust bills are viewed as unlikely to pass under Republican leadership.

In an interview Friday, Cicilline said it’s “very important” that the legislation comes to a floor vote before Congress leaves for its August recess.

“Every day we wait, we are doing significant harm to the ability of small businesses to survive,” Cicilline said.

The fate of lawmakers’ tech antitrust push may hinge on one bill

The legislation’s supporters are up against a host of competing political priorities, as Democrats and the Biden administration scramble to address gun control, inflation, climate policy and the Supreme Court’s reversal of Roe v. Wade.

Cicilline says that lawmakers have the votes to pass the legislation, and the tech executives’ recent visits to Washington reflect how worried they are. Pichai also met with Sen. Dianne Feinstein (D-Calif.), who had previously raised concerns that the bills would single out companies in her home state. He also met with Republican lawmakers including Senate Minority Leader Mitch McConnell (R-Ky.), Senate Minority Whip John Thune (R-S.D.) and Sen. Steve Daines (R-Mont.), said multiple people familiar with the matter who spoke on the condition of anonymity to discuss private meetings. Representatives for McConnell, Daines and Thune did not respond to a request for comment.

In meetings with Republican lawmakers, Pichai warned that the antitrust bills would be bad for innovation. However, the conservative lawmakers were focused on accusations that the company’s email system is politically biased. Pichai also discussed the company’s interest in federal privacy legislation and a key chip subsidies bill, one person said.

“We regularly engage with lawmakers and regulators on a range of issues and to be helpful with their efforts around economic growth, small business support, immigration, cybersecurity, and protecting online information, among other issues,” José Castañeda, a Google spokesman, said in a statement.

He also said that the company does not filter email based on political affiliation and said that it was working to increase transparency data about bulk sending.

A multimillion-dollar campaign is pushing Dems to ditch antitrust reform

Industry groups are pushing the message to policymakers that tech regulation is not a top priority for voters in the 2022 political environment. Chamber of Progress, a left-leaning group funded by Amazon, Apple and Google, has distributed polling to congressional offices that suggests voters in key battleground states like Arizona and Nevada see tech regulation as a significantly lower priority than taming inflation or protecting the border.

The groups have also targeted their ad blitz in states where Democrats face key elections, including Georgia, Nevada, Arizona and Colorado, according to the AdImpact data. The ads play on Americans’ concerns about inflation, and suggest that the legislation could break Amazon Prime’s guarantee of two-day delivery and bust services that Google offers free.

“Families are getting squeezed by rising prices, and now Congress is considering a bill that could make things worse for millions of Americans,” says an ad from the Computer and Communications Industry Association, which is backed by Amazon, Apple, Facebook and Google. The ads then urge people to call their senators to press them to vote “no” on the antitrust measure.

Cicilline argues that by creating more competition, the legislation would help address the economic conditions contributing to inflation.

Industry groups have also sought to torpedo the bills by playing on partisan divisions over tech regulation. The Chamber of Progress is running digital ads suggesting that the antitrust legislation would make it harder for companies to remove violence and misinformation. The ads link to a petition that asserts the bill could prohibit Amazon from taking down anti-vaccine documentaries or could have stopped Apple from booting Parler from the App Store in the wake of the Jan. 6 insurrection.

Cicilline called these arguments “completely false,” saying there is nothing in the bill that would prevent companies from upholding standards for content across their services.

Tech groups and executives have also sought to shift the focus to privacy rather than competition policy, especially after a trio of key lawmakers reached a deal on privacy legislation. Netchoice, an industry trade group with funding from Google and Facebook, has been telling lawmakers that privacy is a bigger priority for voters than antitrust, said spokesman Rob Winterton. During his recent visit to Washington, Cook sent a letter to lawmakers urging them to “advance comprehensive privacy legislation as soon as possible.”

House and Senate members unveil stalled data privacy bill

The pro-regulation groups have also been spending — through far less than their Big Tech counterparts.

The Fight for the Future trucks broadcasting John Oliver around New York and Washington cost about $30,000. The Tech Oversight Project says it will spend about $250,000 by the end of June on ads supporting the legislation, also targeting states where Democrats face challenging races in the fall.

A coalition of smaller tech companies, civil society groups and nonprofits have launched their own response, pressing lawmakers to swiftly move on the legislation ahead of the midterms. That included last-minute trips to Capitol Hill by the CEOs of Kelkoo, a European price comparison site, and Proton AG, a Swiss-based company that provides an encrypted email service.

Proton CEO Andy Yen, who made his first trip to Capitol Hill as CEO to lobby in favor of the bills last week, said the policy debate has long been “dominated by the big tech companies.”

#### Antitrust won’t pass – big tech pressure significantly surpasses Congressional resources and democrats are increasingly concerned for Midterms

Chitkara 6/8/22 – Reporter at Protocol focused on the intersection of politics, technology and society (Hirsh Chitkara; "Antitrust optimism is waning"; Protocol; https://www.protocol.com/newsletters/policy/antitrust-congress-midterms-competition; 6-8-2022, Accessed 6-27-2022)//ILake-AZ

Antitrust's feeble optimism

Yesterday on MSNBC’s “Morning Joe,” Sen. Amy Klobuchar tried to strike an optimistic note on the fate of the long-awaited American Innovation and Choice Online Act. “I believe we’re going to pass this,” she said of the bill, which aims to prevent Big Tech platforms from giving preference to their own products. Klobuchar also reiterated Senate Majority Leader Chuck Schumer’s promise to put the “strongly bipartisan bill” to a vote by early summer.

So what still needs to happen for the bill to pass? It already went through House and Senate subcommittees, so the next step would be for Schumer to call a floor vote. In February, the White House came out in support of the congressional antitrust push, so President Biden would sign the bill into law — if it gets that far.

Big Tech is doubling down on efforts to kill the bill, and that hasn’t escaped Klobuchar’s notice. Despite insisting that the bill will pass, Klobuchar acknowledged that her camp faces unprecedented resistance from the Big Tech lobby.

“I have never seen anything like this,” she said. “They are bullies. They’re making stuff up — making things up left and right that aren’t true.”

This came in response to host Joe Scarborough referencing the anti-antitrust advertising campaign, which he called “outright propaganda.” Klobuchar said firms spent $21 million in ad-buy against the bill just in the past week. Earlier reports showed the Amazon- and Alphabet-backed Computer and Communications Industry Association allocated $8.4 million for TV ads targeting midterm swing states such as Arizona, Georgia, Nevada, New Hampshire and Wisconsin.

The antitrust advocates are severely outmatched when it comes to legal resourcing. Klobuchar said the tech firms have hired “thousands of lawyers and lobbyists,” as compared to the two lawyers on her team.

Big Tech’s efforts are apparently working — Democrats just won’t publicly admit it.

Behind closed doors, Democratic senators have complained to Schumer that forcing an early summer antitrust vote would reduce their chances in midterms, according to POLITICO reporting from May.

If the votes aren’t there, Schumer would likely decline to bring the bill to the floor. That would help Democrats save face, at least relative to publicly voting against an antitrust bill that has been a pillar of their agenda for years.

It would also almost certainly doom the bill. Democrats are projected to lose big in midterms, so “delaying” a vote really means giving up.

The Jan. 6 House committee hearings might be the final nail in the coffin. Would it be nice if D.C. could walk and chew gum at the same time? Of course. But if we’re being honest, that’s not always how things work on the Hill. The Jan. 6 committee hearings will be a media circus, drawing a lot of media attention away from the antitrust bill. The literal “prime time” event kicks off tomorrow and could go all the way until November. It’s supposed to rally support for Democrats ahead of midterms; ironically, it could just make those reelection efforts more difficult by taking away what was supposed to be the signature legislative win for the term.

### 2AC – Plan Bipart

<https://www.sinema.senate.gov/sites/default/files/2022-03/Cybersecurity.Infrastructure.Institutions.Final_.pdf>

Shoring up cyber defense against Russian cyberattacks is bipartisan

Sinema 22 – Arizona Senior Senator (Kyrsten Sinema; "Protecting America Against Russia’s Cyber Threats, Sinema Urges Administration to Help Businesses & States Shore Up Vulnerabilities"; Senator Kyrsten Sinema; https://www.sinema.senate.gov/protecting-america-against-russias-cyber-threats-sinema-urges-administration-help-businesses-states; 3-25-2022, Accessed 6-26-2022)//ILake-AZ

WASHINGTON – Arizona senior Senator Kyrsten Sinema and a bipartisan group of colleagues urged the U.S. Secretaries of Defense and Homeland Security to help private, state, and local institutions shore up their cyber vulnerabilities against Russian threats.

“We implore you to act without delay in providing the necessary resources and working with our private, state, and local institutions to prevent our critical infrastructure, systems, and institutions from being compromised by nefarious attempts to respond to justified sanctions. We must act now, with increased haste, before we find ourselves under a major retaliatory cyber offensive that causes extreme disruption in the lives of everyday Americans,” wrote Sinema and her bipartisan group of colleagues.

Sinema’s bipartisan letter notes the vulnerability of public and private infrastructure relating to potential cyber attacks by Russia. Following international sanctions against Russia in response to Russia’s illegal and unprovoked war in sovereign Ukraine, Sinema and her colleagues raise concerns of Russia retaliating against the United States through cyber attacks.

As Sinema and her colleagues underscore in their letter, cyber threats are growing faster than private and state partners are able to adapt. Those stakeholders, need robust federal support and information to absorb and rebuff offensive cyber operations by foreign adversaries.

### 2AC – AT Tech Leadership

Chinese tech leadership is already cemented in– best studies prove

Lam et al. 19 – Taylor Lam is the Technology, Media, & Telecommunications industry leader at Deloitte China; Frank Li is the Technology sector leader at Deloitte China; Jeff Loucks is the managing directorof Deloitte Services LP and executive director of Deloitte's Center for Technology, Media, and Telecommunications ("China Emerges as Global Tech, Innovation Leader"; WSJ; https://deloitte.wsj.com/articles/china-emerges-as-global-tech-innovation-leader-01572483727; 10-30-2019, Accessed 6-28-2022)//ILake-AZ

China has emerged on the world stage with a wave of innovative, competitive technology companies looking to replicate their successes beyond the Chinese market. As the country rapidly transforms into a global technology leader, executives in multinational companies can benefit from understanding the state of China’s technology industry and what it may mean for their businesses. A recent Deloitte Dbriefs webcast delved into China's technology landscape, recent trends, and predictions for emerging sectors.

The Digital Landscape in China: Size Matters

Although China’s internet penetration rate is only 60% (compared with 89% in the United States), its sheer scale means there are three times more internet users than in the United States—a total of over 800 million. Nearly all of China’s internet users access the web through mobile devices from the country’s biggest smartphone companies, Huawei, Oppo, and Vivo. Now, these companies are looking to take on foreign competitors to lure high-spending customers.

Moreover, 583 million people in China pay with their phones—more than the total U.S. population. The country has been able to kick-start a mobile payment and e-commerce revolution thanks to a developed and pervasive payment infrastructure. Among China’s most-used solutions is Tencent’s WeChat, an all-in-one platform that combines social messaging, mobile payments, and in-app programs that are portals for shopping and gaming.

Internet data in China, meanwhile, is provided by the big three state-owned telecom companies, so the government retains ultimate control over data pricing. Last year, the Chinese government ordered the companies to slash the cost of mobile data by 30% as part of a push to evolve the digital economy, which the government sees as one of the major drivers of growth. China's traditional heavy industries are in decline, and the government wants to stimulate domestic consumption of high-tech services rather than rely on exports, shipping, and manufacturing.

A prime example of this growth was an uptick in Chinese technology, media, and telecommunications companies launching IPOs in 2018: More than 50 went public with a combined market capitalization of over $200 billion.¹ They included Xiaomi, a smartphone software producer, and China Tower Company, which focuses on telecommunications towers.

A Race for 5G Dominance

Countries that adopt 5G first will likely experience disproportionate advantages in the digital world, including increased economic activity and job growth. Markets like China enjoy cooperation at the local level, which is an advantage when rolling out infrastructure. In 2018, China started 5G trials in more than a dozen cities, and this year the government issued the go-ahead for major state-owned mobile carriers to start rolling out 5G, including commercial applications. According to the Global Financial Markets Association, China will account for the largest number of 5G connections in 2025, with 416 million—greater than North America and Europe combined.

China Aims for World Leadership in AI

AI has seen breakthroughs in recent years thanks to advances in processing power and big data collection, among other areas. Many governments are investing significantly in AI, viewing it as a driver of economic growth and competitive advantage globally.

In 2017, China's state council published a plan aiming to become the world leader in AI by 2030. China's investment in AI already accounted for more than half of the world's total investments in 2018. China’s triumvirate of tech giants, known as BAT (Baidu, Alibaba, and Tencent), is investing heavily in AI, including in areas previously dominated by U.S. companies.

A recent Deloitte survey of 1,900 executives at companies that are early adopters of AI found that China places the most emphasis on the strategic importance of AI compared with other countries. Forty-six percent of Chinese companies report having created a comprehensive, detailed, companywide strategy on AI implementation. In addition, 55% percent say they have achieved strong competitive advantage and additional commercial value with AI. Finally, per the survey report, China reportedly has the world's second-highest number of AI companies, following the United States.

China Invests Heavily in Semiconductors

Semiconductor chips are the brains that animate devices ranging from hyperscale servers to smartphones to sensors at the edge of the network; they represent a global market of more than $400 billion. Companies are racing to bring new kinds of chips to market, including those that power AI and connect 5G smartphones.

China is investing heavily in semiconductor production. The country knows its future competitiveness depends on whether it can lead new growth in areas like AI and 5G, which in turn depends on its ability to produce the chips that bring these technologies to life. With the threat of continued supply disruptions arising from trade tensions, it's little wonder that China plans to make semiconductor production an important goal going forward.

Yet, while China is now the largest consumer of semiconductors in the world, it manufactures only about 30% of the chips it needs. In 2018, China's semiconductor consumption accounted for about 41% of the global total, which is predicted to rise to 57% by 2024. China spends more to import semiconductors that analyze data than to import oil, according to a Deloitte analysis. Multinational corporations trying to assess and potentially enter the China semiconductor market can consider whether joint ventures, for example, may be a possible avenue in light of China’s efforts to seek technology independence and establish in-country production facilities.

\*\*\*\*\*

For China, technological independence is really about self-determination. In just the past several decades, it has steadily moved up the value chain in manufacturing and in technology, producing some of the world's largest, most advanced, and most imitated companies and products.

# Bilat CP

### 2AC – Bilateralism Fails

NATO’s interconnectivity means working outside of NATO is unresponsive to cyber threats

Klimburg 12 – Director of the GCSC Initiative and Secretariat, Director Cyber Policy and Resilience Program at The Hague Centre for Strategic Studies, and a former associate and former research fellow of the Science Technology and Public Policy Program and Cyber Security Project at the Harvard Kennedy School’s Belfer Center. Dr. Klimburg is also a nonresident senior fellow with the Atlantic Council, and an associate fellow at the Austrian Institute of European and Security Policy (Alexander Klimburg; "National Cyber Security Framework Manual"; NATO CCD COE; https://ccdcoe.org/uploads/2018/10/NCSFM\_0.pdf; Accessed 6-27-2022)//ILake-AZ

Digital communications are the backbone of society and, whilst they are a capability that NATO exploits for operational and administrative advantage, it is neither an environment that NATO, nor its Member States, can claim to control. The ability to collect, process and deliver vast amounts of data requires huge increases in military and bureaucratic efficiency. At the same time, all NATO nations need to work with the fact that their dependence on cyberspace, including the internet, is a major vulnerability and, unless invested in, will result in deteriorated overall resilience.571 NATO, the armed forces, International Organisations (IOs) and Non-Governmental Organisations (NGOs) that work with it expose themselves to known and unknown risks while operating in the digital domain. Business as usual for NATO includes the procurement and organisation of military capabilities, engaging in the political processes that support the operation and coherence of the North Atlantic Council, and the administration and control of the NATO command elements and forces assigned to NATO activities. It is a huge undertaking with operational, logistic, economic, political, technical, environmental and reputational risks.

The Alliance is inextricably linked to the digital domain and is faced with many threats that create problems for Member States since cyberspace is international by nature. The interconnectivity makes a weakness of one country a weakness in all, which means that states and organisations cannot deal effectively with cyber threats on their own.

# AT – Security K

## 1AR – Link

Our threat construction is real – Putin’s own words draw a pattern of Russian revisionism

Serhan 22 – (Yasmeen Serhan; "Who is Vladimir Putin’s Revisionist History For?"; Atlantic; https://www.theatlantic.com/international/archive/2022/02/putin-russia-ukraine-revisionist-history/622936/; 2-27-2022, Accessed 6-25-2022)//ILake-AZ

To paraphrase one of Barack Obama’s favorite phrases, the arc of history is long, but it bends toward justice. Were Vladimir Putin to offer his own rendition of these words, it would probably go something along the lines of: The arc of history is long, but it bends backwards.

This, at least, appeared to be the thrust of the Russian president’s message this week when he offered a rambling and ahistorical speech dismissing Ukraine’s right to exist and then days later announced Moscow’s intent to invade the country in order to “demilitarize and denazify Ukraine.” In his telling, if Ukraine had once been part of the Soviet sphere, it should be part of Russia. And just as Russia defeated the Nazi regime in Germany, it would do so again—this time in Kyiv.

Putin is not the only world leader who has harkened back to an ahistorical past to justify his decisions in the present. Right-wing nationalists around the world have sought to portray themselves as the primary defenders of a glorious past that their enemies would seek to deny or forget. By whitewashing uncomfortable legacies and seeking to cultivate a politics of historic grievance, Putin has attempted the same. But in his justification for the invasion of Ukraine, Putin’s ahistoricism has bordered on delusion. Whether the Russian people or the rest of the world share in it, for now, appears to be immaterial: If there’s one audience this revisionist history is designed for, it’s Putin himself.

The evolution of Putin’s historical revisionism can be seen throughout his public statements over the years. In 2005, he famously described the collapse of the Soviet Union as the greatest geopolitical catastrophe of the 20th century. Two years later, Putin bemoaned the aftermath of the Soviet era and the pernicious, unipolar world—one led not by Moscow, but by Washington—that it had created. Last year, in perhaps the clearest articulation of his worldview, Putin said that Ukrainians and Russians are “one people—a single whole.” On Monday, he took that sentiment even further, declaring Ukraine to be “an inalienable part of our own history, culture, and spiritual space” whose independence was a product not of self-determination (Ukrainians resoundingly voted in favor of independence from the Soviet Union in a 1991 referendum), but rather “a mistake.”

Unlike his 2014 address announcing Moscow’s annexation of Crimea, which was largely framed as a moment of celebration, this was an angry speech—one ostensibly designed to make Russia’s people angry too, and to justify what was to come. “In territories adjacent to Russia, which I have to note is our historical land, a hostile ‘anti-Russia’ is taking shape,” Putin said in another address ahead of the invasion. “For our country, it is a matter of life and death, a matter of our historical future as a nation.”

It’s hard to know what Putin means by historical future (which is, on its face, an oxymoron), though we can take an educated guess. When Putin speaks of Russia today, he speaks of a country whose greatness is defined by its past—namely, its imperial history and its victory during World War II—which he believes must guide its present. “Putin weaponized history by giving it a function,” Orysia Lutsevych, the head of the Ukraine Forum at the London-based Chatham House think tank, told me. As far as the Russian president is concerned, “history is the fortune teller of the future.”

Such historical narratives can be compelling, especially when they elicit the kind of nostalgic nationalism that has proved potent elsewhere, including in the United States (where Donald Trump’s Republican Party has dubbed itself the defender of “patriotic education”), India (where Hindu nationalists have appealed to pride in India’s past to undermine its secular present), and Hungary (where Prime Minister Viktor Orbán often invokes the territories the country lost after the First World War). “Putin is not the only person who is old enough to have felt that sense of deep, personalized humiliation and shame that came with the loss of power of the Soviet Union at the end of the Cold War,” Keir Giles, the author of ​​Moscow Rules: What Drives Russia to Confront the West, told me. “Anything that reasserts Russia as that great power with a greater status than others and the right to a global presence and global influence in others’ affairs will be popular in those sectors of the Russian population.”

Still, it’s difficult to gauge just how big that sector is or how pervasive the narrative has been among those who don’t share Putin’s semi-mythological view of history. A recent CNN poll, published the day before the start of Moscow’s military invasion of Ukraine, found that though roughly half of Russians support using military force to prevent Ukraine from joining NATO, only 36 percent support doing so as a means of forcing a reunification of the two countries. The lack of support for the latter was most clearly evidenced by anti-war protests that have broken out across Russian cities.

When I spoke with Denis Volkov, the director of the Moscow-based Levada Center, Russia’s last independent pollster, in early February, he told me that though the majority of Russians fear war, few would feel comfortable voicing opposition to it if it came due to fear of reprisals. Indeed, more than 1,700 arrests have already been made. Besides, Volkov said, “public opinion will be no limit to the Russian government.”

Though Putin may feel obliged to justify his war of choice to the Russian people, who with Ukrainians will share the costs of a bloody and drawn-out conflict, his revisionist history is designed to appeal to no one more so than himself. By restoring Russia’s control over its former territories, Putin not only corrects what he sees as a historic wrong but also cements his place in Russian history as the leader who restored the country to its rightful status.