# \*\*1ac modules\*\*

## Resiliency Aff

### Specific Solvency module – cyber exercises

#### Thus the plan - The United States should increase security cooperation with North Atlantic Treaty Organization by expanding military to military cyber exercises.

#### \*\* NATO ahead on tech now – gap closing with Russia, China and non-state actors. NATO investment in tech capacity and innovation necessary to keep gap in capabilities

Magula and Alvarez-Couceiro, 21

[Justin, Army Strategist serving in the Strategic Landpower and Futures Group at the U.S. Army War College, and Paula, graduate of Strategic Studies at the Johns Hopkins University School of Advanced International Studies, "Mainaining and Improving NATO's Technological Edge", Wavell Room, 9/30/21, https://wavellroom.com/2021/09/30/maintaining-improving-natos-technological-edge-technology/, accessed 7/4/22, GDI-cc]

What happens when an alliance’s competitors quickly improve their technology and capabilities to place the alliance at increased risk? The North Atlantic Treaty Organization (NATO) addressed this dilemma during a recent summit in Brussels.  At the summit, the North Atlantic Council built upon[NATO’s 2030 strategic outline](https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf) and presented targets for increased technological collaboration to counter growing threats from Russia, China, and non-state actors. While NATO’s scientific and technical superiority has historically allowed it to outpace competitors, its adversaries are quickly closing the gap.

NATO members still hold advantages in their development of [new technologies](http://wavellroom.com/podcast/technology-and-the-future-of-land-warfare/). According to the Global Innovation Index, seven of the top ten[most innovative countries](https://knowledge.insead.edu/entrepreneurship/the-worlds-most-innovative-countries-2020-15076) globally are part of NATO, while the other three are key NATO partners. Even so, NATO can do more to harness the alliance’s combined technological prowess to better compete and win in a future conflict. As China seeks to become the[world’s innovation leader](https://www.businesschief.asia/leadership-and-strategy/china-aims-be-global-innovation-leaders-next-15-years) and Russia continues to undermine the alliance’s security, NATO will need to out-innovate its competitors and prepare for an uncertain future.

Four areas where NATO can focus on improving its competitive edge are developing its formal organizations, increasing public and private sector collaboration, harnessing and countering Emerging Disruptive Technologies (EDTs), and improving conventional military equipment. NATO must maintain its relative lead in technology sectors to defend its people and enhance its long-term strategic position. Improving science and technology (S&T) innovation will increase alliance collaboration, strengthen public and private sector cooperation, counter hybrid threats, deter adversaries, and harden defenses against attacks. NATO’s effectiveness in the future will heavily depend on its ability to maintain and improve its science and technology capabilities.

#### Cyber exercises key in establishing a resilient society in an age of cyber threats – they build awareness and test responses

**Gafic et al, 2022**

[Melisa, Junior Researcher in the Department of Computer Science and Security at the St. Polten University of Applied Sciences, “Cyber Exercises in Computer Science Education”, ICISSP, Proceedings of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022) https://www.scitepress.org/Papers/2022/108458/108458.pdf, accessed 7/1/22, GDI-CC]

During COVID 19-crisis the security and resilience of critical information system have been more important than ever before. Breaches and cyber security incidents impressively highlighted the importance of cyber security and especially incident response (ENISA, 2020). In order to ensure resilience of systems, and to prepare for a such unpredictable cyber threats, it is necessary to continuously train people how to purposefully react on these threats and to communicate within the team under difficult circumstances (Wilhemson and Svensson, 2014). Therefore, exercises especially cyber exercises, play a central role in establishing a resilient society.

Cyber exercises have gained a lot of attention throughout recent years, especially in the cyber security sector, as an important tool for security training, awareness-building and testing incident response. The EU emphasizes the importance of this field in its strategy for the digital decade (European Commission, 2020). Large exercises, that make it to the news, such as CyberStorm (Cybersecurity & Infrastructure Security Agency (CISA), ), Locked Shields (The NATO Cooperative Cyber Defence Centre of Excellence, 2021) or Cyber Europe (ENISA, 2021), represent only a small fraction of the exercises carried out. Conducting cyber exercises also has an educational value. Through interactive activities, such as simulations and scenarios, exercise participants apply knowledge in practical situations using techniques and tools they are familiar with, thereby deepening their understanding of a particular type of incident (Dewar, 2018).

#### \*Supreme Allied Commander Europe and NAC should increase cyber exercises

**Ahlawat, 2021**

[Urjasvi, Jindal School of International Affairs and Research Intern at the Centre for Security Studies, “NATO: CYBERSECURITY AND CYBER COALITION“CSS ISSUE BRIEF, January 2021, https://jgu.s3.ap-south-1.amazonaws.com/jsia/Urjasvi+-+NATO+Cybersecurity.pdf accessed jcp-tm 6/9]

FUTURE: ACTIONS TO STRENGTHEN CYBERSECURITY

As the Cyber Coalition demonstrates the actions taken by NATO, this segment will further elaborate on more aspects that can be covered in the aforementioned exercises. The core of NATO cybersecurity efforts lies at the member-state level.7 The size and severity of today's cyber-attacks involve a new approach to political, military, and civilian responses. NATO should take a few effective steps in the organisation to establish a quick decision-making mechanism while confronting a cyber-attack. The solution towards more secure cyberspace lies in the functioning and accountability of member states; currently, no mechanism exists to ensure that the member states are adhering to the Cyber Defence Pledge taken in the Warsaw Summit of 2016. NATO can discuss and provide expertise, however, there is no apparatus to enforce that expertise on the member, and the efficiency of the cyber defence efforts depend on the implementation by the members.

The first action can be taken concerning the decision making of NATO, which is divided into NATO as an organisation and its members. In the former aspect, the resource allocation to NATO should be increased as it will help in not only detecting and indicating hostile cyber activities but will allow better use of the civil and military intelligence units. Furthermore, **the powers of the Supreme Allied Commander Europe should be increased by the North Atlantic Council, along with which the CCDCoE should increase cyber defence activities and exercises as it will increase efficiency**. The focus of these exercises should be on dynamic and challenging cyber crisis-conflict situations, fast decision-making processes. Concerning the members’ role, identifying and sharing information about any potential threats to any of the members should be shared; the national intelligence services should supply and exchange such information. Allies and willing partners should continue to work on improving and updating threat assessments, and facilitating closer intelligence cooperation.8 Cyber challenges arrive in the form of networks and to defeat these threats involves an equally well-organized network of multinational and cross-sector collaboration. CC20 did deal with the aspect of decision making, however, as explained above, this aspect has a greater potential to secure the member states of NATO from the cyber threats.

## Space adv –resiliency aff

### Notes

#### You could read this advantage with either preinstitute resiliency mechanism, military to military exercises [general] OR mil to mil – offensive weapons solvency mechanism

### Space advantage

#### Threats in increasing – number and scope of cyber attacks becoming the norm for targeted space based infrastructure

**Tepper**, research coordinator and lecturer for space governance at Laval University, **2022**

(Eytan, “The First Space-Cyber War and the Need for New Regimes and Policies,” Center for International Governance Innovation, Policy Brief No. 173, May 2022, https://practicesource.com/wp-content/uploads/2022/05/apo-nid317939.pdf, accessed 7/4/2022, gdi-tmur)

\*GPS = Global Positioning System

Space-based infrastructure is a critical infrastructure for security and the economy — in fact, it is critical to most aspects of modern life — and therefore is a prime target for malicious attacks (Falco 2019). The most significant current security threat to space-based infrastructure and applications is from cyberattacks. Only a handful of countries have the capabilities to physically destroy satellites (Weeden and Samson 2022) — and they are likely to be exposed as the perpetrators. In contrast, executing a cyberattack requires much less in terms of funds and technological and engineering capabilities. Moreover, the attacker can attempt to cover its tracks, leaving the attacked country uncertain about attribution and its own response. Therefore, cyberattacks are likely to become the leading method of targeting space-based infrastructure for state actors, as well as non-state actors, notably criminal organizations and terrorist groups. There is evidence that such attacks have already occurred: Russia allegedly disrupted Global Positioning System (GPS) signals during North Atlantic Treaty Organization exercises in Finland, Sweden and Norway in 2018 (Harrison et al. 2020), affecting, inter alia, the ability of commercial aircrafts to navigate; Turla, a Russian criminal gang, allegedly hijacked satellite IP (Internet Protocol) addresses (Zetter 2015), which it later used to steal data; and Hamas of Gaza, a terrorist organization, hacked the satellite broadcast of a major Israeli television channel (Leyden 2014). A cyberattack targeting space assets, or space-cyberattack, can jam GPS signals, disabling navigation, or spoof GPS signals, providing misleading locations, in both cases disrupting travel and guided weapons systems. A space-cyberattack can “blind” remote sensing satellites that provide satellite imagery and other data collected by various sensors. It can interrupt communication satellites services, including television, radio and internet. Moreover, it can disrupt banking and payment systems, including the use of credit cards and automated banking machines, which rely on satellite-based precise timing. Indeed, important segments of the global financial system depend on GPS (Fernholz 2017). Further, a space-cyberattack can do more than render a satellite defunct: it can turn it into a weapon, for example, by taking control of it and altering its course so that it crashes into another satellite. Indeed, the combined space-cyber warfare theatre will be the primary battlefield for global powers in the twenty-first century (Boucher 2013). Accordingly, a report published by Harvard’s Belfer Center for Science and International Affairs suggested that the first mission of the new US Space Force should be to ensure cybersecurity of space assets (Falco 2018). In a signal on the future of warfare, the head of the US Indo-Pacific Command, Admiral John Aquilino, recently noted, “We’ve come a long way in a short time to be able to integrate the space and cyber domains” (quoted in Sevastopulo 2022).

#### \*NATO needs a more proactive policy toward cyber security of space assets – Russia and China are deploying offensive tech

\*consistent with OCO version of the aff

Unal 19 [Beyza, senior research fellow with the International Security Department at Chatham House, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, “Cybersecurity of NATO’s Space-based Strategic Assets,” Chatham House Research Paper, July, <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>, accessed 07/04/22, GDI-JCR]

Cyber research is a fast-moving and constantly evolving area of science, and the scope of cyberthreats that countries face is on the rise as malicious actors find new ways to infiltrate weapons systems. The use of electronic warfare methods and cyberattacks in peacetime illustrates the blurred lines of engagement between nations even in the absence of conflict. According to Norwegian military and NATO officials, Russia persistently jammed civilian GPS signals during NATO’s 2018 Trident Juncture exercise in Europe’s High North region, which highlights the growing threat. In November 2018, NATO Secretary-General Jens Stoltenberg stated that electronic warfare and cyberattacks were increasingly being used in operations.14 It was also reported that NATO officials believed Russia is testing this capability through its large-scale exercises, such as Zapad 2017, which was conducted jointly with Belarus in September 2017.15 According to the Consultative Committee for Space Data Systems (CCSDS), the most common cyberthreats to the space segment, ground segment and space-link communication segment include data corruption/modification; ground system loss; interception of data; jamming; denial of service; masquerade (spoofing); replay; software threats; and unauthorized access.16 There is also crossover between offensive and defensive activities in cyberspace and space, given that – technologically – offence is easier and more cost-effective than defence.17 Furthermore, space-related personnel are vulnerable to cyberthreats. Social engineering is becoming an important tool when used by adversaries, and – whether it occurs deliberately or unwittingly – the potential for people to constitute the weakest link in cyber defence is an increasing reality.18 The nature of cyber activities must evolve from being purely defensive to include active, persistent engagement, in order to disrupt attackers of western critical space-based capabilities. Given the importance of space-based systems to critical infrastructure that supports NATO military capabilities, it would be prudent to assume that an adversary is already active in these networks and focus on resilience measures. This increases urgency for advanced techniques, such as AI and machine learning (ML),19 to identify and respond to modern threats. Both China and Russia prioritize electronic warfare, cyberattacks and superiority within the electromagnetic battlespace as part of a strategy to achieve victory in future operations. Available doctrine from these nations highlights a key focus on preventing adversarial satellite-based communication systems from impacting their operational effectiveness20 – a focus shared in US military planning and policy.21 Russian space capabilities and their cybertechnologies pose particular threats to NATO. For its navigational system, Russia relies on its own satellite system GLONASS (Global Navigation Satellite System), rather than the US-provided GPS or the EU’s Galileo system. As part of a series of improvements to its communications technology and GLONASS, Russia is designing new navigation satellites, which are claimed to be highly accurate and longer lasting.22 Russia has been testing its capabilities in a hybrid context in Syria and in Ukraine, particularly relying on capabilities for jamming GPS signals to ground remotely piloted aircraft. It is reported to have conducted denial-of-service attacks on radio and telephone equipment, and to have attempted to steal encrypted military data.23

#### Cyber vulnerability of NATO space assets risks crushing NATO’s military capabilities and deterrence – only fostering cooperation on cyber security can solve deterrence

Lumiste 19 [Liina, International Law Researcher for the NATO Comparative Cyber Defence Centre of Excellence, “Chatham House report: Space – NATO cyber security’s weak spot,” <https://ccdcoe.org/library/publications/chatham-house-report-space-nato-cyber-securitys-weak-spot/>, accessed 07/04/22, GDI-JCR]

In 2018, Norwegian military and allied officials confirmed that Russia had disrupted NATO’s Trident Juncture exercise in Europe’s High North region by persistently jamming GPS signals during the exercise. China has claimed ‘the ability to use space-based systems and to deny them to adversaries as central to modern warfare’. As the dependence of military operations on space-based assets has increased exponentially over the last few decades and space-based assets are potential targets for cyber attack, the newly released Chatham House research paper ‘Cybersecurity of NATO’s Space-based Strategic Assets‘ suggests that NATO should bring space more to the spotlight. The research paper lists cyber threats to space-based strategic assets and capabilities, analyses capability requirements and gives concrete recommendations for ways improve the resilience of the space-based systems. Space-based assets as targets for cyber attacks Strategic military systems depend on space-based assets for the provision of data and for many capabilities, such as positioning, navigation and timing (PNT), intelligence, surveillance and reconnaissance (ISR), missile defence, communications, space situational awareness (SSA) as well as environmental monitoring. For accurate timing and navigation in PNT systems, NATO uses the global positioning system (GPS) which is also well known and widespread in civil use. ISR information and imagery is collected through surveillance and reconnaissance sensors. Both systems are satellite-based. Unmanned aerial vehicle (UAV) systems also rely on satellite-based ‘beyond-line-of-sight’ communication. These are only a few of the possible examples. In addition to the abundance of capabilities, it is noteworthy that the capabilities are also linked and therefore affecting one capability may cause collateral effects on others. As explained in the Space Threat Assessment 2018 published by the Centre for Strategic and International Studies (CSIS), there are several intrusion points for space-based assets: antennas on satellites and ground stations, landlines that connect ground stations to terrestrial networks, and user terminals that connect to satellites. This can result in data or data traffic monitoring, inserting false or corrupted data in the system, or even the permanent loss of a satellite. As with every other technology, people have the potential to be the weakest link in the cyber defence of space-based assets – social engineering is an important tool for the adversary. Vulnerabilities The research paper highlights some of the most important vulnerabilities: use of commercial companies; ‘back-doors’; dual use of satellites; and supply chain security of space technology. Chatham House reports have touched on these topics before. The question of supply chain was raised in the Livingstone and Lewis 2016 report, which observed that there was no coherent global organisation with regard to cyber security in space and that existing approaches had only limited reach into the supply chain. In this year’s research paper, it is again stressed that when the supply chain does not ensure that military security standards are met, items procured may expose NATO systems to vulnerabilities. NATO by itself does not own satellites, but is dependent on member states. In case of need, NATO requests access to products and services from the allies. NATO allies procure equipment and software, which will be integrated into their national defence infrastructure. In most cases, military and commercial assets are not separate. Therefore, NATO does not rely only on military assets, but also uses commercial, civilian and national or multinational assets for operations. Even though commercial methods have proven to be effective, they are accompanied by the inherent risk of lower security requirements. Data exchange between civil and military sectors may cause extra vulnerabilities. As most of the space-based capabilities are dual-use, meaning that assets are used both for military and civilian purposes, the Chatham House research paper recommends that operators ‘apply higher-grade military hardening and cyber protection specifications to civilian capabilities that have the potential to be used in support of military applications’. The research paper also highlights the aspect of NATO’s dependency on member states for communication capacity as a possible source of vulnerabilities. NATO owns satellite communications (SATCOM) ground stations, but no satellites; it is therefore highly reliant on allies to provide space-sourced data, information and services. In addition, ensuring the security of space capabilities is mostly in the hands of the allies. This puts NATO into a position where its main option to protect capabilities of vital importance is to encourage allies to put effort into securing the space-based assets and foster cooperation in space-based systems cyber security. Space as a domain of operations? During the Brussels Summit in 2018, the Alliance recognised space as a ‘highly dynamic and rapidly evolving area, which is essential to a coherent Alliance deterrence and defence posture’ and on 27 June 2019, it approved new space policy. As claimed by NATO’s Secretary General, Jens Stoltenberg, the space policy gives guidance on opportunities and challenges and is not about militarising space, but about information sharing and increasing interoperability. The research paper suggests that, in addition to policy, NATO needs to agree upon space doctrine. While policy directs, assigns tasks and prescribes desired capabilities, doctrine provides principles of how operations should be planned, prepared, commanded, conducted, sustained, terminated and assessed.1 This suggestion becomes even more relevant when taking into consideration recent announcements by some NATO diplomats about NATO’s aims to recognise space as a domain of warfare during the London summit at the end of 2019. This indeed would be a big step towards focusing more on space-based assets and their vulnerabilities. Considering the current context, in which China and Russia are increasing their presence in space, this action by NATO is inevitable. Whether or not NATO claims space as a domain, adversaries will nevertheless develop their aggressive capabilities, from cyber operations to anti-satellite missiles. Therefore, it is prudent to update the approach towards space and space-based assets to face new challenges. Yet, claiming space to be a domain of warfare highlights legal considerations. The Chatham House research paper raises a question from the cyber perspective: whether a cyber attack on a space system has to have kinetic consequences in order to give grounds for collective self-defence according to the Washington Treaty. This can be supplemented with a question on whether causing kinetic consequences that result in debris breaches the responsibility not to cause widespread, long-term and severe damage to the natural environment, as stipulated in article 35 of Additional Protocol I to the Geneva Conventions of 12 August 1949.2 Another question raised is targeting dual-use space technology in international humanitarian law (IHL). The principle of distinction foresees the duty to distinguish between the civilian population and combatants and between civil and military objects. As in the case of cyber objectives,3 dual-use satellites should be counted as military objectives, but would be subject to the rule of proportionality and requirement to take precautions in attack.4 Conclusion The Chatham House research paper makes recommendations that more or less all stress the same things: NATO is highly dependent on space capabilities; space-based systems are vulnerable to cyber attacks and will become more and more appetising targets for adversaries; and NATO must foster cooperation and information sharing between member states. Overlooking these aspects could undermine the credibility of the information provided through the space-based systems, which would in turn affect deterrence and strategic liability. In the broader view, destabilising space-based assets would not only affect military conduct, but also have severe effects on civil infrastructures.

#### Specifically, Risk of cyber escalation in space with Russia is massive and goes nuclear – prioritize this impact because cognitive bias underestimates it

Beebe 19 [George, VP and Director of Studies at the Center for the National Interest, a nonpartisan think tank, former head of Russia analysis at the CIA, “We’re More at Risk of Nuclear War With Russia Than We Think,” October 7, *Politico*, <https://www.politico.com/magazine/story/2019/10/07/were-more-at-risk-of-nuclear-war-with-russia-than-we-think-229436>, accessed 07/04/22, GDI-JCR]

Today, that old dread of disaster has all but disappeared, as have the systems that helped preclude it. But the actual threat of nuclear catastrophe is much greater than we realize. Diplomacy and a desire for global peace have given way to complacency and a false sense of security that nuclear escalation is outside the realm of possibility. That leaves us unprepared for—and highly vulnerable to—a nuclear attack from Russia. The most recent sign of American complacency was the death, a few weeks ago, of the Intermediate-Range Nuclear Forces Treaty—a pivotal 1987 agreement that introduced intrusive on-site inspection provisions, destroyed an entire class of dangerous weaponry, and convinced both Washington and Moscow that the other wanted strategic stability more than strategic advantage. The New START treaty, put in place during the Obama administration, appears headed for a similar fate in 2021. In fact, nearly all the key U.S.-Russian arms control and confidence-building provisions of the Cold War era are dead or on life support, with little effort underway to update or replace them. Meanwhile, U.S. officials from both parties are focused not on how we might avoid nuclear catastrophe but on showing how tough they can look against a revanchist Russia and its leader, Vladimir Putin. Summit meetings between White House and Kremlin leaders, once viewed as opportunities for peace, are now seen as dangerous temptations to indulge in Munich-style appeasement, the cardinal sin of statecraft. American policymakers worry more about “going wobbly,” as Margaret Thatcher once put it, than about a march of folly into inadvertent war. President Donald Trump’s suggestion that the United States and Russia might explore ways to manage their differences diplomatically has produced mostly head-scratching and condemnation. In my more than 25 years of government experience working on Russia matters, I’ve seen that three misguided assumptions underlie how the United States got to this point. The first is that American policymakers think that because neither side wants nuclear war, then such a war is very unlikely to occur. Russia would be foolish, we reason, to cross swords with the powerful U.S. military and risk its own self-destruction, and many Americans find it hard to imagine that modern cyber duels, proxy battles, information operations and economic warfare might somehow erupt into direct nuclear attacks. If the Cold War ended peacefully, the thinking goes, why should America worry that a new shadow war with a much less formidable Russia will end any differently? But wars do not always begin by design. Just as they did in 1914, a vicious circle of clashing geopolitical ambitions, distorted perceptions of each other’s intent, new and poorly understood technologies, and disappearing rules of the game could combine to produce a disaster that neither side wants nor expects. In fact, cyber technologies, artificial intelligence, advanced hypersonic weapons delivery systems and antisatellite weaponry are making the U.S.-Russian shadow war much more complex and dangerous than the old Cold War competition. They are blurring traditional lines between espionage and warfare, entangling nuclear and conventional weaponry, and erasing old distinctions between offensive and defensive operations. Whereas the development of nuclear weaponry in the Cold War produced the concept of mutually assured destruction and had a restraining effect, in the cyber arena, playing offense is increasingly seen as the best defense. And in a highly connected world in which financial networks, commercial operations, media platforms, and nuclear command and control systems are all linked in some way, escalation from the cyber world into the physical domain is a serious danger. Cyber technology is also magnifying fears of our adversaries’ strategic intentions while prompting questions about whether warning systems can detect incoming attacks and whether weapons will fire when buttons are pushed. This makes containing a crisis that might arise between U.S. and Russian forces over Ukraine, Iran or anything else much more difficult. It is not hard to imagine a crisis scenario in which Russia cyber operators gain access to a satellite system that controls both U.S. conventional and nuclear weapons systems, leaving the American side uncertain about whether the intrusion is meant to gather information about U.S. war preparations or to disable our ability to conduct nuclear strikes. This could cause the U.S. president to wonder whether he faces an urgent “use it or lose it” nuclear launch decision. It doesn’t help that the lines of communication between the United States and Russia necessary for managing such situations are all but severed.

#### And, Attack on the Global Navigation Satellite System ripples across sectors, sparks panic

Cesari et al 21 [Laetitia, Consultant at the UN Institute for Disarmament Studies, “Space as NATO’s Operational Domain: The Case of the Cyber Threats against GNSS,” 72nd International Astronautical Congress (IAC), Dubai, United Arab Emirates, 25-29 October 2021, <https://spacegeneration.org/wp-content/uploads/2022/04/IAC-21E927x66298_Space-as-NATOs-Operational-Domain-The-Case-of-the-Cyberthreats-against-GNSS_Paper.pdf>, accessed 07/04/22, GDI-JCR]

The Global Positioning System was originally designed as a military system, to meet tactical and strategic needs on the battlefield, during the Cold War Era. The term traditionally refers to the North American global positioning system, or satellite positioning system, while GNSS refers to the International Multi-Constellation Satellite System. Therefore, GNSS as an umbrella term typically includes GPS, GLONASS, Baidu, Galileo, and any other constellation system. GNSS and GPS work together, however the GNSScompatible equipment can use navigational satellites from other networks beyond the GPS system, which is the main difference from GPS, and more satellites means increased receiver accuracy and reliability. The GNSS can be targeted by cyberattacks via the command connection or ground station, since an unencrypted command link can expose the satellite's capabilities to an opponent, or a ground station could be hacked directly, allowing the ground station to influence satellite control or data. The ITU, while recognizing that “Member States retain their entire freedom with regard to military radio installations” [44] these installations must, so far as possible, take measures to prevent harmful interference [45]. Therefore, when assessing the interference risks associated with conflict zones or planning military exercises, ITU invites Member States to consider that the use of satellite-based systems can potentially be impacted beyond that zone, and therefore, an enhanced civilmilitary coordination is required. NATO’s ballistic missile defence capability is being built around a command-and-control system that enables five key functions: planning, monitoring, informationsharing, interception and consequence management 12 . The security of the system relies on three key elements, confidentiality, integrity and availability. industrial security is paramount (inc also supply chains)” [2]. The consequences of cyber-attacks on space missions are aggravated because of component satellites’ augmented connectivity and use of Internet of Things (IoT) devices in contemporary space systems. The potential impacts of an attack on a communication satellite can endanger national security by generating widespread disruptions to communication channels, not only national level, but also across widespread geographies, cross countries, and cause panic. The attacker can infiltrate the network without being detected and remain undetected. Cyber threats may target different components of a space mission: the ground segment, the space segment, and the link segment. The vulnerabilities stem from the ground segments; mostly generated from network components and the receivers (which receive the data from the satellite). The threats may also target hardware of satellites in the supply chain, and compromise ground units at a later stage [46]. “Cyber vulnerabilities undermine confidence in the performance of strategic systems. As a result, rising uncertainty in information and analysis continues to impact the credibility of deterrence and strategic stability. Loss of trust in technology also has implications for determining the source of a malicious attack (attribution), strategic calculus in crisis decision-making and may increase the risk of misperception” [47] Ground stations - how can we prevent threats? Preventive method and time-based method. Previous attack on ISS. GNSS are specifically vulnerable to hostile cyber operations because of the very low power of their signals and services and constitute potential primary targets in future wars because of their importance not only for military operations, but also for critical national infrastructure and key economic sectors. Unlike physical attacks they are not likely to cause major damages to the satellite navigation system. Recent cyber operations against GNSS were jamming and spoofing [48] although other types of attacks such as hacking or eavesdropping of communications satellite systems, are also technically possible.

#### Disruption of the GNSS system would instantly destroy the global economy and gut virtually every critical infrastructure sector

Graff 18 edited for language [Garrett, editor-in-chief of Washingtonian magazine, instructor at Georgetown University in the Masers in Professional Studies, Journalism, and Public Relations program, former deputy national press secretary for Howard Dean’s presidential campaign, “The New Arms Race Threatening to Explode in Space,” *Wired*, 6/26/18, <https://www.wired.com/story/new-arms-race-threatening-to-explode-in-space/>, accessed 07/05/22]

For decades, America’s satellites had circled Earth at a largely safe remove from the vicissitudes of geopolitics. An informal global moratorium on the testing of anti-satellite weapons had held since 1985; the intervening decades had been a period of post–Cold War peace—and unquestioned American supremacy—high overhead. During those decades, satellites had become linchpins of the American military apparatus and the global economy. By 2007, ships at sea and warplanes in the air had grown reliant on instant satellite communications with ground stations thousands of miles away. Government forecasters relied on weather satellites; intelligence analysts relied on high-­resolution imagery to anticipate and track adversaries the world over. GPS had become perhaps the single most indispensable global system ever designed by humans—the infrastructure upon which the rest of the world’s infrastructure is based. (Fourteen of the 16 infrastructure sectors designated as critical by the Department of Homeland Security, like energy and financial services, rely on GPS for their operation.) Now, Shelton feared, all those satellites overhead had become so many huge, unarmored, billion-dollar sitting ducks. In the decade since China’s first successful anti-satellite missile test, Shelton’s premonition has largely come true: Everything has changed in space. A secretive, pitched arms race has opened up between the US, China, Russia, and, to a lesser extent, North Korea. The object of the race: to devise more and better ways to quickly cripple your adversary’s satellites. After decades of uncontested US supremacy, multinational cooperation, and a diplomatic consensus on reserving space for peaceful uses, military officials have begun referring to Earth’s orbit as a new “warfighting domain.” On the ground, the military is starting to retrain pilots, ship captains, and ground troops in fail-safe forms of navigation that don’t rely on GPS—like celestial navigation. The US military must relearn how to fight “unwired” and defend itself in space. “We knew how to do that, and somehow we forgot,” General John E. Hyten, the head of US Strategic Command, said in 2015. When former director of national intelligence James Clapper left office at the end of the Obama administration, he told me that the increasing sophistication of America’s adversaries in space was one of the top three strategic threats he worried about. Clapper’s successor, Dan Coats, warned last spring that “Russia and China remain committed to developing capabilities to challenge perceived adversaries in space, especially the United States.” Since he took office, President Trump has dropped numerous hints of the warnings he’s evidently getting from military and intelligence leaders. During a spring livestream with astronauts aboard the International Space Station, he alluded, obliquely and without context, to the “tremendous military applications in space.” And he has repeatedly floated the idea of creating a new branch of the armed forces specifically for celestial combat—culminating last week with a speech out-and-out ordering the Joint Chiefs of Staff to begin developing plans for a new “Space Force.” But if space is indeed becoming a war-­fighting domain, it’s important to understand the stakes, not just for America’s strategic standing but for the species. A Russo-Sino-American space war could very well end with a ~~crippled~~ [wrecked] global economy, inoperable infrastructure, and a planet shrouded by the orbiting fragments of pulverized satellites—which, by the way, could hinder us all on Earth until we figured out a way of cleaning them up. In the aftermath of such a conflict, it might be years before we could restore new constellations of satellites to orbit. Preparing for orbital war has fast become a priority of the US military, but the more urgent priority is figuring out how to prevent it. GROWING UP IN Oklahoma City, William Shelton dreamed of becoming a pilot. He got as far as the Air Force Academy before he discovered his eyes weren’t good enough. So instead he became an astronomical engineer. In 1976 he began serving as a launch facility manager at Vandenberg Air Force Base, the military’s oldest space and missile launch base, perched on the California coast north of Santa Barbara. He arrived just as the Air Force was beginning to understand how crucial space would be to its future: The nation’s first early-warning satellites had been put in orbit with the intention of tracking Soviet missile launches, and satellite imagery was becoming increasingly critical to intelligence gathering. Shelton’s poor eyesight, it turned out, had led him to the center of the Air Force’s new frontier. In August 1990, Shelton, then a young lieutenant colonel, took command of the 2nd Space Operations Squadron in Colorado. When he arrived at his post, the Air Force was busy building a new constellation of satellites—launching new ones from Cape Canaveral in Florida every few months to help fill out what he was told would ultimately be a global system aimed at helping the US improve its navigation and increase the precision of its bombs and missiles. This was the new Global Positioning System, and one of Shelton’s first duties at “2Sops” was to build support and enthusiasm for the new effort. To impress visitors (including the brass), he carried around a demo GPS unit that weighed 10 pounds, cost $3,000, and could tell America’s soldiers, sailors, airmen, and Marines exactly where they were on the surface of the planet. The power of the new system that 2Sops ran was proven faster than anyone imagined. The Gulf War caused a rush of final preparations to get GPS ready for battle. Around 2:30 am on January 17, 1991, GPS-equipped helicopters snuck into Iraq, using the technology to guide themselves through the darkened desert and knock out air defense radars. The first bombing campaign of the war had begun. Reporters marveled at precision-­guided bombs zeroing in on their targets and cruise missiles appearing to turn street corners to hit the right buildings. Shelton had a front-row seat to this transformation. As the technology has improved, so has the precision of GPS. The system originally provided accuracy to within 17 yards; with it, you could pinpoint a specific copse of pine trees. Today, if you’re using a smartphone, it can generally locate an object to within five yards—a resolution fine enough to locate a pair of pine trees within that copse. Soon it could be able to zero in on a pine cone: Research from UC Riverside has demonstrated that the latest tech is reliable to within an inch. And research has shown that 1-millimeter accuracy might be eventually possible—which means that the system could locate an individual seed inside that pine cone. Today, troops on the ground use GPS to navigate foreign streets; drone pilots can program a flight plan from thousands of miles away. And because GPS satellites also house America’s detection system for nuclear detonations, we rely on them to tell us if North Korea launches a nuclear weapon, and to tell our missiles and bombs where to find their targets. “When you look at our American way of war, the strategy is largely underpinned by space assets—navigation, early warning, timing,” Shelton says. And that’s just the military. The creators of GPS probably never intended for the system to become the backbone of daily life, but it has. I visited Colorado while reporting this story and tried to keep tabs on everything I did that relied on GPS. There were the obvious navigational moments—my Uber ride to the airport, my American Airlines flight to Denver, my own Google Maps–guided drive in a rental car to Schriever Air Force Base, outside Colorado Springs. But there were also less obvious instances, like the phone calls I made along the way (cellular networks rely on GPS data to keep their stations synchronized), my stop at the ATM (banks use GPS to track deposits and withdrawals), and the fill-up at the gas station (the credit card system also relies on GPS). Moreover, GPS is no longer the world’s sole geolocating mechanism. Russia, China, and the European Union have now all either deployed or begun working on their own full constellations of navigation satellites, ensuring that they won’t have to rely on the US system. It also means that, in the early moments of a war, it’s a fair bet that satellites—the other guy’s satellites—could be among the first targets. DURING THE COLD War, a US army mountain outpost in the Fulda Gap, the shortest route between East and West Germany, served as an early warning trip wire for a Soviet invasion of Europe. If Russian tanks ever made a surprise attack, NATO planners knew that the soldiers there would likely be the first to find out. Today, the members of 2Sops play a similar role. Deep inside the squat, beige, windowless Building 400 at Schriever Air Force Base—the destination I had plugged into Google Maps during my trip to Colorado—10 people at a time remotely operate the heavenly constellation of GPS satellites that guide Tomahawk cruise missiles to their targets, deliver Lyft passengers to their destinations, and help farmers cultivate their crops. They also watch out for any shocks or attacks on the system. The average GPS operators are in their mid-twenties. During one recent shift, the entire Global Positioning System was being operated by two 19-year-old airmen (who, the Air Force emphasizes, are rigorously trained). Their commander, US Air Force lieutenant colonel Peter Norsky, is in his mid-thirties. Together, they watch over the roughly three dozen GPS satellites, troubleshooting the geolocation system and minding the quirks of each orbiting craft—this one’s damaged solar panels, that one’s balky communications links—as if they were remotely tending a stable full of temperamental horses. As integral as GPS is to daily life, the way it actually works is little understood by most people outside of Schriever Air Force Base. Fundamentally, the function of GPS is to provide the globe with a shared clock. GPS satellites allow phone companies to keep their systems in sync, battleships to chart open waters, and ATMs to time-stamp their transactions by triangulating signals from overhead and measuring how long it takes those signals from different satellites to reach a GPS receiver. The system works by making daily calculations, employing Newtonian physics and Einsteinian relativity, to minutely tweak the time broadcast from each GPS satellite as it moves through space—the high-tech version of tuning your grandfather clock to within 100-­billionths of a second. Time is, after all, relative; as of January, the time in space was 18 seconds ahead of Earth’s “Coordinated Universal Time,” since space doesn’t recognize the leap seconds that scientists add to terrestrial time to account for the planet’s slowing rotation. Additionally, the time-keeping device on each satellite gives a subtly different reading, the result of variations in their atomic clocks, which tell time by measuring the precise oscillations of an atom. (Some GPS satellites use rubidium atoms, which are highly accurate day to day; some use cesium, which is more accurate over long stretches.) Any malfunction in the GPS system threatens to plunge the global economy into chaos. Fortunately those glitches are rare, but they’re not unheard of. On January 25, 2016, one of 2Sops’ flight commanders, Captain Aaron Blain, was awoken by a call from work in the middle of the night. User reports from around the country suggested that the system’s precision had “wobbled,” making measurements increasingly inaccurate. Blain raced to Schriever in his Ford pickup and found that the constellation’s timing was off by about 13 microseconds. It was an infinitesimal number—over 25,000 times shorter than the blink of an eye—but for the finely tuned GPS it was a yawning crevice. Left uncorrected, the glitch could have ricocheted through the global economy, corrupting not just driving directions but stock trades too.

### Solvency module – space

#### Cyber exercises key in establishing a resilient society in an age of cyber threats – they build awareness and test responses

**Gafic et al, 2022**

[Melisa, Junior Researcher in the Department of Computer Science and Security at the St. Polten University of Applied Sciences, “Cyber Exercises in Computer Science Education”, ICISSP, Proceedings of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022) https://www.scitepress.org/Papers/2022/108458/108458.pdf, accessed 7/1/22, GDI-CC]

During COVID 19-crisis the security and resilience of critical information system have been more important than ever before. Breaches and cyber security incidents impressively highlighted the importance of cyber security and especially incident response (ENISA, 2020). In order to ensure resilience of systems, and to prepare for a such unpredictable cyber threats, it is necessary to continuously train people how to purposefully react on these threats and to communicate within the team under difficult circumstances (Wilhemson and Svensson, 2014). Therefore, exercises especially cyber exercises, play a central role in establishing a resilient society.

Cyber exercises have gained a lot of attention throughout recent years, especially in the cyber security sector, as an important tool for security training, awareness-building and testing incident response. The EU emphasizes the importance of this field in its strategy for the digital decade (European Commission, 2020). Large exercises, that make it to the news, such as CyberStorm (Cybersecurity & Infrastructure Security Agency (CISA), ), Locked Shields (The NATO Cooperative Cyber Defence Centre of Excellence, 2021) or Cyber Europe (ENISA, 2021), represent only a small fraction of the exercises carried out. Conducting cyber exercises also has an educational value. Through interactive activities, such as simulations and scenarios, exercise participants apply knowledge in practical situations using techniques and tools they are familiar with, thereby deepening their understanding of a particular type of incident (Dewar, 2018).

#### Specifically, Cooperative training exercises focusing on space needed to shore up NATO space cybersecurity

Unal 19 [Beyza, senior research fellow with the International Security Department at Chatham House, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, “Cybersecurity of NATO’s Space-based Strategic Assets,” Chatham House Research Paper, July, <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>, accessed 07/04/22, GDI-JCR]

Training is essential to create awareness and prepare the alliance for worst case scenarios. NATO could promote different types of training that would capture space security and system vulnerabilities to cyberattacks. Training areas could be selected through a lessons-learned analysis where former cases could be used to highlight areas of greatest need. Some examples are as follows: • At the political-strategic level, crisis management exercises (CMX), hybrid warfare exercises and similar training could incorporate cyber resilience and bring space elements into cybersecurity training. • At the technical level, given the complexity of space systems, focused training, modelling and simulation would be key to ensuring design integrity. • Bringing the technical and political communities together in training modules would be helpful. Often the political community and technical community do not metaphorically speak the same language and their concerns do not merge. Such training would be technology-driven and could incorporate modelling and simulation. Thus, technical expertise and knowledge could be transferred into political action plans. • Training may also involve the private sector or contractors. NATO decides whether or not it should delegate parts of the training to the private sector or to conduct it internally. There are advantages and disadvantages in both. One of the advantages in delegating the work to an outside party is that the latter could conduct an analysis without any NATO restrictions and could significantly test NATO’s planning and operations. The main disadvantage is that NATO may not be able to share classified information, which would make the training less comprehensive. • Some of the most useful training methods involve exercises, ‘war gaming’, crisis simulations and scenario planning, as well as online training education programmes, training manuals, and certifications. NATO should also measure the impact of the training and assess its skill-maintenance capacity.

#### And, Member states look to NATO when formulating national space security policy – there’s follow on to the plan for national assets

Unal 19 [Beyza, senior research fellow with the International Security Department at Chatham House, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, “Cybersecurity of NATO’s Space-based Strategic Assets,” Chatham House Research Paper, July, <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>, accessed 07/04/22, GDI-JCR]

If capabilities remain in national hands NATO’s role in the space realm should be considered. It could have the following functions: 1. Intelligence; 2. Creating dialogue with the space components industry; 3. Operational planning; and 4. Coordination/liaison with the allies on personnel requirements, in order to improve alliance knowledge and capacity on the use of space technology in NATO operations. In many areas, NATO allies that have either not invested in space technology or do not have sufficient capability to protect their systems, look to NATO as an informative entity that could guide them towards the best approach for space security. If NATO’s role in the space realm were to be clarified as discussed above, this could help those allies to perform their obligations.

## Supply chain adv –resiliency aff

### Notes

#### You could read this advantage with either preinstitute resiliency mechanism, military to military exercises [general] OR mil to mil – offensive weapons solvency mechanism

### Supply chain Advantage

#### Supply chain attacks have been small, but massive escalation is coming

Higgins 21 [Kelly, Executive Editor of Dark Reading, award-winning technology & business journalist, named one of the Top 10 Cybersecurity Journalists in the US by Onalytica, “Why Supply Chain Attacks Are Destined to Escalate,” 08/05/21, <https://www.darkreading.com/vulnerabilities---threats/why-supply-chain-attacks-are-destined-to-escalate/d/d-id/1341588>, accessed 07/04/22, GDI-JCR]

The epic software supply chain attacks over the past year, including the high-profile breaches of SolarWinds, Microsoft Exchange Server, Kaseya, and Codecov, were only the beginning. "Supply chain attacks are only just starting, and mostly with pretty small vendors that most people had not heard of beforehand," said Corellium COO Matt Tait, in a live conversation via video with Black Hat founder Jeff Moss. But what happens when these attacks get bigger and affect larger vendors and more of their customers? Tait – who also delivered the prerecorded keynote, which was streamed on multiple large screens in a ballroom at the Mandalay Bay Conference Center in Las Vegas yesterday – said in the live portion of the event that the relative impact of these high-profile attacks could have been much worse given they were mostly targeted. He warned there will be more and they could well wreak more extensive and widespread damage to more organizations if the attackers hit larger targets with massive customer bases, such as the recent theft of source code from gaming giant EA Games. "It's likely to start to escalate in the coming months and years," he said. "And when something really big happens ... everything else will look like complete peanuts" in comparison, he said. When a nation-state or cybercrime organization makes that leap and infiltrates more victims, it will no longer be a "sustainable" situation.

#### With supply chains stretched thin, disruption would be economically catastrophic – there’s zero buffer

Murray 22 [Brendan, Trade Tsar at Bloomberg LP, “Cyber Threat Adds Another Curveball to Shipping Outlook,” 2/15/22, <https://www.bloomberg.com/news/newsletters/2022-02-15/supply-chain-latest-cyber-risk-adds-curveball-to-shipping-outlook>, accessed 07/04/22, GDI-JCR]

Jensen recalled a major cyber event in 2017, when shipping giant Maersk was among thousands of companies that shut systems down to assess the data damage. The Copenhagen-based container carrier’s estimate of the cost was around $300 million. Back then, port operators were among those with the most tangible consequences. While goods were moved, the process was slowed as terminals reverted to manual or backup operations. Still, the global economy absorbed the shock without much wider damage. With supply chains stretched to their limits, that’s unlikely to be the case now. No Buffer “In 2017 we could essentially lose the largest carrier in the world for a week and it didn’t cause any major problems,” Jensen said. “Sure, if you had your cargo on board one of those ships it got delayed maybe a week or two and that was annoying, but from a global perspective it was a non-event in terms of disturbing the supply chain. There was plenty of buffer capacity — of ships, terminals, everything. Right now we have zero, as in literally zero, buffer capacity.” Four of the world’s top five container lines are headquartered in western and northern Europe, and at least one has been hit with a cyber attack since the start of the pandemic. Marseille, France-based CMA CGM said in September 2020 that a breach hit services and affected bookings. Days later, the International Maritime Organization, a United Nations agency that serves as the industry’s regulatory body, said it suffered “a sophisticated cyber attack” affecting its public website and internal systems. In mid-January, European Union governments took part in large-scale simulation of a cyber intrusion affecting multiple member countries. The six-week exercise was expected to model attacks on supply chains and some spillover socio-economic effects in other countries. “If they have done their jobs well, they have a good backup plan,” Jensen said. “In the current environment, taking just one major port out of action for two, three, four days on top of what we’re already dealing with — that will have major ramifications on the supply chain.”

#### And, NATO is central to the protection of global supply chains

Granger 22 [Euan, Materials & Supply Chain Manager at Soil Machine Dynamics Ltd, “The Role of NATO in Protecting our Supply Chains,” 05/17/22, <https://www.procurious.com/procurement-news/author/euan-granger>, accessed 07/04/22, GDI-JCR]

NATO plays an active role in global peacekeeping, has built up the concept of co-operative security, and is a deterrent for illegal and terrorist activities. And it is in this role that we see the link between its activities and its importance to global supply chains. Protecting the Supply Chain Current events such as the war in Ukraine and global COVID restrictions, as well as the ongoing threat of terrorist activity has highlighted the importance of stability and continuity in the supply chain. For example, while Ukraine may not be a member of NATO, the NATO countries are using integrated logistics and supply routes to move arms, vehicles and aid into the war zone. Through its actions in the past, as well as actions it is taking now and for the future, NATO is providing support and protection for global supply chains. Here are three key ways that demonstrate the importance of the organisation to the global community: 1. Protection of Key Infrastructure – Energy Security Energy and key utilities, such as oil and gas, are critical for almost every aspect of global supply chains. Disruption to sources or supplies of energy could easily undermine the security of countries and continents, leading to situations where global production is halted, and supply of everything from electronic components to food and drink is disrupted. Vulnerabilities exist not only in infrastructure (oil/gas pipelines; power stations), but also in the systems used to control and manage them, especially in light of the increasing threat of cyber attacks. NATO members have been working since 2008 on energy security programs to help protect key infrastructure and ensure continuity of supply for both nations and the military. 2. Counter Piracy Operations and Protection of Sea Lanes Piracy continues to be a major threat to supply chains and freight in key shipping lanes around the world. While it would seem that the threat of piracy has lessened due to fewer serious incidents reported in the press in recent years, it remains a problem for shipping companies. NATO has in the past assisted in operations such as Operation Shield, an international cooperation to combat piracy of the east coast of Africa. Though this operation has since ended, NATO continues to work with countries and global partners to assist further anti-piracy efforts. Without the protection that NATO affords in conjunction with national navies and governments, there is the potential for disruptions to ships and cargo that would have lasting impacts on global supply chains. 3. Crisis Management including Relief Supplies in event of Natural Disasters NATO plays a key role in crisis and disaster management, both within its member countries and outside of this region. For this, NATO actually forms part of the global supply chain, ensuring that aid, equipment and personnel are able to reach areas affected by natural disasters. This can take the form of physically shipping goods on behalf of its member nations, as well as ensuring that requests for assistance from members or other countries are conveyed to the correct areas of government. While we may not see the work that NATO does as part of, or to support, global supply chains, its importance cannot be overemphasised. Without its efforts since its inception over 70 years ago, the global supply chain would look very different to how it does now.

## OCOs –this is different from resiliency

### Notes

#### This version of the aff is separate from the adv above – and increases military exercises specifically for offensive cyber operations. The expansion neg file has neg – be sure to look under signaling and OCO for cards that turn the claims that OCOs de-escalate conflict. Part of the argument is also that the signals sent by OCOs will increase risk of escalation – AND that OCOs themselves may increase risk of escalation

#### The US unilateral cyber command policies on OCOs fail – and worsen trust issues/harms alliance cohesion pretty good – so make sure you review that section too

#### This 1ac is long – if you see a –in front of a tag, it means that you could probably remove the card/not read it and still have a coherent 1ac

### 1ac

#### Contention 1 – The Status Quo

#### -The status quo cyber-threat landscape remains complex, emerging as a theater for great-power conflict – multiple actors pose a threat in the gray zone to NATO countries

**Maigre, 2022**

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

Introduction What the war in Ukraine says about cyber power is yet not entirely cleared from the fog of war. Many aspects remain uncertain, but given the unpredictability of the Putin regime, the risk of an escalation in hostile cyber exchanges between Russia and NATO states remains high. What is clear is that, as of February 24, 2022, we live in a different world in which the European and global security orders have been shattered. This brief first explores the challenge that cyber threats pose to NATO allies and how the rapidly evolving cyber-threat landscape can alter the inter- national security environment. Secondly, it looks at developments in cyber defense policy within NATO. Finally, the brief analyzes how NATO needs to adapt to address cyber challenges, studying how allies align their sovereign interests, capabilities, and cyber doctrines with NATO operational requirements and strategic ambitions. NATO is set to issue strategic documents in 2022 that will guide the next decade of its military planning. This will certainly require more transatlantic consultation on political-military matters with an emphasis on cyber security and cyber defense. The Cyber Challenge to the World and NATO Allies Malicious cyber activity has increased substantially over the past years while the world has kept turning amid the omnipresent pandemic and now war in Ukraine. States, non-state actors, and criminal groups compete and are increasingly weaponizing sensitive information and infiltrating other countries’ networks to steal data, seed misinformation, or disrupt critical infrastructure. The coronavirus pandemic further complicated the cyber-threat landscape. In March 2020, attempts to mitigate the spread of the coronavirus led to social distancing measures, travel restrictions, and remote work. In a short span of time, IT security profes- sionals had to respond to the challenges of working from home, such as enterprise data movements when employees accessed cloud-based apps via their home internet, corporate software, videoconferencing, and file sharing.1 Even if hardware and software solutions were in place to secure the organization’s data, there were often no established policies to help employees wade through the jungle of threats and vulnerabilities they faced when moving their workplace out of the traditional office environment.2 According to the FireEye Mandiant Special Report: M-Trends 2021, the top five most targeted indus- tries in 2020 were business and professional services, retail and hospitality, finance, healthcare, and high technology. The main methods used were extortion, ransom demands, payment card theft, and illicit trans- fers. Direct financial gain was the likely motive for 36% of intrusions, and an additional 2% of intrusions were likely perpetrated to resell access. In 2021, data theft remained an important mission objective for threat actors; in 32% of intrusions, adversaries stole data.3 Currently, highly organized, technically proficient criminal syndicates comprise the most significant cyber threat to allies. These groups try to steal data or extort money through ransomware. In 2021, promi- nent ransomware attacks struck Colonial Pipeline, the operator of the largest fuel pipeline on the East Coast of the United States; JBS, the largest meat processing company in North America; and Coop, a major supermarket chain in Sweden. Healthcare was also targeted—in May of the same year, the entire health service system of Ireland was disrupted for weeks, and over the spring and summer, dozens of hospitals in Europe and the United States were locked out of life-critical systems by ransomware attacks.4 Another set of threats comes in the form of bellig- erent state actors that seek to steal sensitive data for espionage. In December 2020, Russian intelligence services infiltrated the digital systems run by US tech firm SolarWinds and inserted malware into its code. During the company’s next software update, the virus was inadvertently spread to about 18,000 clients, including large corporations, the Pentagon, the State Department, Homeland Security, the Treasury, and other US government agencies. The hack went unde- tected for months before the victims discovered vast amounts of their data had been stolen.5 There are also politically motivated cyberattacks mandated by states that interfere in democratic processes and political discourse. In September 2020, the internal email system of Norway’s parliament was hacked.6 Ine Eriksen Søreide, the Minister of Foreign Affairs of Norway, underlined the significance of the attack by calling it an important cyber incident that affected the “most important democratic institution” of the country.7 Norwegian authorities later identified Russia as the actor responsible for the attack, marking the first time that Norwegian authorities had made a political attribution to such an attack. Since the beginning of this year, Ukraine’s govern- ment has been hit by a series of cyberattacks that defaced government websites and wiped out the data on some government computers. In mid-Jan- uary, hackers defaced about 70 Ukrainian websites, including the Ministries of Foreign Affairs, Defense, Energy, Education, and Science, as well as the State Emergency Service and the Ministry of Digital Trans- formation, whose e-governance portal gives the Ukrainian public digital access to dozens of govern- ment services. The hackers replaced the home pages of about a dozen sites with a threatening message: “be afraid and expect worse.” After a couple of days,however, most of the sites were restored.8 The inter- national hacktivist collective Anonymous has declared “cyberwar” against Russia’s government, claiming credit for several cyber incidents including distrib- uted denial of service attacks that took down Russian government websites and Russia Today, the state- backed news service.9 Around the globe, aging critical infrastructure has long been vulnerable to attack. The most worrying type of cyberattack is sophis- ticated malware designed by states or state-backed actors that act as “time bombs” in the critical cyber networks of target countries, such as the energy, telecom, and transportation sectors. Around the globe, aging critical infrastructure has long been vulnerable to attack. In 2020, the UK’s National Cyber Security Centre issued a warning of Russian attacks on millions of routers, firewalls, and devices used by infrastruc- ture operators and government agencies.10 On the day of the Russian invasion, ViaSat, a provider of high-speed satellite broadband services, was hacked along with one of its satellites Ka-Sat, whose users included Ukraine’s armed forces, police, and intelligence service. Destructive wiper malware attacks by Russia against Ukraine included Whisper- Gate, discovered in January by Microsoft, in Ukraine’s networks that “provide critical executive branch or emergency response functions”;11 HermeticWizard and IsaacWiper,12 targeting multiple Ukrainian orga- nizations just hours before the Russian invasion began; and CaddyWiper, spotted by researchers at the Slovak internet security company ESET in mid-March.13 All of them were designed to wipe or overwrite critical files on infected systems and leave computer hard drives corrupted and unrecoverable. These incidents demonstrate that, in the words of cyber expert and Silverado Policy Accelerator think tank chairman Dmitri Alperovich, “Cyberattacks have become a theater for great-power conflict in which governments and militaries fight in the hybrid ‘gray zone,’ where the boundaries between peace and war are blurred.”14 The actors navigate a complex web of ambiguous and deeply interconnected challenges, where cyberattacks are not a separate front, but rather an extension of the conflict.

#### NATO doesn’t include offensive cyber effects in mission planning and contributions voluntary – despite state and non-state adversaries attacking NATO members

**Iftimie,** Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business**, 2020**

[Ion, “NATO’s needed offensive cyber capabilities” NDC POLICY BRIEF No. 10 – May 2020 <https://www.ndc.nato.int/news/news.php?icode=1441#:~:text=This%20Policy%20Brief%20looks%20at,cyber%20capabilities%20into%20its%20operations> accessed 7/5/22 GDI-TM]

NATO’s adversaries in the cyber domain

Warfare in the cyber domain is already conducted against NATO member states by both state and nonstate actors. It is also conducted by NATO member states against these external threats. Within the Alliance, however, **offensive cyber effects are not yet part of the mission planning process and integration of national offensive cyber capabilities into joint NATO operations is voluntary.** Integrating these national offensive cyber capabilities into NATO operations, thus requires, not only a clear understanding of these capabilities, but also agreement on the cyber threat environment, characterized by the intent and capabilities of NATO’s current and/or potential future adversaries. State adversaries in the cyber domain include Russia, China and/or Iran. These are countries known to be building offensive cyber capabilities specifically for the purpose of using them against NATO memberstates.7 In Russia’s case, cyber attacks were conducted against the critical infrastructure of NATO member states and partner nations, as for example against US energy infrastructure in 2017 (including against a nuclear powerplant near Burlington, Kansas)8 or against the Ukraine power grid in December 2015. China has also been conducting persistent cyber espionage using offensive cyber capabilities against core military and critical infrastructure of NATO member states for years. For this reason, the US Secretary of Defense, Mark T. Esper, remarked at the 2020 Munich Security Conference that the 5G Huawei infrastructure is a serious threat to NATO.9 Lastly, Iran’s offensive cyber capabilities have also been observed during multiple attacks against the critical infrastructure of NATO partner nations in the Middle East. NATO adversaries in the cyber domain also include non-state actors, such as terrorist organizations. The US and the UK have conducted several successful offensive cyber operations against those entities. These offensive cyber operations had a significant force multiplier effect, in conjunction with conventional actions on the ground, at sea, in the air and from space, that contributed to the defeat of Daesh in both Iraq and Syria.10 Today, most Allies are building offensive cyber capabilities needed to deny adversaries the freedom of maneuver in the cyber domain.

#### -And, despite national development of some offensive cyber capabilities, unilateral policies like US CyberCommand persistent engagement and defend forward cyber posture undermine NATO capacity and create distrust

**Smeets 2021**

(Max Smeets,, Max Smeets is Senior Researcher at the Center for Security Studies, Zurich; Director of the European Cyber Conflict Research Initiative; and an affiliate at Stanford's Center for International Security and Cooperation, “NATO allies’ offensive cyber policy: A growing divide?” THE FUTURE OF EUROPEAN STRATEGY IN A CHANGING GEOPOLITICAL ENVIRONMENT: CHALLENGES AND PROSPECTS edited  Michiel Foulon, and Jack Thompson Hague Centre for Strategic Studies, August 1st, 2021, JSTOR, GDI- TMK)

Steady progress

Member states agree on the critical need for a coherent cyber policy. Almost all NATO allies have developed both a cyber security strategy and a cyber defense strategy.1 Some states have published updated versions over the years to reaffirm cyber security as an issue of national security importance, to tweak institutional responsibilities, or to articulate changes in the threat landscape. In addition, since 2018, most NATO allies have established a military cyber organization (either a command or unit) with a mandate to conduct cyber effect operations – that is, cyber operations intended to disrupt, deny, degrade and/or destroy.2 There is also shared recognition that international law applies in cyberspace, although allies have yet to spell out the legal procedures for operating in this new “domain of warfare.”

These developments have been both reflected in, and aided by, policy progress made at the inter-governmental level. At the Prague Summit in 2002, NATO for the first time recognized that the Alliance should “Strengthen our capabilities to defend against cyber attacks.”3 In 2008, at the Bucharest Summit, there was another milestone development, when NATO adopted a “Policy on Cyber Defense,” aiming to “protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack.”4 In the same year, the Cooperative Cyber Defence Centre of Excellence – a NATO accredited international research institution – was established in Tallinn, Estonia. In 2016, at the Warsaw Summit, cyberspace was officially recognized as a “domain of operations” and allies made a Cyber Defense Pledge to enhance their cyber defenses.5 The 2018 Brussels Summit and 2020 London Summit reiterated NATO’s commitment to implement the Cyber Defense Pledge and operationalize the Cyber Operations Center, responsible for situational awareness and the centralized planning of cyber operations and missions.6 In January 2020, the Allied Joint Doctrine for Cyberspace Operations was published “to plan, execute and assess cyberspace operations (CO) in the context of allied joint operations.”7

Steady divergence

Yet when it comes to the direction of allies’ cyber policy, growing differences are apparent – especially in the development and deployment offensive cyber capabilities. First, even though most states now have – or are in the process of – establishing a cyber command, operational capabilities vastly differ across states.

Whereas some governments are increasingly allocating significant resources to conduct cyber operations – and are now starting to benefit from these investments – the majority of allies still run their cyber commands on a budget of a few million a year –an amount that is insufficient for effective operations in the cyber domain.

Secondly, until a few years ago, NATO members’ strategic visions were largely aligned. National cyber strategies shared a common threat focus on operations that could potentially cause major societal havoc, such as taking down the power grid. Allies’ national strategies were also largely unified in their vision to address this threat, discussing the need for deterrence, resilience, and norms. However, this changed with the publication of the US Department of Defense’s strategy on Defend Forward and US Cyber Command’s vision on Persistent Engagement.8 The United States emphasizes the need to cause friction “wherever the adversary maneuvers,” operating “globally, continuously and seamlessly” (potentially) below the threshold of armed attack. “We must…maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries,” in the words of NSA director and Cyber Command head Gen. Paul Nakasone.9 **Whereas deterrence is about changing your adversary’s cost-benefit calculus, Persistent Engagement is about taking the opportunity away from the adversary to act.10**

Third, NATO member positions on how international law applies – particularly the obligations of states vis-a-vis sovereignty – are now more divergent than a decade ago. Whereas countries like the Netherlands and France are located on the side of the “sovereignty as a rule” camp, the United Kingdom has taken the position that a remote cyber operation by one state into another’s cyber systems or network does not violate the latter’s sovereignty.

#### Thus the plan - The United States should increase security cooperation with North Atlantic Treaty Organization by expanding offensive cyber operations military to military exercises.

#### Advantage 1 - Cyber Threats

#### Failure to deter cyber threats through offensive operations results in two scenarios:

#### Scenario 1 – Critical infrastructure

#### Critical infrastructure attack risk nuclear meltdowns, blackouts and financial crises

**Iftimie,** Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business**, 2020**

[Ion, “NATO’s needed offensive cyber capabilities” NDC POLICY BRIEF No. 10 – May 2020 <https://www.ndc.nato.int/news/news.php?icode=1441#:~:text=This%20Policy%20Brief%20looks%20at,cyber%20capabilities%20into%20its%20operations> accessed 7/5/22 GDI-TM]

Cyber as a hybrid threat to, and enabler of, military operations

All future military confrontations are expected to be fought with cyber weapons. These offensive cyber capabilities in the hands of adversaries pose a significant threat to the military forces and critical infrastructure of NATO member states; and the Alliance recognizes that cyber-attacks (as hybrid threats) can be as damaging as conventional ones. This is because malicious cyber activities against computers that control physical processes can be as dangerous as threats that are purely physical in nature and could lead to explosions, nuclear meltdowns, blackouts, or financial crises. As put by NATO Secretary General, “in just minutes, a single cyberattack can inflict billions of dollars’ worth of damage to our economies, bring global companies to a standstill, paralyze our critical infrastructure, undermine our democracies and cripple our military capabilities”.4

#### Scenario 2 – supply chains

#### Supply chain attacks have been small, but massive escalation is coming

Higgins 21 [Kelly, Executive Editor of Dark Reading, award-winning technology & business journalist, named one of the Top 10 Cybersecurity Journalists in the US by Onalytica, “Why Supply Chain Attacks Are Destined to Escalate,” 08/05/21, <https://www.darkreading.com/vulnerabilities---threats/why-supply-chain-attacks-are-destined-to-escalate/d/d-id/1341588>, accessed 07/04/22, GDI-JCR]

The epic software supply chain attacks over the past year, including the high-profile breaches of SolarWinds, Microsoft Exchange Server, Kaseya, and Codecov, were only the beginning. "Supply chain attacks are only just starting, and mostly with pretty small vendors that most people had not heard of beforehand," said Corellium COO Matt Tait, in a live conversation via video with Black Hat founder Jeff Moss. But what happens when these attacks get bigger and affect larger vendors and more of their customers? Tait – who also delivered the prerecorded keynote, which was streamed on multiple large screens in a ballroom at the Mandalay Bay Conference Center in Las Vegas yesterday – said in the live portion of the event that the relative impact of these high-profile attacks could have been much worse given they were mostly targeted. He warned there will be more and they could well wreak more extensive and widespread damage to more organizations if the attackers hit larger targets with massive customer bases, such as the recent theft of source code from gaming giant EA Games. "It's likely to start to escalate in the coming months and years," he said. "And when something really big happens ... everything else will look like complete peanuts" in comparison, he said. When a nation-state or cybercrime organization makes that leap and infiltrates more victims, it will no longer be a "sustainable" situation.

#### With supply chains stretched thin, disruption would be economically catastrophic – there’s zero buffer

Murray 22 [Brendan, Trade Tsar at Bloomberg LP, “Cyber Threat Adds Another Curveball to Shipping Outlook,” 2/15/22, <https://www.bloomberg.com/news/newsletters/2022-02-15/supply-chain-latest-cyber-risk-adds-curveball-to-shipping-outlook>, accessed 07/04/22, GDI-JCR]

Jensen recalled a major cyber event in 2017, when shipping giant Maersk was among thousands of companies that shut systems down to assess the data damage. The Copenhagen-based container carrier’s estimate of the cost was around $300 million. Back then, port operators were among those with the most tangible consequences. While goods were moved, the process was slowed as terminals reverted to manual or backup operations. Still, the global economy absorbed the shock without much wider damage. With supply chains stretched to their limits, that’s unlikely to be the case now. No Buffer “In 2017 we could essentially lose the largest carrier in the world for a week and it didn’t cause any major problems,” Jensen said. “Sure, if you had your cargo on board one of those ships it got delayed maybe a week or two and that was annoying, but from a global perspective it was a non-event in terms of disturbing the supply chain. There was plenty of buffer capacity — of ships, terminals, everything. Right now we have zero, as in literally zero, buffer capacity.” Four of the world’s top five container lines are headquartered in western and northern Europe, and at least one has been hit with a cyber attack since the start of the pandemic. Marseille, France-based CMA CGM said in September 2020 that a breach hit services and affected bookings. Days later, the International Maritime Organization, a United Nations agency that serves as the industry’s regulatory body, said it suffered “a sophisticated cyber attack” affecting its public website and internal systems. In mid-January, European Union governments took part in large-scale simulation of a cyber intrusion affecting multiple member countries. The six-week exercise was expected to model attacks on supply chains and some spillover socio-economic effects in other countries. “If they have done their jobs well, they have a good backup plan,” Jensen said. “In the current environment, taking just one major port out of action for two, three, four days on top of what we’re already dealing with — that will have major ramifications on the supply chain.”

#### And, NATO is central to the protection of global supply chains

Granger 22 [Euan, Materials & Supply Chain Manager at Soil Machine Dynamics Ltd, “The Role of NATO in Protecting our Supply Chains,” 05/17/22, <https://www.procurious.com/procurement-news/author/euan-granger>, accessed 07/04/22, GDI-JCR]

NATO plays an active role in global peacekeeping, has built up the concept of co-operative security, and is a deterrent for illegal and terrorist activities. And it is in this role that we see the link between its activities and its importance to global supply chains. Protecting the Supply Chain Current events such as the war in Ukraine and global COVID restrictions, as well as the ongoing threat of terrorist activity has highlighted the importance of stability and continuity in the supply chain. For example, while Ukraine may not be a member of NATO, the NATO countries are using integrated logistics and supply routes to move arms, vehicles and aid into the war zone. Through its actions in the past, as well as actions it is taking now and for the future, NATO is providing support and protection for global supply chains. Here are three key ways that demonstrate the importance of the organisation to the global community: 1. Protection of Key Infrastructure – Energy Security Energy and key utilities, such as oil and gas, are critical for almost every aspect of global supply chains. Disruption to sources or supplies of energy could easily undermine the security of countries and continents, leading to situations where global production is halted, and supply of everything from electronic components to food and drink is disrupted. Vulnerabilities exist not only in infrastructure (oil/gas pipelines; power stations), but also in the systems used to control and manage them, especially in light of the increasing threat of cyber attacks. NATO members have been working since 2008 on energy security programs to help protect key infrastructure and ensure continuity of supply for both nations and the military. 2. Counter Piracy Operations and Protection of Sea Lanes Piracy continues to be a major threat to supply chains and freight in key shipping lanes around the world. While it would seem that the threat of piracy has lessened due to fewer serious incidents reported in the press in recent years, it remains a problem for shipping companies. NATO has in the past assisted in operations such as Operation Shield, an international cooperation to combat piracy of the east coast of Africa. Though this operation has since ended, NATO continues to work with countries and global partners to assist further anti-piracy efforts. Without the protection that NATO affords in conjunction with national navies and governments, there is the potential for disruptions to ships and cargo that would have lasting impacts on global supply chains. 3. Crisis Management including Relief Supplies in event of Natural Disasters NATO plays a key role in crisis and disaster management, both within its member countries and outside of this region. For this, NATO actually forms part of the global supply chain, ensuring that aid, equipment and personnel are able to reach areas affected by natural disasters. This can take the form of physically shipping goods on behalf of its member nations, as well as ensuring that requests for assistance from members or other countries are conveyed to the correct areas of government. While we may not see the work that NATO does as part of, or to support, global supply chains, its importance cannot be overemphasised. Without its efforts since its inception over 70 years ago, the global supply chain would look very different to how it does now.

#### Integrated offensive cyber capabilities enhance deterrence and defense against cyber threats

**Iftimie,** Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business**, 2020**

[Ion, “NATO’s needed offensive cyber capabilities” NDC POLICY BRIEF No. 10 – May 2020 <https://www.ndc.nato.int/news/news.php?icode=1441#:~:text=This%20Policy%20Brief%20looks%20at,cyber%20capabilities%20into%20its%20operations> accessed 7/5/22 GDI-TM]

Conclusion

The lack of integrated offensive cyber A2/AD capabilities undermines both the unity of the Alliance and its mandate of defence and deterrence. On the former, the lack of coordination between Allies during unilateral cyber operations could lead to friction when resulting effects infringe on Allied cyber-physical infrastructures. It could also lead to cyber fratricide, when failure to properly attribute Allied digital personas occurs during these military operations. On the latter, while most Allies are developing offensive cyber capabilities, some remain unable to face the growing number of cyber threats unilaterally.

Successful defence and deterrence in the cyber domain calls, thus, for ready collective offensive cyber A2/AD capabilities that, when integrated with NATO operations, would complement national and/ or regional responses to malicious cyber activities. If and when this integration occurs, NATO Flexible Deterrence Options would also need to be agreed upon in order to signal cyber adversaries that Allies will respond with one voice if attacked in the cyber domain. Ultimately, political consensus within the Alliance would still need to be built on the type of needed collective offensive cyber capabilities (such as for A2/ AD purposes) and on how to integrate them into NATO’s existing operations and missions.

#### Advantage 2 – NATO Credibility

#### NATO response to Russia’s invasion of Ukraine include expanding conventional forces - but new investment won’t solve immediately – NATO’s defense of the Baltics hinge on a nuclear deterrent that current has limited credibility

**BOWEN, 2022**

[Tyler, postdoctoral fellow in the Kissinger Center at Johns Hopkins SAIS “RUSSIA’S INVASION OF UKRAINE AND NATO’S CRISIS OF NUCLEAR CREDIBILITY” WOR April 20, 2022 <https://warontherocks.com/2022/04/russias-invasion-of-ukraine-and-natos-crisis-of-nuclear-credibility/> accessed 7/4/22 GDI-TM]

After Russia’s invasion of Ukraine, European NATO allies are now likely to increase investments in their armed forces that could make a successful conventional defense possible in the future. Germany’s decision to double its defense budget is telling in this regard. NATO’s increase in troops deployed to Eastern Europe is also a positive recent development. But these developments will take time to bear fruit.

Currently, NATO’s defense of the Baltics hinges on the threat of responding to a Russian attack with its nuclear arsenal. But Putin’s recent nuclear saber-rattling suggests he may not find this threat credible and believes Washington will back down rather than risk nuclear war. Indeed, even during the Cold War, it was difficult enough to convince the Soviet Union that the United States would trade Berlin for Boston. Expanding the alliance has only heightened this challenge. How can the United States make Putin believe that it is willing to trade Vilnius for New York?

#### Cyber threats erode nuclear deterrent – vulnerabilities undermine effective conventional and nuclear deterrence

**Montgomery and Borghard, National Defense University, 2021**

[Mark and Erica, “Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence” Joint Force Quarterly 102 July 1, 2021 <https://www.ndu.edu/News/Article-View/Article/2684986/cyber-threats-and-vulnerabilities-to-conventional-and-strategic-deterrence/> accessed 7/7/2022 GDI-TM]

Less attention, however, has been devoted to the cross-domain nexus between adversary cyber campaigns below the level of war and the implications for conventional or nuclear deterrence and warfighting capabilities.5 The most critical comparative warfighting advantage the United States enjoys relative to its adversaries is its technological edge in the conventional weapons realm—even as its hold may be weakening.6 Indeed, this is why adversaries prefer to contest the United States below the level of war, in the gray zone, and largely avoid direct military confrontation where they perceive a significant U.S. advantage. At the same time, adversaries are making substantial investments in technology and innovation to directly erode that edge, while also shielding themselves from it by developing offset, antiaccess/area-denial capabilities.7 Moreover, adversaries are engaging in cyber espionage to discern where key U.S. military capabilities and systems may be vulnerable and to potentially blind and paralyze the United States with cyber effects in a time of crisis or conflict.8

Therefore, while technologically advanced U.S. military capabilities form the bedrock of its military advantage, they also create cyber vulnerabilities that adversaries can and will undoubtedly use to their strategic advantage. To support a strategy of full-spectrum deterrence, the United States must maintain credible and capable conventional and nuclear capabilities. However, **adversaries could hold these at risk in cyberspace, potentially undermining deterrence.** If deterrence fails in times of crisis and conflict, the United States must be able to defend and surge conventional capabilities when adversaries utilize cyber capabilities to attack American military systems and functions. In this way, cyber vulnerabilities that adversaries exploit in routine competition below the level of war have dangerous implications for the U.S. ability to deter and prevail in conflict above that threshold—even in a noncyber context. The strategic consequences of the weakening of U.S. warfighting capabilities that support conventional—and, even more so, nuclear—deterrence are acute. Additionally, the scope and challenge in securing critical military networks and systems in cyberspace is immense. Therefore, urgent policy action is needed to address the cyber vulnerabilities of key weapons systems and functions.

#### -And, NATO in a unique window of vulnerability as the conventional forces scale up requiring enhanced US and NATO nuclear deterrent necessary check Russia

**BOWEN, 2022**

[Tyler, postdoctoral fellow in the Kissinger Center at Johns Hopkins SAIS “RUSSIA’S INVASION OF UKRAINE AND NATO’S CRISIS OF NUCLEAR CREDIBILITY” WOR April 20, 2022 <https://warontherocks.com/2022/04/russias-invasion-of-ukraine-and-natos-crisis-of-nuclear-credibility/> accessed 7/4/22 GDI-TM]

For decades, Americans and Europeans did not have to think about the dynamics of large-scale warfare between great powers or the possibility of nuclear escalation. Russia’s unprovoked invasion of Ukraine has shattered that sense of security. What’s more, the invasion of Ukraine, and the rhetoric surrounding it, has revealed the scope of Vladimir Putin’s grand ambitions: He wishes to reconstitute as much of the old Russian/Soviet empire in Eastern Europe as he can. The delegitimization of Ukraine has thrown into doubt the legitimacy of former Soviet republics Latvia, Lithuania, and Estonia and even neighboring states such as Finland and Poland. Putin regards the collapse of the Soviet Union as the “greatest geopolitical catastrophe of the century” and laments that it caused “tens of millions of our fellow citizens and countrymen to live beyond the fringes of Russian territory.” Putin feels that in order to be secure, Russia needs to revise the current balance of power in Europe. This ambition is consistent with scholarship that explains Russian foreign policy as a product of Putin’s illiberal, conservative philosophy and Putin’s desire to develop a Russian sphere of influence in the post-Soviet space. In the long run, the best way for NATO to deter him is to have enough conventional forces in Eastern Europe to deny Russia the ability to take the territory of countries such as Latvia, Lithuania, Estonia, and Poland. But NATO does not have the capability to do this at the moment, and it will take time to develop it. In the intervening “window of vulnerability,” the American extended nuclear deterrent and NATO’s tactical nuclear weapons will form the backbone of European security. The best way to ensure the credibility of this deterrent depends, in turn, on the outcome of the current war. If, as appears likely, Russia gets bogged down in a long drawn-out fight in Ukraine, it may have an incentive to expand the conflict by attacking an Eastern European NATO country. To deter this, the United States and NATO should increase the credibility of their nuclear deterrent by embracing a moderate form of the brinkmanship tactics articulated by an earlier generation of nuclear strategists. This would entail altering America’s and NATO’s nuclear posture such that it threatens to use its nuclear weapons earlier in a conflict. This solution is not ideal and should only be regarded as a short-term fix, but European security today requires NATO to accept a degree of brinkmanship.

#### Escalation because of failed deterrent goes nuclear

**Reach et al**, Policy Analyst at RAND, **2021**

[ Clint, “Competing with Russia Militarily”, RAND, June 22, https://www.rand.org/pubs/perspectives/PE330.html, accessed 6/22/21, Former GDI workshop student-AJ]

\*A2/AD= anti-access/area denial

\*BTG =battalion tactical groups

\*C4ISR =command, control, communications, computers, intelligence, surveillance, and reconnaissance

\*EDI =U.S. European deterrence initiative EW electronic warfare

\*IADS =integrated air defense systems

\*ISR= intelligence, surveillance, and reconnaissance

\*NSNW =nonstrategic nuclear weapons

\*SEAD =suppression of enemy air defenses

Although the overall military power of the United States and the NATO alliance vastly outstrips that of Russia, a regional conflict close to Russia’s borders would pose enor- mous challenges and could result in defeat for the West. Its relatively successful intervention in Syria notwithstanding, Russia’s power-projection capabilities are modest compared with those of the Soviet Union, much less the contempo- rary United States. Around its periphery, however, Russia is a formidable adversary that enjoys considerable local overmatch against the easternmost NATO states. Although at present the Russian government appears to have little appetite to challenge NATO by exploiting this local advan- tage, the possibility that Russian leaders will be tempted to do so in the future cannot be ruled out.

Current Russian military capabilities have benefited from a decade of reform and modernization inaugurated by the 2008 war with Georgia. Although Moscow swiftly subdued the Georgians in that conflict, it revealed numer- ous inadequacies in Russian military equipment and prac- tice. Transitioning away from the mass-mobilization draft army inherited from the Soviet Union, Russian officials evolved toward a smaller, more professional, dynamic force consisting substantially of contract soldiers. Moscow also expended considerable resources updating the Russian mil- itary’s aging stockpile of weapons and military equipment. Russian successes in eastern Ukraine and its intervention in Syria show that these changes have been rather effective.

The current Russian military boasts vastly greater capabilities than those of any adversary the United States has engaged with in combat in many decades. Moscow has fielded sophisticated (albeit untested) IADS that would complicate NATO efforts to secure air superior-ity. Russia could exploit the A2/AD bubble facilitated by these IADS to launch an air-supported ground invasion against NATO forces along its periphery. On the battlefield, Russia has continued the Soviet tradition of emphasizing massed indirect fires and various kinds of armor. Moscow also has a relatively limited arsenal of long-range strike weapons, including ballistic and cruise missiles, that can be employed in either a conventional or a nuclear role. Thanks to these strike capabilities, NATO rear and theater areas might offer little sanctuary from Russian attacks. Furthermore, Russia has modernized electronic warfare, cyber, and counterspace capabilities tailored to undermine NATO’s technical advantages.

The challenge of potential conflict with Russia is significantly exacerbated by Moscow’s formidable nuclear arsenal. Moscow possesses the world’s largest arsenal of NSNW. Even if these weapons are not used, they will play a considerable role in shaping a NATO-Russia war. Any conventional conflict with Russia will have to be fought in a way designed to limit the risk of nuclear escalation, which might constrain NATO from employing its full capabil- ities. For instance, NATO’s SEAD/ destruction of enemy air defense campaign—needed to secure air superiority— might be treated as a highly escalatory threat by Moscow, eliciting an attack on the NATO facilities supporting it. Although there is little reason to believe that Russian leaders would take the decision to go nuclear lightly, if they did make such a decision, it appears that there are highly attractive countermilitary targets for NSNW such as airbases and command and control sites. The destruction of these could significantly diminish NATO’s conventional advantages. Unfortunately, the acquisition of NSNW capa- bilities equivalent to those of Russia are not guaranteed to neutralize this problem: instead, Russian decisionmakers need to be convinced that limited nuclear use is unlikely to yield either military or political benefits.

#### -And, independently, cyberattacks on dual-use C3I system risk escalation from entanglement, misinterpretation, and preemptive countermeasures

**Afina, et. al, 20**

[Yasmin Afina, Research Assistant, International Security Program, and Calum Inverarity, Research Analyst, International Security Program, and Beyza Unal, Research Fellow, International Security Program, “Ensuring Cyber Resilience in NATO’s Command, Control and Communication Systems”, <https://www.chathamhouse.org/2020/07/ensuring-cyber-resilience-natos-command-control-and-communication-systems-0/about-authors>, Chatham House, 17 July 2020, accessed 29 June 2022, GDI-LR]

\*C3- command, control, communications

The increasing reliance on dual-use C3 assets, those used both for conventional and nuclear operations, raises the issue of entanglement and the risk of rapid escalation. These dual-use assets can range from communications satellites to early warning systems, radars and transmitters. According to recent research, notably by James M. Acton, parties to a conflict ‘could have strong incentives to attack the adversary’s dual-use C3I [command, control, communication and intelligence] capabilities to undermine its nonnuclear operations’.117 An attack on a dual-use C3 asset would particularly hold strong incentives for adversaries possessing nuclear weapons and not ruling out their potential use. For instance, a cyberattack on early warning satellites will provide a tremendous advantage to the adversary by either delaying the detection of a missile launch (conventional or nuclear) or even preventing it from being identified in the first place.

James M. Acton addresses two mechanisms that lead to escalation.118 First is a ‘misinterpreted warning’, probably at a time of crisis, where a state’s dual-use C3 assets are targeted by conventional weapons or cyber interferences and the target state might misinterpret these attacks as ‘preparations for an incoming use of nuclear weapons’ by their adversary.119 The targeted state might miscalculate and respond in a highly escalatory way that leads to full-scale conventional or nuclear war. Second, if a state’s C3 capability was attacked by conventional means, it might lose its advantage to destroy an adversary’s nuclear weapon systems. In order to prevent such a situation happening, the state might use pre-emptive countermeasures that would themselves lead to escalation,120 thus adding nuclear ‘use it or lose it’ pressures to conventional crises.

It is important to note that the escalation mechanisms identified by Acton rest on hypothetical situations in which states that have been forced, for the purposes of the argument, into adopting an inherently escalatory posture; in reality, this may not be the inevitable outcome. The role of conventional forces and cyber interferences is highlighted primarily and under specific conditions as a route to escalation, rather than also as a source of potential de-escalation. Although risks of escalation through entanglement might be greater in some cases, it is hard to judge a state’s possible actions only by counting its conventional or nuclear capabilities or by assigning an escalatory role to them. Escalation is a choice, and the logic of escalation mechanisms removes the factor of human agency for conflict avoidance. Ultimately, survival of a state may not, in all instances, be linked to the survival of its nuclear forces.

#### Increased cyber activities disrupt NATO logistics and forward operations – integration and coordination of offensive cyber necessary for NATO operations

**Iftimie,** Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business**, 2020**

[Ion, “NATO’s needed offensive cyber capabilities” NDC POLICY BRIEF No. 10 – May 2020 <https://www.ndc.nato.int/news/news.php?icode=1441#:~:text=This%20Policy%20Brief%20looks%20at,cyber%20capabilities%20into%20its%20operations> accessed 7/5/22 GDI-TM]

Over the past decade, Allies have identified a steep increase in cyber activities targeting the critical infrastructure sectors that NATO military operations rely upon. Directly or indirectly, these malicious cyber activities can also disrupt the Alliance’s logistics and forward operations. NATO’s commitment to “operate and defend itself ”5 in the cyber domain as effectively as in the geographic domains came, thus, as a direct recognition of cyber as a hybrid threat to both the Allies and the Alliance. Compared to the air, land and sea domains, the cyber domain is not constrained by national borders (although certain physical aspects of it might be located within them). This distinction between the cyber and the geographic domains is important to note, because NATO was founded in response to external military threats without the right to intervene in internal security matters, where member states maintain the monopoly over the use of force. In the cyber domain, the distinction between internal and external security threats is harder to ascertain. When integrating offensive cyber capabilities into its defence and deterrence mandate, NATO would inevitably tackle certain aspects inherent to internal security; and yet, not legally infringe on the sovereignty of the Allies as long as effects amounting to force or intervention are not employed against the physical systems residing in these nations.6 Operating in the cyber domain requires, thus, that member states better integrate their offensive cyber capabilities into NATO operations not just to win future wars, but also to avoid elements of friction between Allies, which may arise from unilateral cyber effects to defend critical infrastructure.

#### And, signaling of the plan decreases escalation of conventional conflicts through accommodative signaling that reinforces coercive signaling

**Lonergan**, assistant professor at the Army Cyber Institute at the US Military Academy, and **Lonergan**, senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers, **2022**

[Erica and Shawn, “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises”, Security Studies, 18 Feb 2022, Taylor and Francis, accessed July 1, 2022, JCP-LL]

Signaling for Resolve Versus Accommodation

Snyder and Diesing’s foundational work on coercive diplomacy emphasizes that almost all international crises contain elements of both coercion and accommodation.14 For accommodation, resolve is less imperative than more conciliatory signaling objectives, such as willingness to make conces- sions, compromise, save face, and avoid war.15 Crisis management, as Snyder and Diesing define it, entails ensuring a state can achieve its stra- tegic interests and mitigate potential risks of escalation. The challenge “is to find the optimum mix or trade-off between coercion and accommoda- tion in the particular crisis context, given the distribution of values and military power among the participants.”16

The distinction between coercion and accommodation rests on the rela- tive emphasis on “winning” versus mitigating the risks of war. Coercion weighs the former more heavily, whereas accommodation seeks to “reach some settlement that promises to defuse the issue as a potential source of future crises”—without making too many painful concessions.17 Nevertheless, each contains elements of the other; coercive strategies may include accommodative tactics meant to address controlling escalation risks, and accommodative strategies may include coercive tactics that seek to minimize losses.18 Characteristics of accommodative actions include demonstrating restraint, information sharing, clarifying shared expectations and norms regarding limits on conflict, or creating space for negotiations and diplomacy.19 Accommodative signaling is linked to crisis de-escalation because the former can enable the latter. Even a “controlled reprisal” that is less escalatory than the prior action could prompt both sides to de-escalate.20

#### Offensive cyber operations provides A2/AD to prevent freedom to maneuver in cyberspace – integration of OCOs key to deterrence credibility

**Iftimie,** Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business**, 2020**

[Ion, “NATO’s needed offensive cyber capabilities” NDC POLICY BRIEF No. 10 – May 2020 <https://www.ndc.nato.int/news/news.php?icode=1441#:~:text=This%20Policy%20Brief%20looks%20at,cyber%20capabilities%20into%20its%20operations> accessed 7/5/22 GDI-TM]

The use of area denial weapon systems in the cyber domain

Anti-Access/Area Denial (A2/AD) weapon systems have traditionally been used by NATO and its member states to prevent an adversary’s freedom of maneuver on land, sea or air. In the geographic domains, these capabilities include land mines, missiles (cruise, ballistic, surface to air, anti-ship, etc.), submarines, electronic warfare, and even Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) weapons. In the cyber domain A2/AD is achieved through offensive cyber operations. Those operations have already been used for the purpose of achieving A2/AD by NATO member states in the cyber domain. This is the case of the US-led Operation Glowing Symphony (OGS), where “the United States Cyber Command reportedly acquired administrator passwords to [Daesh] websites. The passwords enabled deletion of digital content, including videos used for recruitment, from cyber infrastructure located in at least five countries outside actively hostile areas of Iraq and Syria. Similar digital content reportedly resided on cyber infrastructure in as many as 30 other States. Changing the passwords reportedly locked IS administrators out of the websites”.11 OGS restricted Daesh’s freedom of maneuver on networks physically residing in Iraq and Syria (which were controlled by the terrorist group), but also worldwide, where a NATO member state (the US) achieved denial of service effects against Daesh. OGS disrupted Daesh propaganda through content removal from servers residing in multiple countries and through restricting access to physical infrastructure needed to store digital data. Combined with operational successes against ISIL on the ground, OGS actions resulted in propaganda efforts being significantly reduced on several global social media platforms, including Twitter. One particular offensive cyber operation acted, ipso facto, as an A2/AD platform where a NATO member state restricted access to physical networks critical for Daesh recruitment, training, radicalization, fundraising, and command and control. Integrating offensive cyber capabilities into NATO’s mandate for cyber deterrence and defence Operationalizing warfighting capabilities in the cyber domain, beyond the traditional geographic domains, requires a new way of fighting in the 21st century, challenging the deterrence and defence mandate of the Alliance. Speaking at the Cyber Defence Pledge Conference in London in May 2019, NATO Secretary General highlighted that **for deterrence to have full effect against state and non-state adversaries, NATO and its member states must be ready to use the full range of capabilities at their disposal, to include national offensive cyber capabilities**. Deterrence is the act of diminishing an adversary’s intent by highlighting the excessive costs for the said adversary if it proceeds with an undesired action. In NATO’s case, deterrence is achieved by highlighting to an adversary the excessive costs delivered through military means in the event of an attack against Allies. For deterrence to be successful, the adversary must believe that NATO is ready and willing to impose these excessive costs across all operational domains, to include the cyber domain. This may call for Allies to develop offensive cyber capabilities and integrate them with NATO operations in order to collectively impose a high enough cost to deter adversaries from aggressive behaviour. To avoid escalation to total war and cyber fratricide during the fog of war, Allies must also agree on a list of Flexible Deterrent Options meant to allow for a gradual increase of pressure in the cyber domain, and then hopefully limiting the scope and intensity of conflict in this domain. NATO Flexible Deterrent Options in the cyber domain could include (as presented in Figure 1): • Increasing NATO’s readiness posture through cyber education, training and exercises; • Deploying NATO Cyber Rapid Reaction teams to conduct defensive cyber operations and protecting critical infrastructure of NATO member states and/or that NATO operations rely upon; • Increasing public awareness of malicious cyber activities and the potential for conflict in the cyber domain; • Taking steps to gain the support of all NATO member states in response to the cyber threat and in accordance with commitments of the 2016 Cyber Defence Pledge and the 2018 Brussels Summit; • Triggering Article 4 of the Treaty to enhance information-sharing and mutual assistance in the cyber domain; • Making official statements addressing violations of international law in the cyber domain; • Alerting and deploying offensive cyber operations forces; • Imposing cyber sanctions;12 • Conducting offensive cyber operations to achieve A2/AD effects in the cyber domain; • Triggering Article 5 of the Treaty; and • Conducting offensive cyber operations in combination with other maneuver forces across all operational domains.

#### -Even if the neg wins that there are sources of disagreement around OCOs, military to military exercises solve while sorting out details improves NATO OCOs through process of consensus building on offensive cyber capabilities

**Lonergan** , assistant professor in the Army Cyber Institute at West Point and research scholar at the Saltzman Institute of War and Peace Studies at Columbia University **and Montgomery**, senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies, **2022**

Next Steps: Addressing Challenges and Mitigating Risks

Given the threat environment facing NATO, as well as the activities of several NATO members, the alliance should deliberately—but purposefully—consider incorporating offensive cyber operations below the level of armed conflict into its deterrence strategy. Any effort to explore a role for offensive cyber operations should also consider the challenges and risks that may come with doing so. A central challenge is that, at the political level, NATO allies lack consensus on the appropriate application of offensive cyber power—especially below the level of armed conflict. Addressing these disagreements among member states is essential because conducting offensive cyber operations often requires maneuvering through or operating on networks controlled by an ally or allies. Right now, NATO members do not collectively agree on the protocols and processes for partner actions in allied networks—and they also disagree on how to define sovereignty in cyberspace, or when an offensive cyber operation would rise to the level of an armed attack.

Offensive cyber operations for NATO also present real interoperability challenges. The role of intelligence in cyber operations is likely to complicate NATO planning processes. Even close allies are likely to be wary about sharing sensitive intelligence for a number of reasons. For instance, they may be averse to sharing information gleaned from signals intelligence collection or because a member state may be using the same exploits for both offensive action and their own espionage—including intelligence collection against allies. Or, allies may simply be worried that sensitive information may become exposed. On top of this, it’s challenging to adjudicate intelligence requirements among allies and to deconflict intelligence and military priorities. It is also not clear whether the alliance has established consensus thresholds that specify the conditions and timeline under which a state would have to notify others of its activities on their networks—if at all.

The alliance should account for, and address, these issues as NATO explores the prospect of incorporating offensive cyber operations below the level of armed conflict into existing NATO simulations and exercises that span the strategic, operational, and tactical levels. A number of important questions about how to coordinate offensive cyber operations and define roles and responsibilities remain unanswered. For instance, how could allies improve intelligence sharing to conduct more rapid attribution, enabling one state or the alliance to respond to adversary cyber activity? What are the conditions under which allies should consider dividing responsibilities for cyber campaign planning and developing accesses and capabilities against strategic targets in, for example, Russia? If some allies are responsible for offensive cyber operations against certain targets, what are the information-sharing and notification requirements?

#### Solvency

#### Now is the key time to act - NATO ahead on tech now – gap closing with Russia, China and non-state actors. NATO investment in tech capacity and innovation necessary to keep gap in capabilities

Magula and Alvarez-Couceiro, 21

[Justin, Army Strategist serving in the Strategic Landpower and Futures Group at the U.S. Army War College, and Paula, graduate of Strategic Studies at the Johns Hopkins University School of Advanced International Studies, "Mainaining and Improving NATO's Technological Edge", Wavell Room, 9/30/21, https://wavellroom.com/2021/09/30/maintaining-improving-natos-technological-edge-technology/, accessed 7/4/22, GDI-cc]

What happens when an alliance’s competitors quickly improve their technology and capabilities to place the alliance at increased risk? The North Atlantic Treaty Organization (NATO) addressed this dilemma during a recent summit in Brussels.  At the summit, the North Atlantic Council built upon[NATO’s 2030 strategic outline](https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf) and presented targets for increased technological collaboration to counter growing threats from Russia, China, and non-state actors. While NATO’s scientific and technical superiority has historically allowed it to outpace competitors, its adversaries are quickly closing the gap.

NATO members still hold advantages in their development of [new technologies](http://wavellroom.com/podcast/technology-and-the-future-of-land-warfare/). According to the Global Innovation Index, seven of the top ten[most innovative countries](https://knowledge.insead.edu/entrepreneurship/the-worlds-most-innovative-countries-2020-15076) globally are part of NATO, while the other three are key NATO partners. Even so, NATO can do more to harness the alliance’s combined technological prowess to better compete and win in a future conflict. As China seeks to become the[world’s innovation leader](https://www.businesschief.asia/leadership-and-strategy/china-aims-be-global-innovation-leaders-next-15-years) and Russia continues to undermine the alliance’s security, NATO will need to out-innovate its competitors and prepare for an uncertain future.

Four areas where NATO can focus on improving its competitive edge are developing its formal organizations, increasing public and private sector collaboration, harnessing and countering Emerging Disruptive Technologies (EDTs), and improving conventional military equipment. NATO must maintain its relative lead in technology sectors to defend its people and enhance its long-term strategic position. Improving science and technology (S&T) innovation will increase alliance collaboration, strengthen public and private sector cooperation, counter hybrid threats, deter adversaries, and harden defenses against attacks. NATO’s effectiveness in the future will heavily depend on its ability to maintain and improve its science and technology capabilities.

#### NATO collective defense and deterrent enhanced by military to military cyber exercises

**Maigre, 2022**

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

Action Plan for the Next Five Years

To make NATO future-proof, it must be cyber-secure and operational. But is it doing enough to address the complex and evolving challenges of cyberspace? NATO’s strategic challenge is to blend its successful conventional deterrence functions with a new strategy for cyber action. NATO’s ability to send a collective message of resistance and to establish a credible threat response is its most valuable asset on the cyber-security front.

Four sets of actions for NATO are proposed. First, denying covertness by attribution: NATO should persuade opponents that they cannot be clandestine in their cyber actions. NATO and its members need to demonstrate that it is difficult or impossible to act covertly and be clear about attributing responsibility for cyberattacks.

Until recently, governments did not publicly release details on cyber incidents. But since 2018, public disclosures of cyberattacks by several Western powers indicate a new multinational policy of state transpar- ency. The growing relevance of attribution is partially due to states becoming better at attributing cyber operations.1 Greater public knowledge of cyberattacks heightens awareness of cyber conflicts and leads to greater public acceptance of cyber countermeasures.

Ultimately, what matters is that states engaging in unlawful actions using cyber means will face conse- quences. With attribution, policymakers show that they know what is happening in these networks and can investigate incidents. It also clearly spells out unacceptable behavior and can help create state prac- tice. The best way to implement the international norms is by calling out behavior and having conse- quences when these norms are breached. Attribu- tion will make clear to the malicious actor that their actions will be seen and addressed. It is the basis, under international law, for countermeasures and self-defense.

When should states publicly attribute cyberat- tacks? Effective public attribution requires a clear understanding of the attributed cyber operation and the cyber-threat actor, but also the broader geopo- litical environment, allied positions and activities, and the legal context. The public attribution frame- work put forward by Max Smeets and Florian Egloff in March 202127 distinguishes four factors that act as enablers or constraints in public attribution. These factors are intelligence, incident severity, geopolitical context, and post-attribution actions. The combina- tion of these four components enables consistent deci- sion-making about whether to publicly disseminate information about an adversary’s actions, privately tell the adversary, or restrict knowledge of the intrusion to the government and potentially other partners.

Collecting and processing intelligence—infor- mation about foreign countries and their agents— provides a technical basis for attribution. How could allies improve intelligence sharing to conduct more rapid attribution and enable a response to adver- sary cyber activity? During the Nordic-Baltic foreign ministers meeting in Tallinn in September 2020, a 90-minute tabletop exercise was organized28 to test the ministers’ ability to respond to and attribute an esca- lating cyberattack. They answered multiple-choice questions on communication of and possible diplo- matic countermeasures to the attack. The minis- ters learned through first-hand experience that a timely exchange of technical intelligence can be key in attributing any cyberattack. “The shared view [of the countries involved]—especially when it comes to complicated issues—is crucial,” said Urmas Reinsalu, Foreign Minister of Estonia.29

Attribution is only as good as the information that allies are willing to share. NATO’s value can be in becoming the preferred platform for sharing cyber information. General Paul Nakasone, who heads US Cyber Command, told the House Armed Services subcommittee on intelligence that “in 35 years” he has never seen a better sharing of accu- rate, timely, and actionable intelligence than what has transpired with Ukraine.30 Sharing information and intelligence with allies “builds coalitions” and can “shine a light on disinformation” campaigns, like the one Russia used to lay the groundwork for their invasion of Ukraine.

As the second course of action**, NATO should use the current crisis to accelerate the progress with setting up NATO’s own cyber command and sharpen allied responses to malicious cyber actions**. Overall, this would give more credibility to its cyber defense. In February 2019, allies endorsed a set of tools to respond to cumulative cyber activities, but not much has happened to take it forward. It is now time to build upon this set and develop concrete steps at the political, military, and technical levels to model alli- ance behavior according to the threat landscape. This means a sharper focus on future responses to high- and low-end cyberattacks along with concrete deter- rence actions and tools for individual sectors and target types. Much of this is based on the high-end cyber capabilities of select individual allies called “volunteer sovereign cyber effects,” where cyber- capable nations deliver voluntarily offensive cyber effects on a target designated by an operational-levelcommander. The NATO Cyber Command would be responsible for matching military needs with the willingness and capabilities of the nations potentially able to deliver such effects.31 **The alliance should clarify which allies are responsible for offensive cyber operations against certain targets and the informa- tion-sharing and notification requirements.**

**A good plan requires practice. The scenarios of cyber responses that are under the Article 5 threshold should be regularly practiced, and the NATO Cooper- ative Cyber Defense Centre of Excellence (CCDCOE) Locked Shields exercise is a good way to do so**. Orga- nized since 2010, it enables cyber-security experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. The focus should be on realistic scenarios simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects. Locked Shields is a unique opportunity to encourage experimentation, training, and cooperation among allies in an authentic but safe training environment.

NATO should also make more use of its Cyber Range, a platform for NATO exercises and training in Estonia operated by the Estonian Ministry of Defense. The Cyber Range already facilitates NATO’s flagship annual cyber defense exercise Cyber Coalition, and NATO CCDCOE has based Locked Shields on Cyber Range for over a decade. The versatility and computing power of the platform allows a different, complex scenario to be simulated every year for an increasing number of participants. The technical, red-teaming exercise CrossedSwords, organized by NATO CCDCOE, tests the capabilities and skills needed when executing a full-spectrum cyber operation in real life, focusing on experimentation with integrating kinetics and offensive cyber operations in the context of a modern battlefield. More operational- and technical-level joint activ- ities should be practiced among allies and with like- minded partners in order to contribute to imposing costs to malicious actors in cyberspace**. Given that NATO’s cyber response teams are stretched thin due to protecting NATO’s own networks, bi- and multilateral collaboration enables countries to share best practices and, in the event of an emergency, provide mutual rapid assistance in crisis response.**

The cyber exercise Baltic Ghost originated from a series of cyber defense workshops in 2013 and should be expanded to include all NATO battlegroups in the Baltics and Poland. Currently it is facilitated by the United States European Command with the objective to develop and sustain cyber partnerships between Estonia, Latvia, Lithuania on one end, and the Mary- land, Michigan, and Pennsylvania Army National Guards on the other end. Building on the success of Baltic Ghost, regular cyber exercises should take place in multinational NATO battlegroups, led by the United Kingdom, Canada, Germany, and the United States, in Estonia, Latvia, Lithuania, and Poland. Future exercises should regularly support NATO enhanced forward presence forces and train participants to respond to aggression in a contested, degraded, and denied cyberspace environment.

#### US and NATO proactive and continuous responses needed to enhance deterrence and defend in great power war competition with Russia and China

**Kramer et al, Atlantic Council, 2020**

[Franklin, “NATO needs continuous responses in cyberspace“ New Atlanticist

December 9, 2020 <https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-/responses-in-cyberspace/> accessed 7/7/22 GDI-TM]

President-Elect Joe Biden’s transition team has declared cyber threats as “one of the defining challenges of our time.” In its early days, the incoming US administration must take on cybersecurity threats as one of its key priorities. Nowhere will that effort be more important than with the United States’ closest Allies at NATO, a cornerstone for Western security. Today, NATO’s security is threatened by Russia’s and China’s continuous cyberattacks on the Alliance and its members. To accomplish its mission of deterrence and defense, NATO needs to implement a strategy of proactive, continuous responses to China and Russia in cyberspace, where great power competition is playing out in real time.

# Advantages – cards for all versions

## Cyber Attacks Impact

### Uniqueness - Cyber threats complexity

#### Cyber-threat landscape complex – multiple avenues for attack on NATO countries

**Maigre, 2022**

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

Introduction What the war in Ukraine says about cyber power is yet not entirely cleared from the fog of war. Many aspects remain uncertain, but given the unpredictability of the Putin regime, the risk of an escalation in hostile cyber exchanges between Russia and NATO states remains high. What is clear is that, as of February 24, 2022, we live in a different world in which the European and global security orders have been shattered. This brief first explores the challenge that cyber threats pose to NATO allies and how the rapidly evolving cyber-threat landscape can alter the inter- national security environment. Secondly, it looks at developments in cyber defense policy within NATO. Finally, the brief analyzes how NATO needs to adapt to address cyber challenges, studying how allies align their sovereign interests, capabilities, and cyber doctrines with NATO operational requirements and strategic ambitions. NATO is set to issue strategic documents in 2022 that will guide the next decade of its military planning. This will certainly require more transatlantic consultation on political-military matters with an emphasis on cyber security and cyber defense. The Cyber Challenge to the World and NATO Allies Malicious cyber activity has increased substantially over the past years while the world has kept turning amid the omnipresent pandemic and now war in Ukraine. States, non-state actors, and criminal groups compete and are increasingly weaponizing sensitive information and infiltrating other countries’ networks to steal data, seed misinformation, or disrupt critical infrastructure. The coronavirus pandemic further complicated the cyber-threat landscape. In March 2020, attempts to mitigate the spread of the coronavirus led to social distancing measures, travel restrictions, and remote work. In a short span of time, IT security profes- sionals had to respond to the challenges of working from home, such as enterprise data movements when employees accessed cloud-based apps via their home internet, corporate software, videoconferencing, and file sharing.1 Even if hardware and software solutions were in place to secure the organization’s data, there were often no established policies to help employees wade through the jungle of threats and vulnerabilities they faced when moving their workplace out of the traditional office environment.2 According to the FireEye Mandiant Special Report: M-Trends 2021, the top five most targeted indus- tries in 2020 were business and professional services, retail and hospitality, finance, healthcare, and high technology. The main methods used were extortion, ransom demands, payment card theft, and illicit trans- fers. Direct financial gain was the likely motive for 36% of intrusions, and an additional 2% of intrusions were likely perpetrated to resell access. In 2021, data theft remained an important mission objective for threat actors; in 32% of intrusions, adversaries stole data.3 Currently, highly organized, technically proficient criminal syndicates comprise the most significant cyber threat to allies. These groups try to steal data or extort money through ransomware. In 2021, promi- nent ransomware attacks struck Colonial Pipeline, the operator of the largest fuel pipeline on the East Coast of the United States; JBS, the largest meat processing company in North America; and Coop, a major supermarket chain in Sweden. Healthcare was also targeted—in May of the same year, the entire health service system of Ireland was disrupted for weeks, and over the spring and summer, dozens of hospitals in Europe and the United States were locked out of life-critical systems by ransomware attacks.4 Another set of threats comes in the form of bellig- erent state actors that seek to steal sensitive data for espionage. In December 2020, Russian intelligence services infiltrated the digital systems run by US tech firm SolarWinds and inserted malware into its code. During the company’s next software update, the virus was inadvertently spread to about 18,000 clients, including large corporations, the Pentagon, the State Department, Homeland Security, the Treasury, and other US government agencies. The hack went unde- tected for months before the victims discovered vast amounts of their data had been stolen.5 There are also politically motivated cyberattacks mandated by states that interfere in democratic processes and political discourse. In September 2020, the internal email system of Norway’s parliament was hacked.6 Ine Eriksen Søreide, the Minister of Foreign Affairs of Norway, underlined the significance of the attack by calling it an important cyber incident that affected the “most important democratic institution” of the country.7 Norwegian authorities later identified Russia as the actor responsible for the attack, marking the first time that Norwegian authorities had made a political attribution to such an attack. Since the beginning of this year, Ukraine’s govern- ment has been hit by a series of cyberattacks that defaced government websites and wiped out the data on some government computers. In mid-Jan- uary, hackers defaced about 70 Ukrainian websites, including the Ministries of Foreign Affairs, Defense, Energy, Education, and Science, as well as the State Emergency Service and the Ministry of Digital Trans- formation, whose e-governance portal gives the Ukrainian public digital access to dozens of govern- ment services. The hackers replaced the home pages of about a dozen sites with a threatening message: “be afraid and expect worse.” After a couple of days,however, most of the sites were restored.8 The inter- national hacktivist collective Anonymous has declared “cyberwar” against Russia’s government, claiming credit for several cyber incidents including distrib- uted denial of service attacks that took down Russian government websites and Russia Today, the state- backed news service.9 Around the globe, aging critical infrastructure has long been vulnerable to attack. The most worrying type of cyberattack is sophis- ticated malware designed by states or state-backed actors that act as “time bombs” in the critical cyber networks of target countries, such as the energy, telecom, and transportation sectors. Around the globe, aging critical infrastructure has long been vulnerable to attack. In 2020, the UK’s National Cyber Security Centre issued a warning of Russian attacks on millions of routers, firewalls, and devices used by infrastruc- ture operators and government agencies.10 On the day of the Russian invasion, ViaSat, a provider of high-speed satellite broadband services, was hacked along with one of its satellites Ka-Sat, whose users included Ukraine’s armed forces, police, and intelligence service. Destructive wiper malware attacks by Russia against Ukraine included Whisper- Gate, discovered in January by Microsoft, in Ukraine’s networks that “provide critical executive branch or emergency response functions”;11 HermeticWizard and IsaacWiper,12 targeting multiple Ukrainian orga- nizations just hours before the Russian invasion began; and CaddyWiper, spotted by researchers at the Slovak internet security company ESET in mid-March.13 All of them were designed to wipe or overwrite critical files on infected systems and leave computer hard drives corrupted and unrecoverable. These incidents demonstrate that, in the words of cyber expert and Silverado Policy Accelerator think tank chairman Dmitri Alperovich, “Cyberattacks have become a theater for great-power conflict in which governments and militaries fight in the hybrid ‘gray zone,’ where the boundaries between peace and war are blurred.”14 The actors navigate a complex web of ambiguous and deeply interconnected challenges, where cyberattacks are not a separate front, but rather an extension of the conflict.

### Uniqueness - Grey zone attacks increasing

#### Multiple examples of grey zone attacks against NATO allies – need focus on offensive cyber operations

**Lonergan** , assistant professor in the Army Cyber Institute at West Point and research scholar at the Saltzman Institute of War and Peace Studies at Columbia University **and Montgomery**, senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies, **2022**

The primary threat to NATO allies in the cyber domain is not from high-end, decisive cyberattacks. Instead, cyber threats more frequently and effectively manifest as gray zone tactics designed to have a corrosive effect without rising to the level of warfare. There are numerous examples of this type of threat. For instance, in July 2021, NATO publicly condemned a range of malicious cyber behavior, including the Microsoft Exchange hack (which NATO attributed to China) and ransomware attacks targeting critical infrastructure. Russia has leveraged cyber and disinformation operations to interfere in democratic elections in the United States in 2016, 2018, and 2020; France in 2017; and Germany in 2017 and 2021—to name just a few examples. Russia also conducted distributed denial-of-service cyberattacks against government websites in Montenegro during the lead-up to, and following, Montenegro’s ascension to NATO in 2017. And when NATO forces were positioned in the Baltics beginning in 2017 as part of NATO’s enhanced forward presence, two threat actors, GhostWriter and Secondary Infektion, conducted a range of disinformation campaigns. Additionally, the reality is that several NATO members are already speaking publicly about offensive cyber operations below the level of warfare and their statements and actions have an effect on the entire alliance. In particular, NATO member nations have not reached a political consensus about the role of offensive cyber operations. In 2018, the US Department of Defense and US Cyber Command issued new strategy and policy documents that articulated a role for the military in conducting offensive cyber operations below the level of armed conflict outside of US-controlled cyberspace (part of the “defend forward” strategy), and there has been some reporting about US offensive cyber operations. For instance, in 2018 the United States disrupted the Russian-linked Internet Research Agency from interfering in the midterm elections. And, more recently, in December 2021 General Paul Nakasone, commander of US Cyber Command, publicly acknowledged that the military played a role in disrupting ransomware groups targeting critical infrastructure. The United States has also worked with other NATO allies, such as Estonia and Montenegro, to conduct “hunt forward” cyber operations on allied and partner networks to uncover and disrupt malicious cyber activity. Other NATO allies have also been more transparent about offensive cyber operations. In 2020, the United Kingdom announced a significant investment in its National Cyber Force, its organizational arm for offensive cyber operations, and its 2022 National Cyber Strategy emphasized the role of offensive cyber operations. In November 2021, General Nakasone and the director of Government Communications Headquarters—the UK government’s principal signals intelligence agency—stated jointly that the two governments were collaborating to “impose consequences” in cyberspace to disrupt adversary operations. The Netherlands has also publicly alluded to conducting offensive cyber operations.

### Uniqueness - Attacks Increasing

#### There’s been an exponential rise in attacks on critical infrastructure – the payoff for attacker is massive

Horwitz 21 [Lauren, senior content director at IoT World Today, winner of the Silver Award from the American Society of Business Publican Editors, “Malicious Attacks on IoT and Critical Infrastructure Gather Pace,” 08/09/21, <https://www.iotworldtoday.com/2021/08/09/malicious-attacks-on-iot-and-critical-infrastructure-and-likely-to-worsen/>, accessed 07/04/22, GDI-JCR]

As the globe continues to wobble through the reverberations of COVID-19, observers say that the impact on critical infrastructure is likely to worsen. Critical infrastructure – which includes government institutions, utilities, transportation and more – is now more vulnerable than ever given an exponential increase in attacks on the IoT technology that powers it. Such technology has become a “soft target,” for malicious actors. That’s because Internet of Things (IoT) technology may be legacy technology, with inadequate updating and patching, and because the financial incentives to breach its security have grown. Attacks on IoT Technology Garner Big Payouts. As a result, ransomware attacks on IoT have become more prevalent, with larger payouts possible for malicious actors. Consider the February 2021 attack on the Oldsmar water plant in Florida; an attempt was made to manipulate the pH in the city’s water to dangerously high acidic levels by increasing sodium hydroxide (lye) by 100 times. In May 2021, the Colonial pipeline was attacked for a ransom. A password leaked onto the dark web enabled malicious actors to access a virtual private network, then gain access to and take down the largest fuel pipeline in the U.S. Colonial paid the malicious attackers — an affiliate of a Russia-linked cybercrime group known as DarkSide — a $4.4 million ransom shortly after the attack. Insiders say that the critical infrastructure environment is rife for breaches. “The OT and ICS [incident command system] space is, honestly, the largest single attack vector with the greatest potential for impact,” said Curtis Simpson, CISO at Armis, in a podcast on critical infrastructure attacks . “OT and ICS are powering some of the most critical infrastructure in the world; it’s critical operations,” Simpson said. One bright spot on the ransomware front is that the U.S. Department of Justice in April 2021 created a ransomware task force, after declaring 2020 the “worst year ever” for extortion-related cyberattacks. And accordingly, in June, the Justice Department said it had seized the majority of the nearly $4.4 million in bitcoin ransom paid to DarkSide for the Colonial Pipeline takedown. Pandemic Times Expand Definition of Critical Infrastructure According to the OECD, the pandemic has unveiled a broader set of infrastructure vulnerabilities beyond transportation and fuel, for example. “Notably, the crisis has brought renewed focus on social or ‘soft’ infrastructure, which is sometimes overshadowed by hard infrastructure like energy and transportation in the context of resilience,” the OECD note indicated. “These infrastructures that maintain the economic, health, education, cultural and social standards of a population are critical elements of modern societies.” Simpson echoed this notion. He said that even a business such as Sysco Foods, where he worked previously, is in some ways critical infrastructure. Sysco is the largest food distributor in the world, and that business, Simpson said, is run entirely on IoT, OT and ICS.

#### Existential risk is high for global miscalculation and collapse of U.S. digital dominance.

Muggah 21 [Robert, principal at the SecDev Group, a co-founder of the Igarapé Institute, 1-11-2021, “Why The Latest Cyberattack Was Different,” Foreign Policy, <https://foreignpolicy.com/2021/01/11/cyberattack-hackers-russia-svr-gru-solarwinds-virus-internet/>, accessed 07/04/22, GDI-JCR]

All during 2020, as the coronavirus pandemic swept around the world, another novel virus with devastating long-term effects spread unnoticed worldwide. Sometime in late 2019 or early 2020, at least one group of advanced hackers inserted malware into network software supplied by SolarWinds, a maker of information technology infrastructure software based in Austin, Texas. The decision to target SolarWinds looks strategic given the company’s vast U.S. and global clientele in the public, private, and nonprofit sectors. Publicly exposed in December 2020, the infectious malware—dubbed Sunburst by the cybersecurity firm FireEye and Solorigate by Microsoft—may turn out to be the most audacious cyberespionage campaign in history. For months, attackers stealthily infiltrated governments and businesses via a Trojan horse-style update to SolarWinds’ Orion cybersecurity management software. Like the coronavirus, Sunburst and another recently discovered piece of malware reveal the downside of global connectivity and the failure of global cooperation to deal with contagion. What sets the SolarWinds attack apart from previous incidents is its **sheer scale**. The company has over 300,000 customers worldwide, according to filings made to the U.S. Securities and Exchange Commission. Throughout 2020, SolarWinds sent out software updates to roughly 18,000 of them. To date, at least 250 networks have reportedly been affected by the booby-trapped file. Shortly after being downloaded, the virus executes commands that create a backdoor in the network to transfer files, disable services, and reboot machines. Targeted institutions include the U.S. departments of Defense, Homeland Security, State, Energy, and the Treasury; all five branches of the U.S. military; the National Nuclear Security Administration, and 425 of the Fortune 500 companies, including Cisco, Equifax, MasterCard, and Microsoft. There have been other major cyberattacks in the past, but none has achieved this kind of penetration. By compromising powerful governments and businesses, including some of the most successful technology companies, the SolarWinds exploit shatters **the illusion of** information security. The hack has also spooked the financial services sector. Within hours of the attack’s discovery, U.S. government officials and cybersecurity experts singled out Russia’s Foreign Intelligence Service (known as the SVR) as the likely culprit. Its elite hacking unit, known in cybersecurity circles as APT29 or “Cozy Bear,” is a familiar adversary. It was reportedly behind digital breaches of the White House, State Department, and Joint Chiefs of Staff in 2014 and 2015, as well as the infamous hack of the Democratic National Committee during the 2016 election campaign. The SVR hacked the party’s servers alongside another Russian team, APT28 or “Fancy Bear,” which is overseen by Russia’s military intelligence agency, commonly known as the GRU. It was the GRU that reportedly stole Democratic campaign emails and dumped them online; in 2018, the U.S. Department of Justice indicted 12 Russians suspected of involvement. A few days after the SolarWinds compromise became public, the U.S. Cybersecurity and Infrastructure Security Agency warned that the hack “poses a grave risk” to federal, state, and local governments, as well as to private companies. Even more ominously, the SolarWinds attack stretches far beyond the company’s own direct clients. This is not an open-and-shut case, however. One of the most frustrating challenges for victims of cyberespionage and cyberwarfare is the difficulty of attributing an attack. While the SolarWinds exploit was linked to the SVR in a joint statement by U.S. intelligence agencies, it is by the attack’s very nature impossible to be certain*.* Complicating matters, another piece of malware that targeted SolarWinds at around the same time—dubbed Supernova by Palo Alto Networks’ Unit 42—appears to have been planted by another actor. Meanwhile, US investigators are exploring the possible involvement of JetBrain, a Czech firm founded in Russia that counts SolarWinds among its clients, in spreading infected code via its TeamCity product. For its part, the Russian Embassy in Washington posted a statement on Facebook denying responsibility and claiming that the attacks were opposed to Russia’s foreign-policy interests. It also added that “Russia does not conduct offensive operations in the cyber domain.” Contradicting his own secretary of state and intelligence services, U.S. President Donald Trump agreed with the Russians, hinting that China might be to blame. What also makes the SolarWinds breach different from past attacks was how it was delivered, and the way it could serve as a **beachhead for future attacks**. Unlike in the case of high-profile phishing and hacking exploits against companies such as Equifax and Sony, it is exceedingly difficult to trace how the SolarWinds compromise occurred and determine which data was accessed and pilfered. That’s because the victims of the SolarWinds attack were not confined to a single organization or department, and it is not possible to simply eliminate the malware by wiping the system clean. To the contrary: Hackers ensured that they would have long-term access by adding new credentials and using administrative privileges to grant themselves permissions to access various parts of their victims’ IT infrastructure. What this means is that this hyper-sophisticated campaign—including the theft of information from protected networks—could go on for years. Even more ominously, the SolarWinds attack is what’s known in security circles as a cascading **supply chain compromise**—which means that it stretches far beyond the company’s own direct clients. While no one yet knows just how many governments and businesses are affected, tens of thousands of other entities are at risk, many of which have little to do with SolarWinds. And because the company’s products are designed to monitor digital networks and are therefore at the very heart of IT infrastructure, they have extensive access and few constraints on their reach. Making matters worse, SolarWinds reportedly encouraged customers to relax existing antivirus and security restrictions, which means that even more of the network was accessible than usual. Attackers made use of this unrestricted access to steal permissions and source code from companies such as Microsoft and compromise even more targets. The exploit is a reminder of the blurred lines between espionage and warfare, and the difficulty of formulating a proportional response. As diplomats know well, there is no established international norm against espionage—clandestine information collection is a tolerated feature of international relations. When spying is publicly exposed, what typically follows are some form of condemnation, sanctions, and a focus on shoring up defenses to keep it from happening again. However, the vast scale of the SolarWinds exploit—and the strong probability of others like it that have yet to be detected—should force a rethink. The potential for weaponizing compromised systems, including by sabotaging public utilities (as was the case in a recent cyberattack tit-for-tat between Israel and Iran), poses an **existential threat.** A closed and controllable internet will reinforce the authoritarian tendencies of some governments and **end U.S. dominance of the digital domain.** The SolarWinds compromise raises even more urgent questions about the governance of the internet. It offers a disturbing reminder of the absence of recognized global safeguards to prevent and respond to cyberattacks. States are operating in a cybernetic Wild West, and this is becoming more dangerous in our interconnected world. The status quo suited the main cyberespionage and cyberwar combatants, such as the United States, China, Israel, North Korea, and Russia. But these latest revelations expose the systemic risks of adopting a laissez-faire approach to managing the digital commons. A determined attacker can wreak havoc on just about any target and then just as quickly cover their tracks and disappear into the digital ether. For two decades a governmental group of experts convened by the United Nations has tried to nail down basic norms for cyber-governance, but the major powers still cannot agree on first principles. **The implications of having no established rules are more dangerous than ever.** A major upgrade of internet governance is required. A coalition of like-minded countries, industry, and civil society groups need to push forward a model that ensures, at minimum, protections for critical infrastructure. Current efforts, such as the multi-stakeholder approach for internet governance undertaken by the United Nations, may be necessary, but they have clearly been insufficient in a digital era where massive compromises are likely to become routine. Not waiting for these efforts and their uncertain outcomes, some countries are trying to establish cyberdeterrence, leading to the emergence of de facto rules of engagement. Yet **the risks of catastrophic miscalculation are likewise growing**. Norms related to cyberespionage also need to be established lest it contributes to unintended outcomes with global ramifications.

#### NATO involvement in Ukraine risks Russian cyberattacks on healthcare industry

Diaz 22 [Naomi, “NATO involvement in Russian invasion of Ukraine could trigger cyberattack against US healthcare industry,” 03/28/22, <https://www.beckershospitalreview.com/cybersecurity/nato-involvement-in-russian-invasion-of-ukraine-could-trigger-cyberattack-against-us-healthcare-industry.html>, accessed 07/04/22, GDI-JCR]

The healthcare industry could become the target of Russian cyberattacks if NATO becomes involved in the war in Ukraine, Politico reported March 27. A direct attack on U.S. healthcare organizations is more likely if more countries get involved in the war in Ukraine, or if sanctions cripple Russia, experts told Politico. U.S. officials have issued repeated warnings that U.S. industries, including the healthcare industry, could be targets of Russian-backed hackers in the wake of the invasion of Ukraine. "If NATO gets involved, or if somehow the U.S. gets involved, that's going to change the whole dynamic," Mac McMillan, CEO of cybersecurity firm CynergisTek told Politico. "Russia is being careful not to do anything overtly to the United States at the moment." The U.S. healthcare industry has become a popular target for hackers as it contains a plethora of vulnerable information that can be used to leverage ransom demands from healthcare providers. In 2021, nearly 50 million Americans had their protected health information breached, which is triple the number reported in 2018.

### Impact - Cyber attacks – critical infrastructure impact

#### Critical infrastructure attack risk nuclear meltdowns, blackouts and financial crises

**Iftimie,** Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business**, 2020**

[Ion, “NATO’s needed offensive cyber capabilities” NDC POLICY BRIEF No. 10 – May 2020 <https://www.ndc.nato.int/news/news.php?icode=1441#:~:text=This%20Policy%20Brief%20looks%20at,cyber%20capabilities%20into%20its%20operations> accessed 7/5/22 GDI-TM]

Cyber as a hybrid threat to, and enabler of, military operations

All future military confrontations are expected to be fought with cyber weapons. These offensive cyber capabilities in the hands of adversaries pose a significant threat to the military forces and critical infrastructure of NATO member states; and the Alliance recognizes that cyber-attacks (as hybrid threats) can be as damaging as conventional ones. This is because malicious cyber activities against computers that control physical processes can be as dangerous as threats that are purely physical in nature and could lead to explosions, nuclear meltdowns, blackouts, or financial crises. As put by NATO Secretary General, “in just minutes, a single cyberattack can inflict billions of dollars’ worth of damage to our economies, bring global companies to a standstill, paralyze our critical infrastructure, undermine our democracies and cripple our military capabilities”.4

### Impact – Critical Infrastructure

#### Infrastructure attacks are a unique terminal risk, threatening economic and societal collapse.

Murphy 19 [Hannah, Tech Correspondent at Financial Times, 10-13-2019,   
“Companies urged to bolster infrastructure cyber defences,” Financial Times, <https://www.ft.com/content/797e1e5e-ca53-11e9-af46-b09e8bfe60c0>, accessed 07/04/22, GDI-JCR]

Hackers have traditionally focused their attention on computer software, resulting in a mushrooming of cyber security companies that promise protections for office-based clients. But there is another, less well-known hacking threat: cyber attacks on big corporate operations, such as **manufacturing facilities or power plants, as well as other vital infrastructure.** Such attacks are becoming more commonplace, fuelling concerns that companies should ramp up their efforts to guard against them. This is no small challenge. For companies with operational technology — the computerised systems used to control industrial operations — the risks of a breach are plentiful; disruptions to machinery processes could dent revenues or cause an accident. For those involved in “critical infrastructure” — the **dams, energy, oil and gas facilities** required for society to function smoothly — the risks are more dramatic and may attract nation state hackers, not just those seeking financial gain. “Our economy will disappear, society will collapse — and these things are possible,” says Sujeet Shenoi, professor of computer science at the University of Tulsa, who has been involved in multiple government-led critical infrastructure projects. “**There’s never been a war** in human history **where** the **critical infrastructure hasn’t been damaged**.” He notes that some 80 per cent of critical infrastructure in the US is privately run. “These companies are not prepared for [a cyber attack]. You need extremely well trained people,” he says, noting the many former government experts are moving into the sector. Historically, critical infrastructure and operational technology were kept separate from the computer networks typically used in corporate headquarters. However, those worlds are now converging as outdated analogue systems have become increasingly digitised. “Systems that have been developed over 30 or 40 years are having the internet introduced to them,” says Casey Ellis, founder and chief technology officer at Bugcrowd, a cyber security group. But **retrofitting systems** that were never intended to be on the internet **creates new opportunities for hackers**, he says. “The attack surface is expanding rapidly.” As with normal IT systems, ransomware and malware can be used to infect operational technology and critical infrastructure. The most high-profile worm was the 2010 Stuxnet malware, which targeted Iran’s nuclear facilities. Operations at the food company Mondelez and drugmaker Merck were disrupted by the ransomware dubbed NotPetya in 2017. Ukraine has suffered a spate of attacks on its power grid system recently, and earlier this year, Norwegian aluminium maker Norsk Hydro had to freeze operations earlier after it fell victim to ransomware. While the marketplace for cyber security companies offering support to such groups is smaller than the traditional IT security space, experts caution that companies should take action. Moves might include assessing company **systems to ensure staff know what devices are connected to the network,** testing and monitoring those systems, and devising a plan for worst-case scenarios. Above all, companies should isolate the most critical systems to ensure they can keep them operating no matter what, says Pedro Abreu, chief product and strategy officer at online security company Forescout, who dubs the process “containing the blast area”. “If a WannaCry [attack] happens, I want to [be able to] shut down that facility or country” while the rest of the network remains running, he says. Various sectors are equipped differently, experts say. Where deep-pocketed energy, and oil and gas groups have been able to pour investment into bolstering their protections, others, such as the water sector, are thought to be lagging. To their advantage, Michael Fabian, principal consultant at Synopsys, notes that operational technology systems are “very restrictive”, meaning that “some expertise is needed to hack [them]”. By comparison, “**people providing consumer services have a massive attack surface**,” he says, citing the likes of Citibank, Target or Amazon. Nevertheless, operational technology systems have their own nuances. First, testing them for vulnerabilities can be difficult because the systems are too sensitive or essential to pause. “There are things that are ultra critical that we can’t put at risk by testing them, but we are doing just that — putting them at risk — by not testing them,” says Charles Henderson, global head of IBM’s hacking unit X-Force Red. This means cyber security companies may have to test for vulnerabilities against a less reliable reproduction of an actual system. And if a problem is uncovered, it is harder to fix. “The life cycles of those systems in the field is extraordinarily long,” says Eric Cornelius, chief product officer at BlackBerry Cylance, a cyber security group. Moreover, even if cyber security companies offer solutions, it can be many years before a system can be updated. For example, many companies would opt to rebuild an offshore gas plant once it has finally stopped running, rather than upgrade at great cost, Mr Cornelius says.

### Impact - Critical Infrastructure Snowballs

#### Attacks on critical infrastructure on the rise. Attacks can ripple across sectors.

Horwitz 21 [Lauren, senior content director at IoT Today, winner of the Silver Award from the American Society of Business Publican Editors, “IIoT Software Vulnerabilities Fuel Critical Infrastructure Attacks—Again,” 08/16/21, <https://www.iotworldtoday.com/2021/08/16/iiot-software-vulnerabilities-fuel-critical-infrastructure-attacks-again/>, accessed 07/04/22, GDI-JCR]

In August 2021, Forescout Research Labs and JFrog Security Research identified 14 vulnerabilities affecting the NicheStack TCP/IP stack, which the organizations dubbed INFRA:HALT. TCP/IP stacks enable vendors to implement basic network communications for IP-connected systems, including IT, operational technology (OT) and Industrial Internet of Things (IoT) devices. Indeed, NicheStack is present in myriad OT devices that are commonly used in several critical infrastructure sectors, such as manufacturing plants, water treatment, power generation and more. The new vulnerabilities enable remote code execution, denial of service, information leak, TCP spoofing, or DNS cache poisoning. Critical Infrastructure Attacks Reveal ICS Weak Spots The vulnerabilities discovered illuminate the risk to critical infrastructure systems should they be compromised by malicious actors. These systems are aging and vulnerable, said experts. “It is … an unfortunate example of the huge vulnerability of an aging infrastructure that has been connected, directly or indirectly, to the Internet,” said Curtis Simpson, CISO at Armis in a recent article on increasing attacks on critical infrastructure. Forrester Research’s Brian Kim said that critical infrastructure organizations need to focus on identifying vulnerable OT devices within their estate, then focus on building a zero-trust strategy, using least privilege and network segmentation to prevent malicious actors from gaining access to critical systems. “One of the best ways we can reduce the impact of a breach is a zero-trust strategy by limiting the communications of these ICS [industrial control systems],” Kime said.. “We can create an allow list that only allows communications with control systems that run a process–allowing least privilege for network connections … is a best practice. And ideally, we should have a barrier between IT and OT and segment each facility to have its own network. JFrog and Forescout research teams will present a webinar on August 19 to provide additional information about how these vulnerabilities were identified and how they can be mitigated. Critical Infrastructure Attacks on the Rise. Last year, there were some 65,000 ransomware attacks, according to the Recorded Future, a Boston-based cybersecurity firm. Cyberattacks on critical infrastructure present certain benefits from the attackers’ perspective, even if the objective of attackers is not a payout. First, malicious attackers can gain access to these vulnerable devices with ease, as OT devices may be older and lack the security protocols of newer technologies. Second, once critical operations are affected, it can grind operations to a halt. Affected organizations have great incentive to pay ransomware demands just r resume operations. “The nature of these vulnerabilities could lead to heightened risk and expose national critical infrastructure at a time when the industry is seeing an increase in OT attacks against global utilities, oil and gas pipeline operators as well as healthcare and the supply chain,” wrote Forescout Research Labs in an announcement regarding the vulnerabilities. Third, access to OT devices can always provide entrée to other systems within organizations. “Once accessed, the stack becomes a vulnerable entry point to spread infectious malware across IT networks,” the researchers continued. Kime noted that attacks like the recent one on Colonial Pipeline revealed that critical infrastructure systems are interconnected, creating the opportunity for ripple effects within these systems, then across the chain to IT systems as well. “An event like Colonial Pipeline has revealed that these are more systems of systems rather than independent, isolated sectors that operate within their own little world,” Kime said. Ultimately, Kime noted, critical infrastructure operators need to shift their perspective to enable more thoroughgoing protection of the critical infrastructure they manage. “There should be a strong focus among critical infrastructure on not just security but resilience,” he said.

#### Network insecurity invites catastrophic attack on infrastructure

Cyrus 21 [Callum, Assistant Editor & Reporter, “Striking Back: An IoT Security Guide for Critical Infrastructure,” 09/06/21, <https://www.iotworldtoday.com/guide/striking-back-an-iot-security-guide-for-critical-infrastructure/>, accessed 07/04/22, JCR] \*IoT = “Internet of Things”

Securing the Internet of Things (IoT) is now a conundrum for policy makers. Fuel deliveries, health care provision and education systems – it’s become clear that ineffectual IoT defenses will expose sections of infrastructure backbone. Malicious attackers have come to realize that going after critical infrastructure can be profitable and almost certainly can have major disruptive impact. Now that attackers have come to recognize this ROI from assaults on critical infrastructure, it becomes more imperative to shore up these resources from attack. Tackling the problem necessitates rapid provision, implementation and verification of cybersecurity resources. The challenge is that many vital services depend on old technology designed for internal networks, before IoT brought new vulnerable endpoints to the attack surface. IoT has changed infrastructure OT security; malware has become pervasive enough to break into systems and, in some cases, extort cash from victims. Hostile nations shelter attackers, which enables the virtual plunder of enemies and stymie any chance of prosecution. A response must be comprehensive in scope but are complicated by the need to avoid unnecessary shutdowns, which also cause operational damage. “Implementing IoT in a world which hasn’t traditionally been connected can lead to improper security hygiene and, thus, higher risk of a breach or attack,” said Hollie Hennessy, cybersecurity expert at analyst firm Omdia. “A breach could result in devastating impact on a national scale. These industries now need to balance this risk, alongside the risk of operational outage, while securing and ensuring visibility across a large, growing portfolio of connected devices,”

### Impact – Water Attacks

#### Shout out to ’21 Scholars!

#### An attack on the water supply risks contamination and disruption – wreaking havoc on public health and services

Maiolo, University of Calabria Professor of Hydraulic Constructions, et al., 18

[Mario, Daniella Pantusa, Environmental Engineering PhD, Hamidi Aziz, Professor of Environmental Engineering, 04-01-2018, Cogent Engineering, “Infrastructure Vulnerability Index of drinking water systems to terrorist attacks,” <https://www.tandfonline.com/doi/full/10.1080/23311916.2018.1456710>, accessed 06-27-2021, HSP]

Regarding water systems they are vulnerable to both manmade and natural threats including, e.g. earthquakes, flood, droughts, terrorist attacks. Safe drinking water is central to the life of an individual and of society; a drinking water contamination incident or the denial of drinking water services would have far-reaching public health, economic, environmental, and psychological impacts. Other critical services such as fire protection, healthcare, and heating and cooling processes would also be disrupted by the interruption or cessation of drinking water service, resulting in significant consequences to the national or regional economies (Department of Homeland Security & US EPA, 2015). Therefore, the issue of the security and risk assessment of such systems is of increasing importance. In this context, numerous definitions exist for the variables of interest in a risk assessment study. These variables include: event or threat, outcome, scenario, exposure, vulnerability, consequences, risk.

Regarding vulnerability, Ezell (2007) argues that a relationship emerges from the literature between vulnerability and risk. Vulnerability highlights the notion of susceptibility to a scenario whereas risk focuses on the severity of consequences to a scenario. As described in Thomas (2006), the National Water Resource Association, NWRA (2002) defines a vulnerability assessment as the identification of weaknesses in security, focusing on defined threats that could compromise the ability to provide a service, while National Oceanic and Atmospheric Administration (2002), defines vulnerability as the susceptibility of resources/assets to negative impacts from threat events. Hence, a vulnerability assessment accounts for the assets that could deter or defray unwanted outcomes from an event and for their susceptibility to failure. Vulnerability is defined by Haimes and Horowitz (2004) to be the manifestation of the inherent states of a system (e.g. physical, technical, organizational, and cultural) that can be exploited by an adversary to cause harm or damage. Copeland (2010) identifies the most likely “vulnerable” water systems to be the relatively small number of water systems serving the largest populated cities in the country.

The terrorist events of recent years have increased the attention on the safety aspects of water infrastructure. In the United States, just after September 11, 2001, the United States Congress approved a series of acts pertaining to vulnerability assessments to assess potential threats to such systems and to identify corrective actions. Over the years various vulnerability assessment methodologies and tools were developed and several studies were conducted on this issue by various institutions not only in USA but worldwide (APWA, AMWA, NACWA, & WEF, 2007; Centre for European Reform [CER], 2005; HSPDs, 2002; Istituto Superiore di Sanità, 2005; US EPA, 2003, 2007, 2009, 2010).

Water systems are vulnerable to a range of intentional threats including contamination, damaged or sabotaged through physical destruction and cyber attack.

Consequences of a water contamination can be significant. A contamination event in a water system can adversely affect the people, the businesses, and the community it serves due to fear, loss of water service, significant economic costs for decontamination and recovery, and the magnitude of adverse public health effects (Clark & Hakim, 2014).

Physical damage has consequences mainly related to the interruption of service and may also cause large economic harms. Vulnerable characteristics of water systems include their physical attributes, e.g. reservoirs, tanks, and pump stations. In addition to physical attributes, a water utility’s SCADA could be vulnerable to cyber attack, for example, turning pumps on or off, filling or emptying tanks inappropriately, or causing water hammer events (Clark & Hakim, 2014).

#### Contamination risks poisoning millions

Weddell, USA Today investigative reporter, & Meyer, USA Today veteran correspondent, 21

[Katie Wedell is an investigative reporter for USA today and Josh Meyer is a veteran correspondent focusing on domestic, national and global security issues, including terrorism, extremism, cybersecurity and transnational criminal organizations, 06-23-2021, USA Today, “How vulnerable is US to hacks?; Worst-case scenarios could be devastating,” Nexis, accessed 06-26-2021, HSP]

Experts said the scariest scenarios involve a hacker either purposefully or inadvertently changing the operations of an industrial control system, such as that for a pipeline, a dam or a water works.

Such an intrusion could lead to prolonged outages, destroy infrastructure and even kill.

When Iranian hackers broke into the computer system that controls the Bowman Avenue Dam in Rye Brook, New York, in 2013, they snooped on passwords and usernames but didn't seize control of the computerized floodgates, which were disconnected for maintenance.

They proved they could sneak into critical infrastructure systems and hijack any one of hundreds of flood control systems in the USA, sending potentially fatal floods toward downriver cities, or wipe out hydro-electric power and water supplies to millions.

Sen. Chuck Schumer, D-N.Y., called it a wake-up call in 2015 when revelations about the breach became public. The nation's critical infrastructure is vulnerable to criminals and needs to be strengthened, he said.

"This cyberattack surely serves as a bucket of ice water to the face," Schumer said.

But it didn't.

Colonial shut down its pipeline out of an abundance of caution. Hackers locked up the company's corporate computer system - possibly affecting email, billing and payroll. The criminals did not access the computer system that controls the flow of fuel through more than 5,000 miles of pipeline, but the company was worried that system might not be completely separate, experts said.

"Imagine loss of control of the pipeline itself and what could have resulted," said Mark Ostrowski, head of engineering for the East Coast at Check Point Software Technologies.

Water

An intrusion into the Oldsmar, Florida, water system in February highlighted vulnerabilities in the water treatment industry.

A hacker broke in through remote access software and briefly increased the amount of sodium hydroxide from 100 parts per million to 11,100 parts per million. Sodium hydroxide, also called lye, can cause irritation, burns and other complications in too large quantities.

A supervisor noticed the tampering - he could see the intruder moving a cursor across the screen, changing settings - and intervened immediately to reverse it. The city said sensors and other safeguards would have caught the problem. Oldsmar, a city of 15,000 residents, is about 15 miles northwest of Tampa.

In March, the Justice Department accused a former Kansas utility worker of remotely tampering with a public water system's cleaning procedures. Last week, NBC News reported that a hacker in January tried to poison an unnamed water treatment plant serving parts of the San Francisco Bay Area.

"If you're a state actor or a highly integrated or networked group of hackers, Black Hat hackers, you can mess with the chlorine levels in your water or the arsenic levels in your water and poison the entire New York City water supply overnight," Bolton said. "New York City wakes up, everyone has a glass of water in the morning or cooks something with water in the morning - and you poison millions of people."

### Impact – grid

#### Shout out to ’21 Scholars

#### Disruption of critical infrastructure would cause catastrophic loss of life

Weiss, United Medical Instruments, National Sales Director & Weiss, UCLA-Olive View Medical Center neurosurgeon, 19

[Matthew & Martin, 5/29/2019, Energy, Sustainability and Society, “An assessment of threats to the American power grid”, Volume 9, No. 18, <https://energsustainsoc.biomedcentral.com/articles/10.1186/s13705-019-0199-y#Sec2>, accessed 7-3-21, AFB]

Consequences of a sustained power outage

The EMP Commission states “Should significant parts of the electrical power infrastructure be lost for any substantial period of time, the Commission believes that the consequences are likely to be catastrophic, and many people will die for the lack of the basic elements necessary to sustain life in dense urban and suburban communities.” [67].

Space constraints preclude discussion on how the loss of the grid would render synthesis and distribution of oil and gas inoperative. Telecommunications would collapse, as would finance and banking. Virtually all technology, infrastructure, and services require electricity.

An EMP attack that collapses the electric power grid will collapse the water infrastructure—the delivery and purification of water and the removal and treatment of wastewater and sewage. Outbreaks that would result from the failure of these systems include cholera. It is problematic if fuel will be available to boil water. Lack of water will cause death in 3 to 4 days [68].

Food production would also collapse. Crops and livestock require water delivered by electronically powered pumps. Tractors, harvesters, and other farm equipment run on petroleum products supplied by an infrastructure (pumps, pipelines) that require electricity. The plants that make fertilizer, insecticides, and feed also require electricity. Gas pumps that fuel the trucks that distribute food require electricity. Food processing requires electricity.

In 1900, nearly 40% of the population lived on farms. That percentage is now less than 2% [69]. It is through technology that 2% of the population can feed the other 98% [68]. The acreage under cultivation today is only 6% more than in 1900, yet productivity has increased 50 fold [69].

As stated by Dr. Lowell L Wood in Congressional testimony:

“If we were no longer able to fuel our agricultural machine in the country, the food production of the country would simply stop, because we do not have the horses and mules that used to tow agricultural gear around in the 1880s and 1890s”.

“So the situation would be exceedingly adverse if both electricity and the fuel that electricity moves around the country……… stayed away for a substantial period of time, we would miss the harvest, and we would starve the following winter” [70].

People can live for 1–2 months without food, but after 5 days, they have difficulty thinking and at 2 weeks they are incapacitated [68]. There is typically a 30-day perishable food supply at regional warehouses but most would be destroyed with the loss of refrigeration [69]. The EMP Commission has suggested food be stockpiled for a possible EMP event.

### Impact - Cyber attacks – NATO operations [need offensive capabilities]

#### Increased cyber activities disrupt NATO logistics and forward operations – integration and coordination of offensive cyber necessary to address

**Iftimie,** Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business**, 2020**

[Ion, “NATO’s needed offensive cyber capabilities” NDC POLICY BRIEF No. 10 – May 2020 <https://www.ndc.nato.int/news/news.php?icode=1441#:~:text=This%20Policy%20Brief%20looks%20at,cyber%20capabilities%20into%20its%20operations> accessed 7/5/22 GDI-TM]

Over the past decade, Allies have identified a steep increase in cyber activities targeting the critical infrastructure sectors that NATO military operations rely upon. Directly or indirectly, these malicious cyber activities can also disrupt the Alliance’s logistics and forward operations. NATO’s commitment to “operate and defend itself ”5 in the cyber domain as effectively as in the geographic domains came, thus, as a direct recognition of cyber as a hybrid threat to both the Allies and the Alliance. Compared to the air, land and sea domains, the cyber domain is not constrained by national borders (although certain physical aspects of it might be located within them). This distinction between the cyber and the geographic domains is important to note, because NATO was founded in response to external military threats without the right to intervene in internal security matters, where member states maintain the monopoly over the use of force. In the cyber domain, the distinction between internal and external security threats is harder to ascertain. When integrating offensive cyber capabilities into its defence and deterrence mandate, NATO would inevitably tackle certain aspects inherent to internal security; and yet, not legally infringe on the sovereignty of the Allies as long as effects amounting to force or intervention are not employed against the physical systems residing in these nations.6 Operating in the cyber domain requires, thus, that member states better integrate their offensive cyber capabilities into NATO operations not just to win future wars, but also to avoid elements of friction between Allies, which may arise from unilateral cyber effects to defend critical infrastructure.

### Impact - Cyber threats– Russia

#### Russia uses electronic warfare as part of whole strategy including kinetic combat operations requiring a NATO response

**Maigre, 2022**

[Merle, senior cybersecurity expert at e-Governance Academy in Estonia. In 2017–2018, she served as director of the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE), “NATO IN A NEW ERA: GLOBAL SHIFTS, GLOBAL CHALLENGES NATO’s Role in Global Cyber Security” German Marshal Fund APRIL 06, 2022 [https://www.gmfus.org/news/natos-role-global-cyber-security accessed jcp-TM 6/8](https://www.gmfus.org/news/natos-role-global-cyber-security%20accessed%20jcp-TM%206/8)]

\*EW- electronic warfare

While they can offer some advantages in military operations, cyberattacks also have limitations in feasi- bility and effect. In the event of military attacks, military objectives can be supported by intelligence-gathering operations, operations aimed at disrupting the oppo- nent’s military, and psychological operations against the opponent’s public.15 Nevertheless, sophisticated cyberattacks require a lot of luck, but also skill and time—for example, the 75-minute power outage in 2016 in Kyiv took 31 months to prepare.16

The Russian military exercise Zapad 2021 in September included one of the largest uses of elec- tronic warfare, which has been increasingly on display in eastern Ukraine since 2014 and in Syria since 2015. Roger McDermott, a leading analyst on Russian military developments has described that “Russia’s growing technological advances in EW [electronic warfare] will allow its forces to jam, disrupt, and interfere with NATO communications, radar and other sensor systems, unmanned aerial vehicles, and other assets.”17 Russia sees EW as a seam- less whole, ranging from kinetic combat operations on the battlefield to missions in cyberspace and the information domain.18 While there were no public sources confirming any navigation or communica- tions disruption by the Baltic-Polish defense leader- ship during Zapad 2021, it is nevertheless important that NATO continue to adapt to the evolving cyber- threat landscape.

### Impact - Disinformation

#### state actors and non-state actors use cyberattacks to target democratic institutions through disinformation and disrupt NATO’s reliability

**Păunescu, 2021**

[Dragoș-Mihai, PnD in International relations at the Carol I National Defence University, “NATO’S ENCOUNTERS IN THE CYBER DOMAIN”, 11/9/2021, Vol 17 no 1 2021 – Proceedings of the 17th International Scientific Conference Strategies XXI, https://revista.unap.ro/index.php/XXI\_FSA/article/view/1274/, accessed 6/29/22, GDI- CC]

Since the end of the Cold War, radical groups, terrorist organizations together with  intelligence agencies and military regimes that controlled weapons of mass destruction, represented  the most plausible world’s threats. In the last two decades, the security environment witnessed a  significant shift: the world’s most relevant state actors shifted the focus from being nuclear powers  competing in an arms race to becoming cyber powers that allows much softer tools to be employed to  achieve military objectives.

Nowadays increasing connectivity and reliance on information technology is a vulnerability  recognized by NATO and national security doctrine as it is being targeted by cyber-attacks and  subversion of democratic institutions carried out by disinformation.

Just as in the traditional domains, cyber threats for NATO are emerging from a wide range of  sources that include state actors, especially China and Russia, but also a significant number of non state actors, including proxies and criminal organizations. Cyber operations performed by opposite  actors are likely to target NATO Computer & Information Systems (CIS) infrastructure and data bases  to affect the communications’ confidentiality, reliability or availability either in reality or in perception.

Due to the interconnected and omnipresent nature of cyberspace and the fact that cyber  operations are cheap, accessible, discreet, stealthy and have the element of plausible deniability, they  can result in disproportionate effects against a technology-dependent organization or even nation.

### Impact – C3I Escalation

#### Cyberattacks on dual-use C3I system risk escalation from entanglement, misinterpretation, and preemptive countermeasures

**Afina, et. al, 20**

[Yasmin Afina, Research Assistant, International Security Program, and Calum Inverarity, Research Analyst, International Security Program, and Beyza Unal, Research Fellow, International Security Program, “Ensuring Cyber Resilience in NATO’s Command, Control and Communication Systems”, <https://www.chathamhouse.org/2020/07/ensuring-cyber-resilience-natos-command-control-and-communication-systems-0/about-authors>, Chatham House, 17 July 2020, accessed 29 June 2022, GDI-LR]

\*C3- command, control, communications

The increasing reliance on dual-use C3 assets, those used both for conventional and nuclear operations, raises the issue of entanglement and the risk of rapid escalation. These dual-use assets can range from communications satellites to early warning systems, radars and transmitters. According to recent research, notably by James M. Acton, parties to a conflict ‘could have strong incentives to attack the adversary’s dual-use C3I [command, control, communication and intelligence] capabilities to undermine its nonnuclear operations’.117 An attack on a dual-use C3 asset would particularly hold strong incentives for adversaries possessing nuclear weapons and not ruling out their potential use. For instance, a cyberattack on early warning satellites will provide a tremendous advantage to the adversary by either delaying the detection of a missile launch (conventional or nuclear) or even preventing it from being identified in the first place.

James M. Acton addresses two mechanisms that lead to escalation.118 First is a ‘misinterpreted warning’, probably at a time of crisis, where a state’s dual-use C3 assets are targeted by conventional weapons or cyber interferences and the target state might misinterpret these attacks as ‘preparations for an incoming use of nuclear weapons’ by their adversary.119 The targeted state might miscalculate and respond in a highly escalatory way that leads to full-scale conventional or nuclear war. Second, if a state’s C3 capability was attacked by conventional means, it might lose its advantage to destroy an adversary’s nuclear weapon systems. In order to prevent such a situation happening, the state might use pre-emptive countermeasures that would themselves lead to escalation,120 thus adding nuclear ‘use it or lose it’ pressures to conventional crises.

It is important to note that the escalation mechanisms identified by Acton rest on hypothetical situations in which states that have been forced, for the purposes of the argument, into adopting an inherently escalatory posture; in reality, this may not be the inevitable outcome. The role of conventional forces and cyber interferences is highlighted primarily and under specific conditions as a route to escalation, rather than also as a source of potential de-escalation. Although risks of escalation through entanglement might be greater in some cases, it is hard to judge a state’s possible actions only by counting its conventional or nuclear capabilities or by assigning an escalatory role to them. Escalation is a choice, and the logic of escalation mechanisms removes the factor of human agency for conflict avoidance. Ultimately, survival of a state may not, in all instances, be linked to the survival of its nuclear forces.

#### Risk of escalation to global nuclear war is high

Orlov 20 [Vladimir, Head of the Center for Global Trends and International Organizations at the Diplomatic Academy, Ministry of Foreign Affairs of the Russian Federation, Professor at MGIMO University, “‘No Holds Barred’ and the New Vulnerability: Are We in for a Re-Run of the Cuban Missile Crisis in Cyberspace?,” 2/14/20, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3538078>, accessed 07/04/22, GDI-JCR]

Not hundred per cent of the dialogue has been frozen, fortunately. Certain informal, mostly offthe-record, meetings of US and Russian experts on cyber agenda continue taking place, both through Track 2 and Track 1.5. One of the most intellectually stimulating meetings, with frank exchanges, took place in Vienna in December 2018. The report produced after the meeting stressed “the significant risk […] that cyber-attacks could conceivably lead to a military escalation that may further trigger a nuclear weapons exchange, a fact that became more explicit with the adoption of the current Nuclear Posture Review. This issue gets complicated given that third parties may have the capabilities to invoke a cyber conflict between Russia and the United States. Whether a country or a non-state actor, they could put the two countries on the verge of an armed conflict by attacking critical infrastructure of either of them and making it look as if the aggressor were the other one”[22]. However, one should have no illusion: such informal meetings may be fully fruitful only when their reports and policy recommendations are utilized by the governments. And for that, a warmer climate in bilateral relations is a must. So far, we see exactly the opposite: mercury falling to freezing levels. Risk of cyber clashes growing into a chaotic global cyber war has been emphasized by the UN Secretary-General Antonio Guterres in his Agenda for Disarmament: “Malicious acts in cyberspace are contributing to diminishing trust among States… States should implement the recommendations elaborated under the auspices of the General Assembly, which aim at building international confidence and greater responsibility in the use of cyberspace.[23]” However, as the members of the US-Russian Track 1.5 working group on strategic stability recently concluded, “without a constructive dialogue on cyber issues between the United States and Russia, the world would most likely fail to agree on any norms of responsible behavior of states in cyber space”[24]. Do we really have to survive a cyber equivalent of the Cuban Missile Crisis to realize the importance of achieving some kind of agreement on cyber issues, and on the broader agenda of international information security?[25] Or is that kind of talk plain old alarmism? I don’t want to sound a fatalist, but I am even less keen on sounding like an ostrich that’s buried its head in the sand. We cannot ignore the obvious: whether the world’s most powerful actors like it or not, the world is sliding to another major crisis like the one in 1962. The cyber war is already raging. There are no rules of engagement in that war. The uncertainty is high. The spiral of tension is getting out of control. The cyber arms race is gaining momentum. And there are no guarantees that the next crisis will be controllable, or that it will result in a catharsis as far as international information security regulation is concerned. There’s no telling what will happen once the cyber genie is out of the bottle.

### Impact - Cyber warfare

#### Cyberwarfare causes collateral damage that outrides conventional

**Bonefeld-Dahl**, Director General of DIGITALEUROPE, **2022**

(Cecilia, “Preparing Europe for cyberwarfare,” The Parliament Magazine, March 28, 2022, lexis, accessed 6/28/2022, gdi-tmur)

\*ICT = Information and Communication Technology

The invasion of Ukraine shows why we must be serious about building Europe's digital shield. Cybersecurity must no longer be seen as a secondary concern. It is essential that we use all available tools and resources to protect ourselves.

Russia invaded Ukraine in February 2022, but the war had begun many years earlier. Since at least 2014, there has been an almost constant barrage of cyber-attacks on Ukrainian critical infrastructure.

One example is the 'NotPetya' ransomware attack of 2017, which resulted in over 2000 attacks across the world. Microsoft Defender Security Research estimated that the vast majority of infections hit Ukraine. One of the major targets was the National Bank of Ukraine, as well as government ministries, transport systems and, worryingly, the Chernobyl radiation monitoring system.

As well as destabilising Ukraine, the collateral damage was huge. According to Wired, the White House put the final figure on the damage at $10 billion. Both the UK and US attributed the attacks to the Russian security services, and the EU levied sanctions against individuals in Russia suspected to be involved.

As we have now seen, cyberwarfare can outride traditional warfare. By breaking into the ICT systems of ministries, hospitals, media outlets and other critical infrastructure, cyber-attacks can grind government business to a halt, disrupt vital supplies and sow confusion.

### AT: Squo solves – national cybersecurity efforts sufficient

#### Cooperation between NATO nations is key for cybersecurity- NATO facilitates development, information sharing, and better protected networks.

**Ackerman 20**

(Robert Ackerman, Retired Editor in Chief, SIGNAL Magazine, and Senior Director, SIGNAL Media; former war correspondent at AFCEA International, graduated from Boston University in communications, “NATO Expands Cybersecurity Activities” Signal Magazine, May 2020, Proquest, accessed 6/29 GDI- TMK)

From partnerships with industry to dual-use Al cyber capabilities, the alliance is playing the field. NATO is doubling down on cyberspace defense with increased partnerships and new technology thrusts. Information exchanges on threats and solutions, coupled with research into exotic capabilities such as artificial intelligence, are part of alliance efforts to secure its own networks and aid allies in the cybersecurity fight. The threats the alliance networks face constitute relatively the same ones confronting other organizations. NATO faces the double challenge of securing its own networks and information assets, as well as helping its member nations improve their own national cyber resilience. In the past, NATO viewed cybersecurity as somewhat of a technical challenge. But that perspective evolved over time as the cyberscape underwent changes. This came less from choice and more of necessity as a result of the amount and content of malicious cyber activity, explains Christian Liflander, head of section, Cyber Defense, Emerging Challenges Division, NATO. NATO does not have any tanks, ships or aircraft, with a few exceptions such as the AWACS aircraft operated from Geilenkirchen Air Base in Germany. However, when it comes to cyber defense, NATO has its own capability that defends its networks and maintains their operation in the face of adversarial actions. Unlike combat forces, cyber defenders are all NATO staff members. This force is not dependent on individuals loaned from member nations. Instead, it staffs its own personnel to form a core of cybersecurity expertise. One constant over the next few years will be the need to remain resilient, Liflander states. NATO networks must be built and operated in ways that deny benefits to cyber attackers. This includes NATO being able to run networks in a degraded environment. Yet this is easier said than done, he offers. While NATO will continuously work to improve its cyber defense, its adversaries also will become more sophisticated and capable. "The changing threat landscape will continue to challenge us," Liflander says. "I don't really think there will be an endpoint where we can declare mission accomplished," he states. "It is a continuous task, a continuous mission, making sure that networks are well-defended." The alliance is looking to manage risk differently, he offers. "It's not only a technical risk that we're looking at; it's a risk to a mission." The alliance must be certain that an operational commander is able to operate in cyberspace with the same freedom of maneuver available on land, at sea and in the air. National cybersecurity resilience also presents the dichotomy of continuity and change. Member nations often face threats to their critical infrastructure or other soft elements in addition to hardened government networks. Attackers can be nation-states, organized criminals, individual hacktivists or even those working as proxies, although the vast majority of attacks are nonstate activities such as ransomware. "NATO's role in helping allies improve national resilience will become even more critical," Liflander offers. And NATO is no different in terms of potential threats to its networks. The alliance is looking at issues such as military supply chains, training and education, situational awareness and resourcing cyber defense. But Liflander emphasizes that NATO does not want to fall into the trap of viewing cybersecurity as simply a technology issue. This brings into play training and cyber hygiene, he notes. Neither the alliance nor its member nations have unlimited resources for cyber defense, so they must ensure that their resources are applied effectively, Liflander notes. NATO will serve as an important facilitator for allies as they develop their national cyber capabilities. "It starts with resources. If you're not spending resources, you're not going to improve," he declares. Liflander offers that NATO is one of the most sophisticated cyber actors among international organizations, and that comes from both its mandate and its partnered approach. "We have quite understood that no one, however powerful, can go it alone," he declares. "You need to cooperate. That's a prerequisite in order to do your job well." NATO's network has a global footprint, and the alliance is responsible for its cyber defense. The member nations are responsible for their own national networks. But, Liflander points out, dedicated cyber attackers do not necessarily differentiate between the two types. Depending on vulnerabilities, they can be exploited in both sets of networks, he says. Cybersecurity among NATO and its members is almost symbiotic, he continues. Malicious activity that takes place in NATO's network almost certainly can be found in individual nations' networks, which increases the importance of information sharing among the allies. Such malicious cyber activity can target military aspects as well as have effects on the civilian critical infrastructure. Because of these linkages between military and civilian spheres, NATO is working on critical infrastructure protection, including telecommunications. "Not making sure that your national networks are well-defended can create and introduce a vulnerability that can also be exploited for political purposes," Liflander offers. "It can undermine unity or allied cohesion for some other purposes."

## China

### NATO response Ukraine – key to Taiwan

#### International leadership on Ukraine key to Taiwan sovereignty – cooperation and planning over Ukraine spillover

**Zelikow,** Professor of History at the University of Virginia and Executive Director of the 9/11 Commission, **2022**

[Philip, “The Hollow Order Rebuilding an International System That Works” Foreign Affairs July/August 2022 <https://www.foreignaffairs.com/articles/world/2022-06-21/hollow-order-international-system?utm_medium=social&utm_campaign=tw_daily_soc&utm_source=twitter_posts> accessed July 4 GDI-TM]

ON THE CLOCK

The need for a new world order is apparent, and policymakers are already at work trying to address the evident failures of the existing system. In doing so, they have again invoked values and philosophies. Biden, for instance, has described the war in Ukraine and tensions with China as part of “an ongoing battle in the world between democracy and autocracy.” French President Emmanuel Macron declared that Russia’s invasion had called democracy “into question before our eyes.”

Yet the best, most unifying organizing principle for what will be the fourth system of world order is practical problem solving. It’s convenient to perceive the world as apportioned into democracies and autocracies, but it is also self-regarding and divisive. People are more likely to come together around problems that command wide interest and embrace corrective actions that require wide participation. After years of theatrics that have resulted in catastrophes and growing fear, the system can no longer afford to place inclusiveness and symbolism ahead of teamwork and results.

To erect a new system, policymakers should start by addressing the most pressing current crisis: Ukraine. The military issues are already receiving intense attention. Yet economic issues may determine the outcome of the war as Russia tries to break not just Ukraine’s armed forces but its hope for a better future. The G-7 and allied countries must prepare a far-reaching strategy of Ukrainian reconstruction, tied to the ongoing process of EU accession for Ukraine and funded in part by frozen Russian state and state-related assets. Such an action, with expert assistance from EU staff and hundreds of billions of dollars in reconstruction aid, would be a peaceful counteroffensive on an epic scale. Ultimately, it would help Ukrainians believe and see that they can have a better future.

But to address the challenges Russia has created, the free world can’t focus only on Ukraine. Unless a fundamental change occurs in Moscow, the United States and Europe will also have to redefine their defense for the 2020s, from the Arctic to the Mediterranean (a process already underway), to deter further aggression. And sadly, when a leader such as Putin makes ominous threats about escalation, the United States and its friends must develop credible plans for a wider war with Russia.

For this new system to succeed at keeping the peace, the responsible countries will also need to engage in military planning beyond Europe. For example, the war in Ukraine affects diplomatic calculations on all sides of the dispute over Taiwan’s sovereignty. Because of the international response to aid Ukraine, Beijing can see that Japan, the United States, and other countries now feel much greater pressure to defend Taiwan. It is now harder for China to sustain the fiction that it can peacefully reunify the island with the mainland. The free world’s ability to defend Taiwan has long involved considerable pretense, but the war in Ukraine has also revealed that well-prepared global economic action may be a more powerful and less provocative way to deter conflict than reliance on more traditional military tools. China should see that Japan and others around the world are preparing for the possible financial and commercial earthquake that would immediately accompany a war with the United States and Japan over Taiwan.

### China internal link – monitoring NATO response

#### China monitoring NATO cohesion and responses to the Ukraine invasion to prepare for war on Taiwan

Helmy, 2022

[Nadia, Professor of Political Science, Faculty of Politics and Economics at the Beni Suef University in Egypt, "U.S- NATO role in the cyber conflict and Taiwan to confront China after the Ukraine war", Modern Diplomacy, 4/13/22, https://moderndiplomacy.eu/2022/04/13/u-s-nato-role-in-the-cyber-conflict-and-taiwan-to-confront-china-after-the-ukraine-war/, accessed 7/3/22, GDI-cc]

In light of such current global conditions, especially after the Ukraine war, it becomes difficult for us to be very optimistic about the possibility of achieving significant progress on any issue between the two parties. However, it will be possible for the United States of America and China to conclude some agreements, especially if they will be in the interest of the two countries after the deterioration in the global economy after the Russian war against Ukraine.

  Hence, Beijing is carefully studying the reaction of the international community to the Russian invasion of Ukraine. It is certain that China will analyze the most prominent aspects of the benefits of Russian military operations in Ukraine, in order to benefit from this in its strategy towards Taiwan.

 The most important thing to me is the Chinese insistence on monitoring and analyzing the extent of the unity and cohesion of the North Atlantic Treaty Organization (NATO) and other American alliances, as well as the extent to which the alliance and Western countries are able to bear the consequences and costs of sanctions on Russia.

 Here, we find that China is trying to monitor and analyze all the course of the war in Ukraine, and the Chinese analysis on (the most prominent defensive military roles of the “US Pentagon” and NATO after the Ukraine war, and the impact of (combining misinformation and the US cyber-attacks on the ground), then the Chinese focus on this relationship, due to the extent and scope of the formation of the defense and military positions of the US Department of Defense “the Pentagon” and the military alliance of NATO towards directing the future conflict of linking and the relationship between Ukraine and Taiwan, and their influence on China.

  China is well aware of the most important and most prominent (logistical differences between Moscow’s invasion of Ukraine and any possible attack it might have made in its efforts to annex Taiwan). Here, I can analyze China’s assertive position, that it cannot invade Taiwan’s borders in a scenario similar to the Russian army’s incursion into Ukrainian territory. Where China will work to search where the opportunity lies and how to take advantage of the Ukrainian crisis. Here, China will try to achieve balance in its dealings with the developments of events in Ukraine.

 Therefore, China is also trying to play (the role of neutrality Diplomacy regarding the burning crisis between Russia and Ukraine), and it is not expected that China will act in the same way that Russia did.  Ukraine.

### AT: China not a cyber military threat

#### Even Chinese espionage targeting US businesses tied to undermining US military advantages

**Kim ‘22**

(Wonny K. Kim, Innovation and Information Operations Officer in the U.S. Army Reserve 75th Innovation Command, Master of International Affairs from Columbia University, Master of Science in Technical Intelligence from National Intelligence University, and B.A. in Philosophy and Psychology from Binghamton University, ““Explicit” Bargains are Essential to Forming Desired Norms in Cyberspace,” Cyber Defense Review, Spring 2022, JSTOR, accessed 6/30/22, GDI- TMK)

THE SITUATION

The US National Cyber Strategy published in 2018 envisions an open, reliable, and secure cy- berspace, one that supports American prosperity, liberty, and security.[11] The key to realizing this vision is accepting cyber norms that “define acceptable behavior to all states and promote greater predictability and stability in cyberspace”[12] and that “attribute and deter unacceptable behavior in cyberspace.”[13] The accompanying 2018 Department of Defense (DoD) strategy emphasizes long-term strategic competition from the People’s Republic of China (PRC), which has “expanded that competition to include persistent campaigns in and through cyberspace that pose long-term strategic risk to the Nation as well as to our allies and partners.”[14] The DoD strategy further notes that, “China is eroding US military overmatch and the Nation’s economic vitality by persistently exfiltrating sensitive information from US public and private sector institutions.”[15]

Aligning National Cyber Strategy goals with DoD’s characterization of the threat requires an assessment of unacceptable PRC behavior. It is critical to note that DoD characterized PRC’s espionage as the persistent exfiltration of sensitive information, which sought to damage US in- terests: through the erosion of US military overmatch and the erosion of US economic vitality.

Eroding US military overmatch is obviously a serious concern, but espionage with the intent to understand and neutralize military advantages has been accepted normative behavior since at least as early as Sun Tzu in the 5th Century, BCE.[16]

It is not espionage itself that is the relevant issue here; rather, it is the intent to erode US economic vitality. This is precisely the issue that President Obama raised with President Xi in the 2015 agreement: espionage “with the intent of providing competitive advantages to com- panies or commercial sectors,”[17] hereafter referred to as intellectual property-theft (IP-theft).

### AT: plan causes China backlash

#### Non-unique - US already retaliating against China over cyber

Helmy, 2022

[Nadia, Professor of Political Science, Faculty of Politics and Economics at the Beni Suef University in Egypt, "U.S- NATO role in the cyber conflict and Taiwan to confront China after the Ukraine war", Modern Diplomacy, 4/13/22, https://moderndiplomacy.eu/2022/04/13/u-s-nato-role-in-the-cyber-conflict-and-taiwan-to-confront-china-after-the-ukraine-war/, accessed 7/3/22, GDI-cc]

The tension between the United States of America and China does not depend on geopolitical issues, especially in Taiwan and the South China Sea, as other issues, such as: (electronic security and cyber technology), are among one of the most prominent manifestations of tension between the two countries as well and cast a shadow on other features of political and economic competition and strategy between the two sides. The United States of America accused China of being behind several (electronic attacks and massive data breaches targeting American institutions and economic entities). Therefore, the United States of America linked this with opposition to China’s leadership in the communication technology of Chinese G5 networks. Therefore, it is expected that the US will continue to seek to limit Chinese technology markets and isolate them from the rest of the world, especially with Washington continuing to put obstacles in the way of Chinese companies obtaining industrial components and important American-made devices. The United States of America has already begun to implement stricter restrictions on technology transfer to China, so expectations indicate that more American restrictions will be imposed on China. And the US Department of Defense (the Pentagon) is working, starting from this year in 2022, to fill all the regulatory loopholes that allowed the well-known Chinese company to manufacture semiconductors, known as the “Semi Conductor ” company. And that Chinese company, which is the largest chip maker in China, has purchased important American technology. We find that Chinese companies and economic entities are likely to be added to the blacklist of the US Department of Commerce, with discussions on export controls between the United States and its allies as well as scrutiny of foreign direct investment issues in China. During the year of 2020, China launched a campaign targeting major technology companies, including the Chinese e-commerce giant “Alibaba”, “Tencent” and major real estate companies, such as “Evergrand and Kisa”, and others. Here, we see that these Chinese and American measures will negatively affect foreign investment in Chinese companies, which will make international investors in a state of complete caution. After the Ukraine war, it is expected that the Chinese, American, and global economy will (witness a significant slowdown in the coming period. According to my estimation, the decline in global growth will exacerbate tensions between the two parties).

## Great Power War [Russia and China]

### US key – cooperation

#### US fostered cybersecurity and cooperative efforts strengthen defense and deterrence against Russia and China

Mazarr, 2022

[Michael, senior political scientist at the RAND Corporation and previous professor and associate dean of academics at the the U.S. National War College, "Understanding Competition: Great Power Rivalry in a Changing International Order—Concepts and Theories", RAND Coorperation, 3/1/22, JSTOR, accessed 7/4/22, GDI-cc]

As Table 2 suggests, there are critical roles in peacetime competition for military services doing what they have always done. This includes training and advising, exercises, senior-leader engagements, humanitarian response and medical aid missions, and other missions. This analysis therefore points to a very specific, critical, but limited role for DoD in the contest short of war that is a part of the larger rivalries with Russia and China. The war in Ukraine has, if anything, underlined the importance of DoD’s role in competitive activities short of war. It was precisely these efforts—in terms of security assistance, train and advise missions, Foreign Military Sales and military aid deliveries, and cooperative efforts in such areas as cyber and defense institution building—that improved Ukraine’s ability to resist Russian aggression. In cases like this, in which the United States will not be willing or able to undertake a direct military role in countries threatened by Russian or Chinese coercion or aggression, peacetime support and cooperation will be the leading defense tool to deter and respond to attacks.

### Impact helper – Focus on Great Power War - solves terrorism

#### Focus on Russia and China increase tools to fight terror

**Becker et al.**, affiliated with the Centre for Security, Diplomacy and Strategy at the Vrije Universiteit Brussels, **2022**

(Jordan, academy professor and director of the Social Science Research Lab at West Point academy, “DON’T LET RUSSIA DOMINATE THE STRATEGIC CONCEPT,” War on the Rocks, JUNE 28, 2022, <https://warontherocks.com/2022/06/dont-let-russia-dominate-the-strategic-concept/>, accessed 7/3/2022, gdi-tmur)

Focusing on geopolitical competition with China and Russia will likely lead NATO allies to shift resources from the fight against terrorism. This structural situation requires NATO to develop a sustainable approach to mitigate terrorist threats. Fortunately, the key requirements for this complement the requirements of great power competition. Both involve improving defensive capabilities, maintaining crisis response capacity, and continuing to enhance intelligence sharing. For example, partnership structures like those used to support Ukraine since 2014 can be used to deepen cooperation in combatting terrorism globally. Similarly, many of the elements inherent in great power proxy warfare are compatible with combatting terrorism — for NATO this principally involves partner capacity building and information operations. The gains that NATO, and particularly NATO special operations forces, have made in coordinating the fight against non-state adversaries will help in great power competition, and their continued engagement will prevent basic counterterrorism capabilities from withering. The 2022 Strategic Concept can offer high-level political direction in support of incorporating irregular warfare into a broader approach to deterrence and defense.

## Liberal International Order

### Uniqueness – LIO erosion

#### Uniqueness – international order undermined by lack of action – Ukraine invasion creates opportunity for new leadership

**Zelikow,** Professor of History at the University of Virginia and Executive Director of the 9/11 Commission, **2022**

[Philip, “The Hollow Order Rebuilding an International System That Works” Foreign Affairs July/August 2022 <https://www.foreignaffairs.com/articles/world/2022-06-21/hollow-order-international-system?utm_medium=social&utm_campaign=tw_daily_soc&utm_source=twitter_posts> accessed July 4 GDI-TM]

There they were, meeting in Beijing on February 4: Chinese President Xi Jinping and Russian President Vladimir Putin. Shortly before the start of the 2022 Winter Olympics, the two leaders released a remarkable 5,300-word joint statement about how the partnership between China and Russia would have “no limits.” The document went on at length about the two nations’ commitment to democracy. It called for a universalist and open world order, with the United Nations at the center. It stressed a commitment to international law, inclusiveness, and common values. It did all this even though Russia, as Xi and Putin both knew, was sending tanks and missile launchers to the Ukrainian border. By comparison, the September 1940 joint statement issued by Germany, Italy, and Japan was a model of candor. The Axis powers were at least truthful when they announced that it was “their prime purpose to establish and maintain a new order of things.” Russia, meanwhile, has described its war against Ukraine as one of liberation. It decided that the country’s Jewish president was a Nazi. It declared that there was really no such thing as “Ukraine.” And it argued that a NATO alliance with a U.S. force commitment in Europe that was only one-seventh as large as it had been at the height of the Cold War was now an existential threat. In their statement, China and Russia achieved peak hypocrisy. But the existing world order, which aspired to build a global commonwealth, had already been failing. The free world’s leaders had long ago started favoring performative commitments over the real action needed to safeguard the planet from crises. They expanded NATO without meaningfully responding to increasing Russian aggression. Distracted and chastened by misadventures in the Muslim world, Washington in particular disengaged from practical deeds, even as its rhetorical commitment to the international order varied. The United States’ high defense spending had more to do with satisfying domestic constituencies than with supporting any positive strategy. The world’s transition from fossil fuels to renewable energy sources was based on hollow pledges and private action. As support for globalization waned, the United States and other countries retreated from trade agreements and neglected international institutions for civilian and common economic action. The world’s drive in the early years of this century to improve global health and human development petered out. The emptiness of the supposed international system was especially obvious at the end of 2019, when the COVID-19 pandemic broke out. Charged with unprecedented global responsibilities, China and the United States stepped down, not up. Beijing withheld crucial information about the outbreak. Washington withdrew from the World Health Organization just when it most needed U.S. leadership. Wealthy countries began a mad scramble to develop vaccines, but they moved too slowly to create other treatments and hoarded whatever shots and therapeutics pharmaceutical companies could produce, leaving the rest of the world behind. The best estimates suggest that the virus caused about 15 to 20 million deaths and trillions of dollars of economic damage. By the spring of 2020, “for all practical purposes the G7 ceased to exist,” wrote the foreign policy experts Colin Kahl and Thomas Wright in August 2021. “Pandemic politics,” they continued, “ultimately dealt the final blow to the old international order.” Six months after they published those words, Russia invaded Ukraine. It was an attack that could truly have buried the old system, as Moscow believed it would. Yet Ukraine’s inspiring fight has helped the G-7 roar back to life. Its members have organized an economic counteroffensive, and they have joined a coalition providing military aid. Amid the wreckage of so many past hopes, it is possible to imagine a reconstructed world order emerging from this crisis. **But for a new system to succeed, its would-be architects must organize actions**, not more theatrics. Over the course of world history, the most powerful idealism has usually been the idealism of what works. Today, that means crafting a practical international order focused on a few basic problems that rally broad interest. Many leaders want to stop unprovoked wars of aggression, especially those that might spark a third world war. They would welcome a new vision of economic order that does not ignore security but is also not a huckster’s promise that everything can be made at home. They would like to convert jolting energy shocks, such as the one caused by Russia’s invasion, into a managed transition to a more carbon-free future. They want to be better prepared for the next pandemic. And most world leaders, and even many ordinary Americans, still hope that China will choose to be part of these solutions, not one of the wreckers of a new international system. These aspirations may seem modest. They do not include holding war crimes trials or spreading democracy. But effective common action on just these items will be an enormous task. The world order is deglobalizing and dysfunctional, facing challenges that have never been more planetary in scope. Leaders must craft a system focused on actually addressing these issues rather than on striking the right pose.

### Impact Revitalized LIO– pandemics

#### International order key to pandemic – COVID reveals weakness in the system

**Zelikow,** Professor of History at the University of Virginia and Executive Director of the 9/11 Commission, **2022**

[Philip, “The Hollow Order Rebuilding an International System That Works” Foreign Affairs July/August 2022 <https://www.foreignaffairs.com/articles/world/2022-06-21/hollow-order-international-system?utm_medium=social&utm_campaign=tw_daily_soc&utm_source=twitter_posts> accessed July 4 GDI-TM]

But nowhere has the hollowness of the current world order been more starkly revealed than in global health. After the SARS epidemic of 2003, amid concerns about China’s role in informing the rest of the planet about the outbreak, the nations of the world ceremoniously enacted a set of “international health regulations,” which defined the rights and duties of states to prevent and contain international public health dangers. The outbreak of COVID-19 revealed that the elaborate provisions for global surveillance and early warnings were a sham. The pandemic also showed that the planet’s main public health agency—the World Health Organization—was weak, and it demonstrated that the world’s major powers were far too self-interested to mount a truly global response. The most substantial investigation so far of the world’s reaction to COVID-19, by an independent panel with access to the WHO’s staff and documents, found it was “a preventable disaster.” As they wrote, “Global political leadership was absent.”

It’s a conclusion that is difficult to escape. China’s government has blocked proper investigations into the outbreak’s cause and continues to stonewall the WHO. In his own gesture of theatrical pretense, then U.S. President Donald Trump moved to pull his country out of the WHO during the spring of 2020, turning the crisis into a blame game focused on China, with the organization as an accomplice. Yet the Trump administration had no alternative agenda for meaningful global action. Its acclaimed vaccine development program encouraged an “every country for itself” approach to acquisition and bypassed the challenge of developing effective therapeutics.

### Impact Revitalized LIO – clean energy

#### Reglobalization for clean energy necessary to develop alternative stable sources of clean energy and stable supply chains

**Zelikow,** Professor of History at the University of Virginia and Executive Director of the 9/11 Commission, **2022**

[Philip, “The Hollow Order Rebuilding an International System That Works” Foreign Affairs July/August 2022 <https://www.foreignaffairs.com/articles/world/2022-06-21/hollow-order-international-system?utm_medium=social&utm_campaign=tw_daily_soc&utm_source=twitter_posts> accessed July 4 GDI-TM]

The invasion of Ukraine has also highlighted the need for more decisive, concerted action on the world’s transition to clean energy. More than any other event since the Iranian revolution of 1979, the war spotlights the danger of relying too much on particular supplies of fossil fuels. Europe should end its dependence on Russian oil, gas, and coal as quickly as it can. At the global level, policymakers will need to boost fossil fuel supplies from more dependable sources in the short term, but they should treat these sources as “transition assets” (to quote the energy experts Jason Bordoff and Meghan O’Sullivan) that will be quickly wound down as governments embrace the transition. The switch to greener sources will need to include a renewed commitment to advanced forms of nuclear energy.

The energy transition will require much more concerted work to find, extract, and process diverse and secure supplies of the minerals needed for renewable sources. Both the United States and Europe know that they cannot let vital supply chains such as these operate according to market forces alone, since these markets have been distorted by vast Chinese state projects that operate with limited regard for the environment and for workers. Countries that regard each other as secure sources—and that accept the cost burdens of sustainable production—must form their own supply network with its own commercial system and pricing. Such a plan requires strong international participation. No country alone can source and process the metals needed for the transition to carbon-free energy.

Such trading among partners, or “friend shoring,” as U.S. Treasury Secretary Janet Yellen put it, is far preferable to the “Buy American” public procurement requirements that Washington has put in place to placate protectionists. Indeed, the United States is not self-sufficient with regard to almost any major global commodity. In this time of crisis, Americans may be tempted by the idea of a “Fortress America”—in which they bring all production onshore—but that is an illusion. The United States needs and benefits from production chains that run through other countries, whether for mineral resources or medical supplies. It needs to rebuild export markets shriveling from past trade war rhetoric and present interest-rate policies that boost an overvalued dollar. The best way to cope with deglobalization is to reglobalize among friends. As major firms operating around the world rethink their business models, the free world should create structures to help these companies see new opportunities.

## Nuclear forces/deterrent

### SQuo – increased focus on nuclear arms racing and use

#### Cold War nuclear taboo at risk – increased focus on nuclear weapons and arms racing along with Putin rhetoric increase chance of use as Ukraine war goes on

**Tannenwald,** a senior lecturer in political science at Brown University , **2022**

[Nina, “Is Using Nuclear Weapons Still Taboo? The world is starting to forget the realities of nuclear weapons” Foreign Policy JULY 1, 2022,<https://foreignpolicy.com/2022/07/01/nuclear-war-taboo-arms-control-russia-ukraine-deterrence/> accessed july 4 GDI-TM]

In the first decades after World War II, many U.S. military and political leaders, and much of the public, expected or feared that nuclear weapons would be used again. Hiroshima and Nagasaki made the horrors of atomic bombings visible for all. The notion that nuclear war could happen at any moment permeated American society. Many Cold War-era buildings—including schools, airports, and even motels—were constructed with a fallout shelter in the basement. The instruction to “duck and cover” in the event of a nuclear attack (rather than run to a window to look out) became part of U.S. civil defense drills that every U.S. citizen, including schoolchildren, was encouraged to practice. Movies such as On the Beach (1959), a piece of post-apocalyptic science fiction, depicted a world annihilated by nuclear war. Military strategists such as Herman Kahn, one of the historical inspirations for the madman title character of Stanley Kubrick’s classic black comedy Dr. Strangelove, proselytized about “thinking the unthinkable”—the need to think about how we would fight and survive a nuclear war. Events such as the Cuban missile crisis made these fears palpably real. For 13 days in October 1962, the world came the closest it ever has to nuclear war. Many people at the time believed the world was about to end in mushroom clouds. Yet, during the same period, norms of restraint developed. A nuclear taboo—a normative inhibition against the first use of nuclear weapons—emerged as the result of both strategic interests and moral concerns. A global grassroots anti-nuclear movement, along with nonnuclear states and the United Nations, actively sought to stigmatize nuclear weapons as unacceptable weapons of mass destruction. After the scare of the Cuban missile crisis, the United States and the Soviet Union also pursued arms control agreements to help stabilize the “balance of terror.” These norms of nuclear restraint helped foster the now nearly 77-year tradition of nonuse of nuclear weapons, the single-most important feature of the nuclear age. But today, most of these arms control agreements have been torn up, and nuclear-armed states are once again engaged in costly arms races. We are in a period of nuclear excess rather than restraint. All of this brings us to the current moment and the big question suddenly on everyone’s minds: Do Russian leaders share the nuclear taboo? Would Russian President Vladimir Putin use a nuclear weapon in the war in Ukraine? He certainly wants the world—and in particular the United States—to at least think he might. On the day he announced the beginning of a “special military operation” in Ukraine, Putin warned that any country that attempted to interfere in the war would face “such consequences that you have never experienced in your history,” which many took to be a veiled nuclear threat. Other Russian officials have made similar statements over the course of the war. So far, it is likely that these threats are more about deterring NATO than actual use. Russia has apparently not increased the alert levels of its nuclear forces but rather activated a communications system that could transmit a launch order. Russian officials are certainly aware that any use of nuclear weapons would bring devastating consequences for Russia and for Putin himself, including widespread condemnation and global opprobrium. As Anatoly Antonov, Russia’s ambassador to the United States, claimed in early May, “It is our country that in recent years has persistently proposed to American colleagues to affirm that there can be no winners in a nuclear war, thus it should never happen.” Still, the risk that Putin would use a nuclear weapon is not zero, and the longer the war goes on the more the risk goes up.

### Squo – Russia nuclear use – Ukraine

#### Increased risk of nuclear use as war goes on – Russia escalate to de-escalate strategy makes it more thinkable

**Ashford**, senior fellow at the Atlantic Council’s Scowcroft Center for Strategy and Security, **and Kroenig,** deputy director of the Atlantic Council’s Scowcroft Center for Strategy and Security **2022**

[Emma and Mathew, “Would Putin Use Nuclear Weapons?” Foreign policy MARCH 11, 2022 <https://foreignpolicy.com/2022/03/11/putin-russia-nuclear-weapons-ukraine-war-no-fly-zone/> accessed 7/4/22 GDI-TM]

Emma Ashford: Hey, Matt. So, we’re now in week three of the Russo-Ukrainian war. It has been a surprising few weeks: European states decided to massively increase their defense spending, the United States just banned Russian oil imports, and—perhaps most surprisingly—the Ukrainians have managed to drag this fight out far longer than most observers thought possible.

Matthew Kroenig: Yes, the world has changed dramatically in the past several weeks. I feel as if 10 years’ worth of developments have been packed into several days. I never thought, for example, I would ever see Germany decide to more than double its defense spending.

But you overlooked what may have been the most frightening development: a renewed risk of nuclear war between Russia and the West. Russian President Vladimir Putin placed Russian nuclear forces on alert for the first time since the end of the Cold War. What do you make of this threat?

EA: It couldn’t have been a clearer signal if Putin himself had airdropped into Ukraine and planted a giant sign saying “Keep out!” in front of the border. Indeed, in addition to the alert, we’ve also had public statements from Putin and Russian Foreign Minister Sergey Lavrov effectively threatening nuclear retaliation if the West intervenes further in Ukraine. The Russian government is reminding everyone in no uncertain terms that Russia is a nuclear power.

MK: Indeed. As a specialist in nuclear strategy, I have to say I wasn’t at all surprised. In fact, I was predicting that the Ukraine crisis would become a nuclear crisis several months ago.

This is Russia’s so-called “escalate to de-escalate” strategy: threatening (and if necessary carrying out) nuclear strikes on the assumption that the West will back down and the Kremlin can get its way.

At this early stage of the crisis, I think these threats are mostly a bluff to get the United States and NATO to curtail their support to Ukraine, but I do think there is a real risk of Russian nuclear use if the war continues.

#### Brink – Ukraine war increases risk of nuclear war and showcases fragility of deterrence strategies

**Tannenwald,** a senior lecturer in political science at Brown University , **2022**

[Nina, “Is Using Nuclear Weapons Still Taboo? The world is starting to forget the realities of nuclear weapons” Foreign Policy JULY 1, 2022,<https://foreignpolicy.com/2022/07/01/nuclear-war-taboo-arms-control-russia-ukraine-deterrence/> accessed july 4 GDI-TM]

In March 1990, the New Yorker published a cartoon by Jack Ziegler that captured the optimism at the end of the Cold War. The cartoon shows an executive sitting at his desk as a worker enters the office carrying a large bomb with fins. “Bring that H-bomb over here, will you, Tom, and just slip it into my ‘out’ box,” the executive says. “Sure thing, boss!” the worker responds.

The image of putting nuclear bombs “in the outbox” was emblematic of the hope many had that a new era of cooperation between the United States and the former Soviet Union was emerging. The fear of a nuclear war breaking out between the world’s two superpowers receded, and many hoped that nuclear weapons, although they would still exist, would no longer be central to international politics. Mikhail Gorbachev, the Soviet Union’s last leader, declared in June 1991 that “the risk of a global nuclear war has practically disappeared.”

Today, more than 30 years later, nuclear bombs are back in the inbox. Fear of nuclear war between the United States and Russia has returned with a vengeance. As a result of Russia’s brutal invasion of Ukraine and Russian officials’ alarming nuclear threats, the world is closer to the use of nuclear weapons out of desperation—or by accident or miscalculation—than at any time since the early 1980s.

The Russia-Ukraine war serves as a harsh reminder of some old truths about nuclear weapons: There are limits to the protection nuclear deterrence provides. (Usable conventional weapons may get you more protection.) In a crisis, deterrence is vulnerable, not automatic and self-enforcing. There is always the chance that it could fail.

### Impact - Cyber threats - deterrence

#### Cyber undermines deterrence by distorting or degrading capabilities of conventional and nuclear forces

**Montgomery and Borghard, National Defense University, 2021**

[Mark and Erica, “Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence” Joint Force Quarterly 102 July 1, 2021 <https://www.ndu.edu/News/Article-View/Article/2684986/cyber-threats-and-vulnerabilities-to-conventional-and-strategic-deterrence/> accessed 7/7/2022 GDI-TM]

Credibility lies at the crux of successful deterrence. The target must believe that the deterring state has both the capabilities to inflict the threatening costs and the resolve to carry out a threat.14 A **deterring state must therefore develop mechanisms for signaling credibility to the target**.15 Much of the Cold War deterrence literature focused on the question of how to convey resolve, primarily because the threat to use nuclear weapons—particularly in support of extended deterrence guarantees to allies—lacks inherent credibility given the extraordinarily high consequences of nuclear weapons employment in comparison to any political objective.16 This raises questions about decisionmakers’ willingness to follow through on a nuclear threat. However, the credibility conundrum manifests itself differently today. Specifically, the potential for cyber operations to distort or degrade the ability of conventional or even nuclear capabilities to work as intended could undermine the credibility of deterrence due to a reduced capability rather than political will.17 Moreover, given the secret nature of cyber operations, there is likely to be information asymmetry between the deterring state and the ostensible target of deterrence if that target has undermined or holds at risk the deterring state’s capabilities without its knowledge.

#### Cyber threats undermine the deterrence posture

**Montgomery and Borghard, National Defense University, 2021**

[Mark and Erica, “Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence” Joint Force Quarterly 102 July 1, 2021 <https://www.ndu.edu/News/Article-View/Article/2684986/cyber-threats-and-vulnerabilities-to-conventional-and-strategic-deterrence/> accessed 7/7/2022 GDI-TM]

Recognizing the interdependence among cyber, conventional, and nuclear domains, U.S. policymakers must prioritize efforts to reduce the cyber vulnerabilities of conventional and nuclear capabilities and ensure they are resilient to adversary action in cyberspace. Cyber threats to these systems could distort or undermine their intended uses, creating risks that these capabilities may not be reliably employable at critical junctures. Additionally, cyber-enabled espionage conducted against these systems could allow adversaries to replicate cutting-edge U.S. defense technology without comparable investments in research and development and could inform the development of adversary offset capabilities. Vulnerabilities such as these have important implications for deterrence and warfighting. Deterrence postures that rely on the credible, reliable, and effective threat to employ conventional or nuclear capabilities could be undermined through adversary cyber operations. And, if deterrence fails, cyber operations to disrupt or degrade the functioning of kinetic weapons systems could compromise mission assurance during crises and conflicts.

### Impact - US NATO nuclear deterrent – stops Russia expansion

#### US and NATO should engage in alter their nuclear posture and declaratory policy to allow for asymmetric escalation – brinksmanship deters Russian invasion of eastern flank

**BOWEN, 2022**

[Tyler, postdoctoral fellow in the Kissinger Center at Johns Hopkins SAIS “RUSSIA’S INVASION OF UKRAINE AND NATO’S CRISIS OF NUCLEAR CREDIBILITY” WOR April 20, 2022 <https://warontherocks.com/2022/04/russias-invasion-of-ukraine-and-natos-crisis-of-nuclear-credibility/> accessed 7/4/22 GDI-TM]

The Art of Brinkmanship

In response to this challenge, the United States and NATO should embrace the paradox of brinkmanship, which involves trying to prevent war by making it hard to contain once it starts. In the words of Thomas Schelling, “by arranging it so that we [the United States] might have to blow up the world, we would not have to.” This involves making “threats that leave something to chance,” or threats that, once enacted, would “initiate a process that may quickly get out of hand.”

States use tactical nuclear weapons to bid up the shared risk of nuclear escalation in the event of a war. Because tactical nuclear weapons are less destructive than “strategic” nuclear weapons, they are seen as more usable and blur the firebreak between conventional and nuclear war. At the same time, the use of tactical nuclear weapons generates a higher risk of general nuclear conflict than does the use of conventional forces, meaning that threats to use tactical nuclear weapons early in a war increase the shared risk of disaster. This is why states who face conventional inferiority tend to invest more heavily in these weapons.

Brinkmanship tactics also involve a trade-off between deterrence and the risk of escalation. A state could employ a “minimal brinkmanship” strategy that generates low risk of nuclear use, and if the state lacks the conventional strength to deny the adversary its objectives in a war, this could incentivize the adversary to attack. On the other hand, a state could enact a “maximum brinkmanship” strategy that generates high risk for nuclear war in the event of a conflict, but that high risk could generate restraint on the part of the adversary. The United States used a form of maximum brinkmanship in the 1958–59 Berlin Crisis by threatening escalation to nuclear use very early in a war over Berlin. As one of Daniel Ellsberg’s colleagues described that strategy to him: “We send in a series of increasingly larger probes. If they’re all stopped, we fire a [nuclear] warning shot. If that doesn’t work, we blow up the world.”

The degree of brinkmanship in a state’s defense strategy lies on a scale from the minimum to the maximum end. Where a state’s strategy should fall on the scale depends on the adversary’s intentions and capabilities. Against an adversary with conventional inferiority, it makes little sense to run a higher risk of nuclear war. For an adversary with aggressive motivations, the risks of maximum brinkmanship may be justified. However, if an adversary is not planning on using force, a maximum brinkmanship strategy could make them feel insecure and prompt them to launch the attack that the state was attempting to deter.

Brinkmanship in the Baltics

What kind of adversary does NATO face in Moscow? The answer depends on the outcome of the current conflict. Based on current developments, it seems all too likely the result will be an aggravated Russia that is stuck in a grinding war in Ukraine. After six weeks of fighting, the Russian advance in Ukraine has stalled. This slow progress has prompted Russian forces to resort to horrific indiscriminate violence against civilians in these areas. At this moment, a quick victory toppling the Ukrainian government and leading to an emboldened Russia looks unlikely.

At the same time, Russia is unlikely to accept defeat in Ukraine anytime soon. Reports came out on March 29 that Ukraine and Russia were making progress on peace talks, but Russia’s lead negotiator Vladimir Medinsky stressed that there was “still a long way to go” before Russia would agree to a ceasefire. Instead, Russia appears to have changed its war aims from taking Kyiv to consolidating control over eastern Ukraine. Fighting for this objective is likely to be costly and raises the probability that this war will be a protracted conflict. Western sanctions against Russia will remain in place during the war, and Western countries will continue to provide assistance to Ukrainian armed forces. That assistance will flow through Eastern European member states.

To break out of a stalemated war and achieve victory, Putin could try to target supplies in transit while they are still in an Eastern European NATO country, especially Poland. Putin could also conduct a limited attack against a Baltic State in order to take territory that is majority Russian-speaking. That could bolster his claim of defending Russian speakers abroad. He may be incentivized to do this if the economic sanctions prove too harsh on the Russian economy, and he sees no way out of the crisis except by expanding the war. That pathway to escalation is similar to Imperial Japan’s rationale for attacking Pearl Harbor in 1941.

This scenario poses a serious test for deterrence for NATO. A strike on supplies going to Ukraine would be difficult to defend against, and Russian forces could overwhelm the NATO forces assigned to an initial defense of the Baltics. **The best response to the threat of these scenarios is to prevent them from happening in the first place. To do that, a modest degree of brinkmanship could prove effective.** Here, the United States and NATO should alter their nuclear posture and declaratory policy to allow for asymmetric escalation.

### Impact - Deterrence Good – breakdown risks escalation

#### War in Ukraine highlight value of deterrence and the risks of deterrence breakdown and unintended escalation

**Tannenwald,** a senior lecturer in political science at Brown University , **2022**

[Nina, “Is Using Nuclear Weapons Still Taboo? The world is starting to forget the realities of nuclear weapons” Foreign Policy JULY 1, 2022,<https://foreignpolicy.com/2022/07/01/nuclear-war-taboo-arms-control-russia-ukraine-deterrence/> accessed july 4 GDI-TM]

The United States and NATO have reciprocated neither the discourse of Russian officials (nuclear threats) nor the claimed behavior (enhanced readiness of nuclear arsenals) but rather have funneled vast amounts of conventional weapons to Ukraine while promising to pursue accountability for Russian war crimes. Despite scattered calls in the United States for the creation of a “no-fly zone” over some or all of Ukraine, the Biden administration wisely resisted. In practice, this would mean shooting down Russian planes and risk igniting World War III. Yet, as the war drags on, the United States may be sleepwalking into an expanded—and therefore more dangerous—war. Russia’s weak military performance has tempted defense hawks and unrequited Cold Warriors to shift the goals from simply helping to prevent Ukraine’s defeat to, as U.S. Defense Secretary Lloyd Austin suggested on April 25, creating a “weakened” Russia. An alarming number of foreign-policy commentators, including retired U.S. military officers and NATO supporters who should know better, have cavalierly urged the Biden administration to get much more aggressive in helping Ukraine or even pursue total victory, despite the risk of nuclear escalation. Using the war to reassert U.S. hegemony is a dangerous game. There is a whiff of nuclear forgetting in the air. One reason the Cold War remained cold was that U.S. leaders recognized that confronting a nuclear-armed adversary imposes constraints on action. When the Soviet Union invaded Hungary in 1956 and Czechoslovakia in 1968, the United States refrained from responding with military force. Yet today there is an entire generation (or more) of people for whom the scary realities of the Cold War and “duck and cover” are the stuff of history books, rather than lived experience. As the historian Daniel Immerwahr wrote recently, “This is the first decade when not a single head of a nuclear state can remember Hiroshima.” In making nuclear dangers vivid again, the Russia-Ukraine war reminds us of not just the benefits but also the significant risks and limits of nuclear deterrence. Deterrence has likely kept Russia from expanding the war to NATO countries such as Poland and Romania. Russia’s nuclear arsenal has kept NATO from intervening directly, but it has also failed to help Russia take or hold significant territory in Ukraine or compel Kyiv to surrender. Most importantly, the war reminds us that controlling escalation is a giant unknown. We have no idea what would happen if a nuclear weapon were actually used. The war also reminds us that norms are ultimately breakable. In the last few years, numerous norms that we once thought were robust have been undermined. Norms of democracy are under siege in the United States and elsewhere. Internationally, states have eroded norms of territorial integrity, multilateralism, arms control, and humanitarian law. The nuclear taboo, while widely shared, is more fragile than other Some might argue that the taboo and deterrence are robust because no rational leader would see a benefit to starting a nuclear war. The prominent international relations realist Kenneth Waltz, a proponent of nuclear deterrence, famously wrote that nuclear weapons create “strong incentives to use them responsibly.” The problem is that, even if true some of the time, this may not always be true. Not all leaders may be rational or responsible. This view also overlooks the possibility that nuclear war could begin through accident, misperception, or miscalculation. In short, the nuclear taboo and deterrence are always at risk.

### AT NATO focused on conventional deterrent

#### Conventional forces necessary but not sufficient for defense against Russia

Mengelkamp et al, 2022

[Lukas, Ph.D. student in history at the University of Marburg where he studies the history of the critique of nuclear deterrence, "A CONFIDENCE-BUILDING DEFENSE FOR NATO", War on the Rocks, 6/27/22, https://warontherocks.com/2022/06/a-confidence-building-defense-for-nato/, accessed 7/4/22, GDI-cc]

NATO knows what it needs to do at the upcoming Madrid Summit, but it still does not know how. The alliance is determined to strengthen conventional deterrence on its eastern front and soon its northern flank. [Some allies](https://news.usni.org/2022/03/30/baltic-presidents-forward-defense-needed-to-deter-russia) argue that this requires abandoning NATO’s [“tripwire” approach](https://carnegieendowment.org/2018/03/28/preventing-escalation-in-baltics-nato-playbook-pub-75878) and adopting a strategy of [“forward defense.”](https://news.usni.org/2022/03/30/baltic-presidents-forward-defense-needed-to-deter-russia) Instead of maintaining small, multi-national contingents in the Baltic States and Poland, NATO would deploy sufficient forces to defeat a potential Russian attack and even be able to conduct counter-offensives. This would involve permanently stationing large contingents as close as possible to Russia and Russian-controlled territory.

The problem with forward defense, however, is that while it sounds good, it is not clear what it would mean in practice, or how it would play out against the many divergences and disagreements between NATO members. Instead, allies should embrace a strategy of confidence-building defense. To revive this late Cold War concept, NATO’s eastern members would create a highly mobile net of dispersed artillery, while more powerful European allies would build and supply heavy weapons depots in those countries, then prepare to rapidly deploy significant forces in case of a crisis. This approach would enable European allies to contribute to their own security, lessen first-strike pressures, and avoid deepening a dangerous new security dilemma with Russia.

### AT Russia will stop in Ukraine

#### Russia poor performance in Ukraine won’t be replicated in other countries – and Russia poses ongoing threat to NATO countries

**BOWEN, 2022**

[Tyler, postdoctoral fellow in the Kissinger Center at Johns Hopkins SAIS “RUSSIA’S INVASION OF UKRAINE AND NATO’S CRISIS OF NUCLEAR CREDIBILITY” WOR April 20, 2022 <https://warontherocks.com/2022/04/russias-invasion-of-ukraine-and-natos-crisis-of-nuclear-credibility/> accessed 7/4/22 GDI-TM]

Risk to the Baltics

The goal for the United States and its NATO allies should be to protect Eastern European countries such as Latvia, Lithuania, Estonia, and Poland from a Russian attack. Eastern European NATO countries, especially the Baltic states, do not have the capabilities to do this on their own. The Russian military is performing poorly in the initial phase of the war in Ukraine, but this should not be taken as evidence that NATO countries in Eastern Europe have adequate capabilities for conventional defense. Indeed, these countries may fare worse against a Russian invasion than Ukraine has done, as their militaries are smaller than the Ukrainian military. Plus, the Russian operation in Ukraine appears to have been informed by wildly optimistic assumptions that the Ukrainians lacked the will to put up a fight and that resistance would crumble in short order. This could be why the first phase of the Russian invasion used only a fraction of the 190,000-strong force it amassed around Ukraine. The United States and NATO should expect that a Russian attack on a NATO country would have different assumptions and go differently, perhaps with Russia using many more of its forces in the opening phase of the campaign.

Many Russian forces are bogged down in Ukraine, but Russia still has the conventional strength to expand the current war into NATO territory. For example, Russia could leverage its strength in conventional long-range strike to attack convoys of supplies going into Ukraine. Indeed, this is something that Russia has recently threatened to do. Furthermore, Russia could try to hold territorial gains in eastern and southern Ukraine instead of fighting offensive missions to take more territory. A new “defensive” focus in Ukraine could free more Russian forces for an attack on an Eastern European NATO country. In short, Russia still has the capability to conduct strikes against NATO allies and to turn the focus of its combat power on them should it choose to do so.

### AT Conventional military investment solves Russia threat

#### Conventional upgrades inevitable – but even new investment now won’t solve immediately and current nuclear deterrent not credible

**BOWEN, 2022**

[Tyler, postdoctoral fellow in the Kissinger Center at Johns Hopkins SAIS “RUSSIA’S INVASION OF UKRAINE AND NATO’S CRISIS OF NUCLEAR CREDIBILITY” WOR April 20, 2022 <https://warontherocks.com/2022/04/russias-invasion-of-ukraine-and-natos-crisis-of-nuclear-credibility/> accessed 7/4/22 GDI-TM]

After Russia’s invasion of Ukraine, European NATO allies are now likely to increase investments in their armed forces that could make a successful conventional defense possible in the future. Germany’s decision to double its defense budget is telling in this regard. NATO’s increase in troops deployed to Eastern Europe is also a positive recent development. But these developments will take time to bear fruit.

Currently, NATO’s defense of the Baltics hinges on the threat of responding to a Russian attack with its nuclear arsenal. But Putin’s recent nuclear saber-rattling suggests he may not find this threat credible and believes Washington will back down rather than risk nuclear war. Indeed, even during the Cold War, it was difficult enough to convince the Soviet Union that the United States would trade Berlin for Boston. Expanding the alliance has only heightened this challenge. How can the United States make Putin believe that it is willing to trade Vilnius for New York?

### AT Russia – escalate to de-escalate policy

#### No Russia escalate to de-escalate policy – only escalation

**Ashford**, senior fellow at the Atlantic Council’s Scowcroft Center for Strategy and Security, **and Kroenig,** deputy director of the Atlantic Council’s Scowcroft Center for Strategy and Security **2022**

[Emma and Mathew, “Would Putin Use Nuclear Weapons?” Foreign policy MARCH 11, 2022 <https://foreignpolicy.com/2022/03/11/putin-russia-nuclear-weapons-ukraine-war-no-fly-zone/> accessed 7/4/22 GDI-TM]

EA: It’s funny you should mention “escalate to de-escalate.” Though a favorite of Washington defense planners—perhaps because it justifies having a larger, more diverse nuclear arsenal—military analysts who focus on Russia largely argue that there is no such concept in Russian military doctrine. The only Russian work that actually proposes an escalate-to-de-escalate policy was an article in a military journal, and there were a few muddled official statements. This position was never confirmed or followed up on in official government writing or doctrine. There’s no formal evidence that the Russians have such a policy, and there’s certainly no incentive to keep it quiet if they do have one. I remain unconvinced.

### AT Russia won’t escalate to nuclear use

#### Evidence of escalation to de-escalate policy clear – and Russia threatening use in Ukraine

**Ashford**, senior fellow at the Atlantic Council’s Scowcroft Center for Strategy and Security, **and Kroenig,** deputy director of the Atlantic Council’s Scowcroft Center for Strategy and Security **2022**

[Emma and Mathew, “Would Putin Use Nuclear Weapons?” Foreign policy MARCH 11, 2022 <https://foreignpolicy.com/2022/03/11/putin-russia-nuclear-weapons-ukraine-war-no-fly-zone/> accessed 7/4/22 GDI-TM]

MK: Oh boy, where to begin. First, I have never met anyone who harbors the goal of building more nukes for fun and is just going around looking for excuses to do so. Those, like me, who support the United States having flexible nuclear options for Russia do so because they see a real threat against which the country must defend.

Second, the U.S. government, including in the 2018 Nuclear Posture Review, states that Russia has such a doctrine. You are right that some think tank experts have disputed this, but, as we have seen over the past few weeks, the U.S. government has pretty good insight into Russian defense planning. I trust the U.S. government over outside experts on this point.

Third, the academic debate about whether there is a formal Russian doctrine or not misses the point entirely. The real question is, would Russia find it attractive to threaten to use (and in certain circumstances actually use) nuclear weapons in order to win a conflict with the West? And, as we are seeing this week, the answer is unequivocally yes.

#### Risk of nuclear escalation from Putin threats – and US drawin increases risk of nuclear escalation

**Ashford**, senior fellow at the Atlantic Council’s Scowcroft Center for Strategy and Security, **and Kroenig,** deputy director of the Atlantic Council’s Scowcroft Center for Strategy and Security **2022**

[Emma and Mathew, “Would Putin Use Nuclear Weapons?” Foreign policy MARCH 11, 2022 <https://foreignpolicy.com/2022/03/11/putin-russia-nuclear-weapons-ukraine-war-no-fly-zone/> accessed 7/4/22 GDI-TM]

MK: As you know, military threats are most effective when one doesn’t have to carry them out. Russia is starting with threats in the hope that will work, but it retains the option of following through with actual nuclear strikes if it comes to that. We saw Russia run a similar playbook in 2014. As Putin invaded Crimea and eastern Ukraine’s Donbass region, he said, “Russia is one of the leading nuclear powers. … It’s best not to mess with us.” Russian officials relayed similar threats to Western leaders. And while Russia did not put its nuclear forces on high alert, Putin later bragged that he almost did. So, essentially, Russia is backstopping its conventional aggression with nuclear threats. Step 1: Invade your neighbors. Step 2: Threaten nuclear war to prevent outside interference that could reverse your conquest.

EA: That’s a better characterization. As the Georgetown University professor Caitlin Talmadge pointed out last week, the Russians are largely using their nuclear weapons as an umbrella, presuming that the stability-instability paradox—which suggests that states with nuclear weapons are even more likely to start a war, assuming that nuclear weapons will prevent the worst outcomes—will hold that and they’ll be able to get away with conventional military activity as a result. But for the United States, the result is the same whether or not Russia says it out loud. The United States doesn’t have an interest in getting in a shooting war with Russia, particularly given the risks of nuclear escalation that come with it. There’s a reason why, during the Cold War, the superpowers typically kept conflict contained to proxies.

MK: So you don’t think there is any risk that Russia will use nuclear weapons? I don’t want to overstate this. It is very unlikely at this point, but depending on how this conflict develops, I see a real threat. In fact, I think Putin would use nuclear weapons in Ukraine, for example, as a last resort in a desperate effort to stave off an embarrassing military defeat. And while you are right that the United States has an incentive to avoid nuclear war, so does Putin. The United States is a nuclear superpower, and a nuclear exchange would also result in unacceptable costs for Russia. If the West simply cowers in response to his nuclear threats, we are essentially telling him, “Threaten nuclear war and you can invade whomever you want.”

EA: I do think there is a risk of nuclear escalation here, which is why I’m so concerned about increasing the United States’ and NATO’s exposure to this conflict. The United States and Europe have already placed unprecedented and punishing sanctions on the Russian economy. They’re continuing to arm and supply the Ukrainians and taking a number of diplomatic steps. But Ukraine isn’t a NATO member. It isn’t under America’s nuclear umbrella. The United States should not get into a war for Ukraine. And too many of the options on the table at this point—such as a no-fly zone—risk pulling the United States directly into this conflict in ways that could eventually go nuclear.

### AT Putin posturing – won’t use

#### Russian military actions demonstrate willingness to break norms – and poor performance risks use of tactical nuke out of frustration

**Tannenwald,** a senior lecturer in political science at Brown University , **2022**

[Nina, “Is Using Nuclear Weapons Still Taboo? The world is starting to forget the realities of nuclear weapons” Foreign Policy JULY 1, 2022,<https://foreignpolicy.com/2022/07/01/nuclear-war-taboo-arms-control-russia-ukraine-deterrence/> accessed july 4 GDI-TM]

Which brings us back to Putin. In 1999, Putin launched himself to power as Russia’s prime minister, overseeing the country’s shockingly brutal second war in Chechnya. Since then, Russia under Putin has shown itself willing to violate important international norms, including those against territorial conquest (Crimea, Ukraine) and against attacking civilian targets. Shredding the rules of war, the Russian military has inflicted devastation and cruelty on civilians in Chechnya, Syria, and now Ukraine. In Ukraine, Russia shelled Europe’s largest nuclear power plant at Zaporizhzhia, a reckless act that set part of the facility on fire. Such strikes risk nuclear disaster.

Russian officials have portrayed Ukraine’s national identity and existence as a threat to Russia and have employed increasingly exterminationist language in their stated quest to “denazify” Ukraine as well as to justify the war to the Russian public. Coming on top of what appear to be appalling Russian war crimes in the Ukrainian cities of Bucha, Kherson, Mariupol, and elsewhere, such talk raises the specter of genocide. Leaders who are willing to engage in genocide might not feel many inhibitions about using a nuclear weapon.

We do not know what is in Putin’s head, of course. But the worry is that if the war continues going badly for Russia, Putin might reach for a tactical nuclear weapon—a low-yield bomb designed for use on the battlefield—out of frustration. While smaller than the big city-razing strategic ones, they are still tremendously destructive thermonuclear weapons with all the devastating effects of the Hiroshima bomb.

The United States and Ukraine do not have identical interests in this war. While Russia’s aggression, protected by nuclear threats, must not pay, the United States has an obligation to avoid a wider war that could increase the risk of direct U.S.-Russian confrontation. Of all the lessons of the past, the risk of nuclear war is one we forget only at our deepest peril.

## Rapid Response Force

### Uniqueness – Rapid Reaction Force

#### NATO mobilizing Reaction Force for first time – and increasing its troop presence in Black Sea region

**Shea, 2022**

[Jamie, Associate Fellow, International Security Programme “NATO must now transform old missions into new strategy” Chatham House, June 21 2022 <https://www.chathamhouse.org/2022/06/nato-must-now-transform-old-missions-new-strategy> accessed GDI-TM]

Transitioning from temporary to permanent deployment

NATO has also mobilized its high-readiness Reaction Force for the first time and aims to establish four new multinational battalions in the Black Sea region – with France offering to lead the one in Romania, Italy in Bulgaria, and the Czech Republic in Slovakia. Most of these deployments are on a temporary basis, but the receiving allies would understandably like them to stay longer and for NATO to commit to permanent stationed forces.

Although this would oblige the alliance to break formally from the pledge it made to Moscow in 1997 not to station substantial combat forces or nuclear weapons or build military infrastructure on the territory of its new member states in eastern Europe, this was a political undertaking linked to circumstances prevailing at the time.

Given Russia’s behaviour, there is no reason why NATO should not now abandon it. There is also a question over whether NATO could also repeal the NATO-Russia Founding Act and the NATO-Russia Council, or simply leave them in suspension for a future, more cooperative, and less bellicose Russian regime.

### Uniqueness – NATO troop posture

#### Uniqueness – brink – NATO facing decision in force posture shift from Enhanced Forward Presence

**Shea, 2022**

[Jamie, Associate Fellow, International Security Programme “NATO must now transform old missions into new strategy” Chatham House, June 21 2022 <https://www.chathamhouse.org/2022/06/nato-must-now-transform-old-missions-new-strategy> accessed GDI-TM]

Beyond showing the flag along its eastern flank, NATO does face longer-term issues which need to be clarified in its new Strategic Concept. First is whether to abandon its current strategy of reinforcement and military mobility across Europe – known as the Enhanced Forward Presence in the NATO jargon – in favour of the deployment of heavy armoured brigades or even divisions in fixed positions close to borders. This will be expensive in the long-run and deprive allies of the flexibility they have enjoyed since the end of the Cold War to use their forces as and where they wish – from deployments in the Sahel or Afghanistan to fighting forest fires or building emergency hospitals for COVID-19 patients at home. The only exception is when they have put forces on rotation into the NATO high readiness forces or the European Union (EU) Battle Groups. Germany’s commitment gives NATO more options The decision of Germany to increase its defence spending to two per cent of GDP and to devote €100 billion to modernizing the Bundeswehr makes it technically possible for NATO to move to a Cold War-style forward, armoured defence. But it is unclear how quickly Berlin could raise its new divisions given its problems with procurement and government/industry relations in the defence sector. It may make more sense for Germany not to launch new acquisition programmes but to buy existing off-the-shelf capabilities – as it has recently done with its decision to buy 35 US F35 aircraft – which other European countries are also acquiring, offering economies of scale and cheaper operating and maintenance costs. But if Germany abandons ambitious defence projects with France – which prefers a ‘buy European’ approach – such as the Future European Air Combat System, the relationship with France will become strained and French plans for EU self-reliance in the military field put at risk. As a country averse to war fighting and narrow military approaches to security, it is uncertain how much of the conventional defence burden in NATO Germany would be willing to take on, so this could be the opportunity to create more integrated European units with France, the Benelux, Poland, and Italy, even with the post-Brexit UK. The UK has doubled the size of its forces in Estonia and sent 1,000 troops to Poland, as well as devoting a substantial portion of its army, navy, and airforce to regular NATO exercises in the Baltic region. London was also the first ally to grant Sweden and Finland a temporary security guarantee pending full integration into the alliance. NATO will likely settle on a compromise, increasing the size of its battalions on its eastern flank – turning them into battle groups – but giving each one a larger reserve force which will remain in Germany or other European allied countries.

## Russia /NATO credibility OCO adv

### Impact – deterrence fail = US Russia war

#### Russian aggression in Baltics draws US into direct conflict with Russia

**Yousif, 2022**

[Elias “NATO’s Frontline – How Russia’s Invasion of Ukraine is Shaping Security Cooperation with the Baltics” Stimson Center March 2, 2022 <https://www.stimson.org/2022/natos-frontline-shaping-security-cooperation-with-baltics/> accessed 7/7/22 GDI-TM]

The invasion of Ukraine has sparked a substantial expansion in NATO presence in the Baltics. Over the course of the last several weeks and months, the United States has deployed an additional 15,000 troops and advanced U.S. defense equipment to Europe, including F-35 fighters and an infantry battalion taskforce to the Baltics. Other NATO allies are also expanding their presence to add to rotational deployments in the Baltics, including the UK, Germany, Norway, and Denmark. NATO has also, for the first time, activated its Response Force, a contingent of more than 40,000 allied special operations and maritime troops now on high alert.

Nevertheless, the NATO presence in the Baltics is often seen less as a practical defense measure but rather as a “tripwire” for any potential Russian assault, making it clear that such military action against NATO’s eastern flank would be against many members of the alliance, including the United States. Still, the future of Eastern Europe remains deeply unsettled, with renewed focus on potential fault lines between Russia and its Baltic neighbors. And while the Biden Administration has made it clear that U.S. troops will not be engaged in Ukraine, Estonia, Latvia, and Lithuania are NATO allies and host to hundreds of U.S. troops. **Any spillover of the crisis there could trigger a direct confrontation between Moscow and Washington, with dire consequences for international security.** With the Russian invasion wreaking increasing violence on Ukraine, many eyes will be turned to Estonia, Latvia, and Lithuania to judge the contagion of this conflict.

#### US Russia war massive and goes nuclear – prioritize this impact because cognitive bias underestimates it, and deterrence can’t solve it.

Beebe 19 [George, VP and Director of Studies at the Center for the National Interest, a nonpartisan think tank, former head of Russia analysis at the CIA, “We’re More at Risk of Nuclear War With Russia Than We Think,” October 7, *Politico*, <https://www.politico.com/magazine/story/2019/10/07/were-more-at-risk-of-nuclear-war-with-russia-than-we-think-229436>, accessed 07/04/22, GDI-JCR]

Today, that old dread of disaster has all but disappeared, as have the systems that helped preclude it. But the actual threat of nuclear catastrophe is much greater than we realize. Diplomacy and a desire for global peace have given way to complacency and a false sense of security that nuclear escalation is outside the realm of possibility. That leaves us unprepared for—and highly vulnerable to—a nuclear attack from Russia. The most recent sign of American complacency was the death, a few weeks ago, of the Intermediate-Range Nuclear Forces Treaty—a pivotal 1987 agreement that introduced intrusive on-site inspection provisions, destroyed an entire class of dangerous weaponry, and convinced both Washington and Moscow that the other wanted strategic stability more than strategic advantage. The New START treaty, put in place during the Obama administration, appears headed for a similar fate in 2021. In fact, nearly all the key U.S.-Russian arms control and confidence-building provisions of the Cold War era are dead or on life support, with little effort underway to update or replace them. Meanwhile, U.S. officials from both parties are focused not on how we might avoid nuclear catastrophe but on showing how tough they can look against a revanchist Russia and its leader, Vladimir Putin. Summit meetings between White House and Kremlin leaders, once viewed as opportunities for peace, are now seen as dangerous temptations to indulge in Munich-style appeasement, the cardinal sin of statecraft. American policymakers worry more about “going wobbly,” as Margaret Thatcher once put it, than about a march of folly into inadvertent war. President Donald Trump’s suggestion that the United States and Russia might explore ways to manage their differences diplomatically has produced mostly head-scratching and condemnation. In my more than 25 years of government experience working on Russia matters, I’ve seen that three misguided assumptions underlie how the United States got to this point. The first is that American policymakers think that because neither side wants nuclear war, then such a war is very unlikely to occur. Russia would be foolish, we reason, to cross swords with the powerful U.S. military and risk its own self-destruction, and many Americans find it hard to imagine that modern cyber duels, proxy battles, information operations and economic warfare might somehow erupt into direct nuclear attacks. If the Cold War ended peacefully, the thinking goes, why should America worry that a new shadow war with a much less formidable Russia will end any differently? But wars do not always begin by design. Just as they did in 1914, a vicious circle of clashing geopolitical ambitions, distorted perceptions of each other’s intent, new and poorly understood technologies, and disappearing rules of the game could combine to produce a disaster that neither side wants nor expects. In fact, cyber technologies, artificial intelligence, advanced hypersonic weapons delivery systems and antisatellite weaponry are making the U.S.-Russian shadow war much more complex and dangerous than the old Cold War competition. They are blurring traditional lines between espionage and warfare, entangling nuclear and conventional weaponry, and erasing old distinctions between offensive and defensive operations. Whereas the development of nuclear weaponry in the Cold War produced the concept of mutually assured destruction and had a restraining effect, in the cyber arena, playing offense is increasingly seen as the best defense. And in a highly connected world in which financial networks, commercial operations, media platforms, and nuclear command and control systems are all linked in some way, escalation from the cyber world into the physical domain is a serious danger. Cyber technology is also magnifying fears of our adversaries’ strategic intentions while prompting questions about whether warning systems can detect incoming attacks and whether weapons will fire when buttons are pushed. This makes containing a crisis that might arise between U.S. and Russian forces over Ukraine, Iran or anything else much more difficult. It is not hard to imagine a crisis scenario in which Russia cyber operators gain access to a satellite system that controls both U.S. conventional and nuclear weapons systems, leaving the American side uncertain about whether the intrusion is meant to gather information about U.S. war preparations or to disable our ability to conduct nuclear strikes. This could cause the U.S. president to wonder whether he faces an urgent “use it or lose it” nuclear launch decision. It doesn’t help that the lines of communication between the United States and Russia necessary for managing such situations are all but severed.

### Impact – Escalation Ukraine war = Russian imperialism

#### Failure to stop Putin in Ukraine increases risk of Russian imperialism and invasion other European countries

**Dickinson**, editor of the Atlantic Council’s UkraineAlert Service **2022**

[Peter, “Putin admits Ukraine invasion is an imperial war to “return” Russian land” Atlantic Council, June 10, 2022 <https://www.atlanticcouncil.org/blogs/ukrainealert/putin-admits-ukraine-invasion-is-an-imperial-war-to-return-russian-land/> accessed 7/7/22 GDI-TM]

This openly imperialistic agenda represents an unprecedented challenge to international law and poses a grave threat to the entire post-WWII global security system. It also exposes the absurdity of appeals to appease Moscow or accept some kind of negotiated settlement that would avoid “humiliating” Russia. There can be no compromise with the Kremlin as long as Putin continues to deny Ukraine’s right to exist and declares his intention to annex entire regions of the country. If Putin is not decisively defeated in Ukraine, he will surely go further in his mission to “return” lost Russian lands. The list of former Russian imperial possessions that could potentially become targets is extensive and includes Finland, the Baltic States, Poland, Belarus, Moldova, Georgia, Armenia, Azerbaijan, and the nations of Central Asia. Nor can future Russian attacks on the former Warsaw Pact countries of Central Europe be entirely ruled out. If this sounds far-fetched, it is important to remember that almost nobody in Ukraine believed a Russian invasion was even remotely possible until it actually happened. Today’s brutal colonial war in Ukraine is a reminder that unlike the other great European empires of the nineteenth and twentieth centuries, Russia never underwent a period of de-imperialization. Despite collapsing spectacularly in both 1917 and 1991, Russia’s imperial identity is still very much intact and has become a central pillar of the Putin regime. Until Russia enters the modern era and becomes a post-imperial power, peace in Europe will remain elusive. The best way to speed up this process is to ensure Ukraine wins the war.

### Impact - Russia – proxy threats

#### Impact –use of proxy cyber threats destabilize infrastructure and NATO missions – past Russian attacks prove

**Păunescu, 2021**

[Dragoș-Mihai, PnD in International relations at the Carol I National Defence University, “NATO’S ENCOUNTERS IN THE CYBER DOMAIN”, 11/9/2021, https://revista.unap.ro/index.php/XXI\_FSA/article/view/1274/, accessed 6/29/22, GDI- CC]

Russia represents a significant cyber threat to NATO and this has already been demonstrated  by integrating cyber in the operations carried out during the Georgia and Ukraine/Crimea conflicts.  Cyber is a low cost and deniable tool, especially when “non-state” proxies are used. The use of  Moscow proxies to disrupt and destabilize the civilian population and critical infrastructure particularly  in its near abroad, but also in NATO/EU space bordering Russian territory, is a distinct possibility.

Generally, a proxy is in the service of a state-actor when the respective state lacks the  required skills, knowledge and means to operate in cyberspace. Another important reason for state  actors to use proxies could be associated to political unwillingness to openly employ state resources,  especially in those cyber operations that contradict legal, ethical, cultural or assumed norms. A state operating through proxies could demonstrate plausible deniability, whilst not exposing state-owned  technical capability.

Often Moscow has an important influence on elections, public opinion and even politicians  using information warfare and cyber-attacks. Russian also interfered with NATO exercises and other  Baseline Activities and Current Operations (BACO) using cyber operations, but also Electronic  Warfare (EW) interference (including GPS jamming) to disrupt Alliance’s events. To estimate the  impact and the effectiveness of such activity coordinated by Moscow is difficult given the challenges  faced by NATO and its members individually to implement effective cyber defense capabilities.

### \*\* Answer to Answer Blocks \*\*

### AT: NATO not key to stop Russia

#### NATO can crush Russia with sustained US leadership

**Hooker**, Non-Resident Senior Fellow at the Atlantic Council, **2022**

(Jr R.D., "The State of NATO: An American View," Survival, Vol. 64, no. 3, pg. 103-113, 2022, Taylor & Francis, accessed 6/30/2022, gdi-tmur)

At the June 2021 NATO summit in Brussels, leaders agreed to develop an updated Strategic Concept for approval in 2022 based on a new consensus. If the Strategic Concept is to be more than a rhetorical exercise, it must substantively address the difficulties that beset the Alliance and the challenges facing it. The mortal threat posed by a vengeful Russia should form the core of the next version.

The good news is that NATO holds most of the cards. Its combined GDP is some 20 times greater than Russia’s, and its overall defence spending about 14 times greater. NATO’s 30 allies and close, official partners such as Australia, Finland, Japan, South Korea and Sweden constitute most of the economic and military power on the planet, and their combined populations dwarf Russia’s. In key capabilities such as theatre logistics; strategic airlift; intelligence, surveillance and reconnaissance; and sealift, NATO swamps Russia’s modest holdings, while the list of Russia’s allies is both short and unimpressive.

Nevertheless, NATO must have the will to compete, and the US must lead and encourage, as it has since the Ukraine crisis began. The Ukraine crisis has illuminated one founding premise of the Alliance that had been obscured: that America’s support for NATO is not based on altruism.

### AT: Ukraine sanctions reduce Russia threat

#### Russia still a threat despite setbacks – resources and nuclear arsenal

**Hooker**, Non-Resident Senior Fellow at the Atlantic Council, **2022**

(Jr R.D., "The State of NATO: An American View," Survival, Vol. 64, no. 3, pg. 103-113, 2022, Taylor & Francis, accessed 6/30/2022, gdi-tmur)

For seven decades, the North Atlantic Treaty Organization has been the backbone of American and European security, in tandem with nuclear deterrence, as a guarantor of peace in Europe and a major force for global stability. The unifying and most obvious threat is Russia, a quasi-imperial power intent on reasserting control and influence over its ‘near abroad’ and regaining its place as a great power on the world stage. With its attempted conquest of Ukraine, Russia has yet again used military aggression to reassert dominance in the territories of the former Russian empire. This follows a decade of Russian belligerence in Chechnya, Georgia, Donbas and Syria.

Russia’s probable resilience

Russia’s substandard military performance and Ukraine’s steadfast resistance have cast doubt on Vladimir Putin’s goal of outright conquest. Russia, of course, has survived several major setbacks in the last century – Finland in 1940, western Russia in 1941, Grozny in 1995 – only to recover and prevail. Absent direct NATO intervention, a negotiated settlement guaranteeing Ukrainian neutrality that leaves Putin in possession of Luhansk, Donetsk, Crimea and the land bridge connecting them through Mariupol remains a possibility, along with eventual sanctions relief. Such an outcome, even at high cost, would enable Putin to claim success. After rebuilding his economy and military, more aggression in pursuit of Putin’s grand vision and ambitions is possible and perhaps likely.

The Baltic states represent exactly the kind of emerging, prosperous Western democracies on former Soviet territory that Putin is known to detest and fear. They each possess ethnic-Russian minorities, especially Estonia and Latvia. They stand between Mother Russia and Kaliningrad, home of Russia’s Baltic Fleet, but isolated and separated by 300 kilometres from the Russian border. Wrenching the Baltic states from NATO control would restore the strategic depth Russia lost in the 1990s and end future NATO expansion for Ukraine and Georgia. These are tempting rewards, and Moscow might imagine grasping them after a period of truce in Ukraine and recovery at home, or in a spasm of desperation if things turn more dire.1

The Baltic region is not the only European area of interest to Russian planners. Russia’s seizure and annexation of Crimea in 2014–15 effectively turned the Black Sea into a Russian lake.2 With 28,000 troops in Crimea, supported by the S-400 air-defence system and anti-ship cruise-missile batteries, Russia is well postured to dominate the Black Sea region.

The West often prefers to describe Russia as ‘in decline’, fostering the view that the threat will soon dissipate.3 This is a mistake. Despite its failures in Ukraine, Russia is still a formidable adversary, possessed of enormous territory, vast natural resources, a strong and intact culture, and an educated and patriotic population enamoured with its historical status as a great power. Russia still has the world’s strongest nuclear arsenal. To be sure, while its economy ranked sixth in the world in terms of purchasing power parity before Ukraine, devastating sanctions are likely to hobble Russia for some time. Nevertheless, it is unlikely to fade into irrelevance.4

## Space capabilities

### SQ = Inaction on Space Security

#### Not enough attention to cyber vulnerabilities in the status quo

Unal 19 [Beyza, senior research fellow with the International Security Department at Chatham House, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, “Cybersecurity of NATO’s Space-based Strategic Assets,” Chatham House Research Paper, July, <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>, accessed 07/04/22, GDI-JCR]

Strategic military systems depend heavily on space-based assets for navigation and targeting, timing, positioning, command and control, operational monitoring, intelligence gathering and reconnaissance, among other functions. However, the increasing vulnerability of space-based assets, ground stations, associated command and control systems, and the personnel who manage the systems, has not yet received the attention it deserves. This is particularly true in regard to the so-called ‘New Space’ revolution: the growing role of the private sector in space. For example, during the Iraq war of 2003–11, there was a 560 per cent increase in the US reliance on commercial satellites for military purposes.9 Policy influencers and policymakers are struggling to grasp the full impact of cyber vulnerabilities in the context of both space-based assets and strategic systems. Just as with physical attacks on space-based assets – such as anti-satellite weapon (ASAT) strikes10 – cyberattacks have the potential to wreak havoc on strategic weapons systems and undermine deterrence by creating uncertainty and confusion. Cyberthreats pose a significant and complex challenge due to the absence of a warning and speed of an attack, the difficulty of attribution, and the complexities associated with carrying out a proportionate response. Given the progress made in the areas of strategic conventional weapon systems – for example, the development of advanced cruise missiles and hypersonic glide vehicles – it is essential for NATO and its allies to be able to rely upon space-based systems for early observation and detection; this may enable them to identify and attribute activities and to launch effective, calibrated responses. Cyber technology and innovation are accessible across much of the world, levelling the field and creating opportunities for states outside the NATO alliance – such as China, Russia and North Korea, for example – to instigate high-impact attacks on allied-owned strategic assets

#### \*NATO needs a more proactive policy toward cyber security of space assets – Russia and China are deploying offensive tech

Unal 19 [Beyza, senior research fellow with the International Security Department at Chatham House, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, “Cybersecurity of NATO’s Space-based Strategic Assets,” Chatham House Research Paper, July, <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>, accessed 07/04/22, GDI-JCR]

Cyber research is a fast-moving and constantly evolving area of science, and the scope of cyberthreats that countries face is on the rise as malicious actors find new ways to infiltrate weapons systems. The use of electronic warfare methods and cyberattacks in peacetime illustrates the blurred lines of engagement between nations even in the absence of conflict. According to Norwegian military and NATO officials, Russia persistently jammed civilian GPS signals during NATO’s 2018 Trident Juncture exercise in Europe’s High North region, which highlights the growing threat. In November 2018, NATO Secretary-General Jens Stoltenberg stated that electronic warfare and cyberattacks were increasingly being used in operations.14 It was also reported that NATO officials believed Russia is testing this capability through its large-scale exercises, such as Zapad 2017, which was conducted jointly with Belarus in September 2017.15 According to the Consultative Committee for Space Data Systems (CCSDS), the most common cyberthreats to the space segment, ground segment and space-link communication segment include data corruption/modification; ground system loss; interception of data; jamming; denial of service; masquerade (spoofing); replay; software threats; and unauthorized access.16 There is also crossover between offensive and defensive activities in cyberspace and space, given that – technologically – offence is easier and more cost-effective than defence.17 Furthermore, space-related personnel are vulnerable to cyberthreats. Social engineering is becoming an important tool when used by adversaries, and – whether it occurs deliberately or unwittingly – the potential for people to constitute the weakest link in cyber defence is an increasing reality.18 The nature of cyber activities must evolve from being purely defensive to include active, persistent engagement, in order to disrupt attackers of western critical space-based capabilities. Given the importance of space-based systems to critical infrastructure that supports NATO military capabilities, it would be prudent to assume that an adversary is already active in these networks and focus on resilience measures. This increases urgency for advanced techniques, such as AI and machine learning (ML),19 to identify and respond to modern threats. Both China and Russia prioritize electronic warfare, cyberattacks and superiority within the electromagnetic battlespace as part of a strategy to achieve victory in future operations. Available doctrine from these nations highlights a key focus on preventing adversarial satellite-based communication systems from impacting their operational effectiveness20 – a focus shared in US military planning and policy.21 Russian space capabilities and their cybertechnologies pose particular threats to NATO. For its navigational system, Russia relies on its own satellite system GLONASS (Global Navigation Satellite System), rather than the US-provided GPS or the EU’s Galileo system. As part of a series of improvements to its communications technology and GLONASS, Russia is designing new navigation satellites, which are claimed to be highly accurate and longer lasting.22 Russia has been testing its capabilities in a hybrid context in Syria and in Ukraine, particularly relying on capabilities for jamming GPS signals to ground remotely piloted aircraft. It is reported to have conducted denial-of-service attacks on radio and telephone equipment, and to have attempted to steal encrypted military data.23

### Cyber Attacks Increasing

#### Cyber becoming the norm for ASAT attacks

**Tepper**, research coordinator and lecturer for space governance at Laval University, **2022**

(Eytan, “The First Space-Cyber War and the Need for New Regimes and Policies,” Center for International Governance Innovation, Policy Brief No. 173, May 2022, https://practicesource.com/wp-content/uploads/2022/05/apo-nid317939.pdf, accessed 7/4/2022, gdi-tmur)

\*GPS = Global Positioning System

Space-based infrastructure is a critical infrastructure for security and the economy — in fact, it is critical to most aspects of modern life — and therefore is a prime target for malicious attacks (Falco 2019). The most significant current security threat to space-based infrastructure and applications is from cyberattacks. Only a handful of countries have the capabilities to physically destroy satellites (Weeden and Samson 2022) — and they are likely to be exposed as the perpetrators. In contrast, executing a cyberattack requires much less in terms of funds and technological and engineering capabilities. Moreover, the attacker can attempt to cover its tracks, leaving the attacked country uncertain about attribution and its own response. Therefore, cyberattacks are likely to become the leading method of targeting space-based infrastructure for state actors, as well as non-state actors, notably criminal organizations and terrorist groups. There is evidence that such attacks have already occurred: Russia allegedly disrupted Global Positioning System (GPS) signals during North Atlantic Treaty Organization exercises in Finland, Sweden and Norway in 2018 (Harrison et al. 2020), affecting, inter alia, the ability of commercial aircrafts to navigate; Turla, a Russian criminal gang, allegedly hijacked satellite IP (Internet Protocol) addresses (Zetter 2015), which it later used to steal data; and Hamas of Gaza, a terrorist organization, hacked the satellite broadcast of a major Israeli television channel (Leyden 2014). A cyberattack targeting space assets, or space-cyberattack, can jam GPS signals, disabling navigation, or spoof GPS signals, providing misleading locations, in both cases disrupting travel and guided weapons systems. A space-cyberattack can “blind” remote sensing satellites that provide satellite imagery and other data collected by various sensors. It can interrupt communication satellites services, including television, radio and internet. Moreover, it can disrupt banking and payment systems, including the use of credit cards and automated banking machines, which rely on satellite-based precise timing. Indeed, important segments of the global financial system depend on GPS (Fernholz 2017). Further, a space-cyberattack can do more than render a satellite defunct: it can turn it into a weapon, for example, by taking control of it and altering its course so that it crashes into another satellite. Indeed, the combined space-cyber warfare theatre will be the primary battlefield for global powers in the twenty-first century (Boucher 2013). Accordingly, a report published by Harvard’s Belfer Center for Science and International Affairs suggested that the first mission of the new US Space Force should be to ensure cybersecurity of space assets (Falco 2018). In a signal on the future of warfare, the head of the US Indo-Pacific Command, Admiral John Aquilino, recently noted, “We’ve come a long way in a short time to be able to integrate the space and cyber domains” (quoted in Sevastopulo 2022).

### Cyber exercises/Military to military exercises key

#### Cooperative training exercises needed to shore up NATO space cybersecurity

Unal 19 [Beyza, senior research fellow with the International Security Department at Chatham House, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, “Cybersecurity of NATO’s Space-based Strategic Assets,” Chatham House Research Paper, July, <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>, accessed 07/04/22, GDI-JCR]

Training is essential to create awareness and prepare the alliance for worst case scenarios. NATO could promote different types of training that would capture space security and system vulnerabilities to cyberattacks. Training areas could be selected through a lessons-learned analysis where former cases could be used to highlight areas of greatest need. Some examples are as follows: • At the political-strategic level, crisis management exercises (CMX), hybrid warfare exercises and similar training could incorporate cyber resilience and bring space elements into cybersecurity training. • At the technical level, given the complexity of space systems, focused training, modelling and simulation would be key to ensuring design integrity. • Bringing the technical and political communities together in training modules would be helpful. Often the political community and technical community do not metaphorically speak the same language and their concerns do not merge. Such training would be technology-driven and could incorporate modelling and simulation. Thus, technical expertise and knowledge could be transferred into political action plans. • Training may also involve the private sector or contractors. NATO decides whether or not it should delegate parts of the training to the private sector or to conduct it internally. There are advantages and disadvantages in both. One of the advantages in delegating the work to an outside party is that the latter could conduct an analysis without any NATO restrictions and could significantly test NATO’s planning and operations. The main disadvantage is that NATO may not be able to share classified information, which would make the training less comprehensive. • Some of the most useful training methods involve exercises, ‘war gaming’, crisis simulations and scenario planning, as well as online training education programmes, training manuals, and certifications. NATO should also measure the impact of the training and assess its skill-maintenance capacity.

#### Crisis Management Exercises with space assets, coordination/standardization of national security frameworks

Cesari et al 21 [Laetitia, Consultant at the UN Institute for Disarmament Studies, “Space as NATO’s Operational Domain: The Case of the Cyber Threats against GNSS,” 72nd International Astronautical Congress (IAC), Dubai, United Arab Emirates, 25-29 October 2021, <https://spacegeneration.org/wp-content/uploads/2022/04/IAC-21E927x66298_Space-as-NATOs-Operational-Domain-The-Case-of-the-Cyberthreats-against-GNSS_Paper.pdf>, accessed 07/04/22, GDI-JCR]

NATO has to review and renew its strategies for building defences by policy development and raising awareness against new and evolving threats, to protect space-based technologies that supplement lost capabilities and negate adversarial interference with space systems. NATO relies on its Allied capabilities; therefore, it is essential to have a unique coordinate system to respond during a crisis. The already existing exercises, such as the Crisis Management Exercise (CMX) which focus on cyber, and resilience should be implemented with space assets. This internal and partner consultation and decision-making procedures at the strategic politicalmilitary level would help to strengthen the alliance response and resilience. Therefore, NATO has to operate with a renewed focus on improving proficiency in Allied Cyberspace and Electromagnetic Spectrum Operations, by building awareness, developing policies and strategies, acquiring new capabilities, working with industry and academia, and training people to become experts. Building defence is possible by “raising awareness” throughout the NATO systems, and by creation of regulation through NATO security framework , in a standardized and collective way which require a proactive effort to prevent, detect and prepare forces to respond to incidents, by developing guidelines, resources, and working groups focusing on emerging technologies to protect the space assets, and test coherency of the rules and their application by raising preparedness, building blocks between law and policy requirements for collective defence. The traditional policy creation mechanisms are based on multilateralism. States and most of the traditional international organizations struggle to adapt themselves to evolving realities of the new technologies and their applications and implications in new domains, such as cyber and space. Another aspect is to keep the will and interests of member states alive for policy development. This requires NATO to revise and update/adapt its mechanisms, in a way to support a clear-eyed, inclusive policy development, to overcome siloed or single domain-based approaches, to manoeuvre and react in the extremely complex environments. As a military-security organization, and as to its foundational concerns, unlike UN, NATO cannot represent an open forum for the intellectual construction, however, can support and benefit from the effective participation of the commercial actors, which own operate and manage these new domains, and can assess and adapt these new policies created to remain at the speed of relevance, as highlighted in JAPCC 2021 meeting this year

### Internal link - NATO Cyber Coop Key

#### Cyber vulnerability of NATO space assets risks crushing NATO’s military capabilities and deterrence – only fostering cooperation on cyber security can solve.

Lumiste 19 [Liina, International Law Researcher for the NATO Comparative Cyber Defence Centre of Excellence, “Chatham House report: Space – NATO cyber security’s weak spot,” <https://ccdcoe.org/library/publications/chatham-house-report-space-nato-cyber-securitys-weak-spot/>, accessed 07/04/22, GDI-JCR]

In 2018, Norwegian military and allied officials confirmed that Russia had disrupted NATO’s Trident Juncture exercise in Europe’s High North region by persistently jamming GPS signals during the exercise. China has claimed ‘the ability to use space-based systems and to deny them to adversaries as central to modern warfare’. As the dependence of military operations on space-based assets has increased exponentially over the last few decades and space-based assets are potential targets for cyber attack, the newly released Chatham House research paper ‘Cybersecurity of NATO’s Space-based Strategic Assets‘ suggests that NATO should bring space more to the spotlight. The research paper lists cyber threats to space-based strategic assets and capabilities, analyses capability requirements and gives concrete recommendations for ways improve the resilience of the space-based systems. Space-based assets as targets for cyber attacks Strategic military systems depend on space-based assets for the provision of data and for many capabilities, such as positioning, navigation and timing (PNT), intelligence, surveillance and reconnaissance (ISR), missile defence, communications, space situational awareness (SSA) as well as environmental monitoring. For accurate timing and navigation in PNT systems, NATO uses the global positioning system (GPS) which is also well known and widespread in civil use. ISR information and imagery is collected through surveillance and reconnaissance sensors. Both systems are satellite-based. Unmanned aerial vehicle (UAV) systems also rely on satellite-based ‘beyond-line-of-sight’ communication. These are only a few of the possible examples. In addition to the abundance of capabilities, it is noteworthy that the capabilities are also linked and therefore affecting one capability may cause collateral effects on others. As explained in the Space Threat Assessment 2018 published by the Centre for Strategic and International Studies (CSIS), there are several intrusion points for space-based assets: antennas on satellites and ground stations, landlines that connect ground stations to terrestrial networks, and user terminals that connect to satellites. This can result in data or data traffic monitoring, inserting false or corrupted data in the system, or even the permanent loss of a satellite. As with every other technology, people have the potential to be the weakest link in the cyber defence of space-based assets – social engineering is an important tool for the adversary. Vulnerabilities The research paper highlights some of the most important vulnerabilities: use of commercial companies; ‘back-doors’; dual use of satellites; and supply chain security of space technology. Chatham House reports have touched on these topics before. The question of supply chain was raised in the Livingstone and Lewis 2016 report, which observed that there was no coherent global organisation with regard to cyber security in space and that existing approaches had only limited reach into the supply chain. In this year’s research paper, it is again stressed that when the supply chain does not ensure that military security standards are met, items procured may expose NATO systems to vulnerabilities. NATO by itself does not own satellites, but is dependent on member states. In case of need, NATO requests access to products and services from the allies. NATO allies procure equipment and software, which will be integrated into their national defence infrastructure. In most cases, military and commercial assets are not separate. Therefore, NATO does not rely only on military assets, but also uses commercial, civilian and national or multinational assets for operations. Even though commercial methods have proven to be effective, they are accompanied by the inherent risk of lower security requirements. Data exchange between civil and military sectors may cause extra vulnerabilities. As most of the space-based capabilities are dual-use, meaning that assets are used both for military and civilian purposes, the Chatham House research paper recommends that operators ‘apply higher-grade military hardening and cyber protection specifications to civilian capabilities that have the potential to be used in support of military applications’. The research paper also highlights the aspect of NATO’s dependency on member states for communication capacity as a possible source of vulnerabilities. NATO owns satellite communications (SATCOM) ground stations, but no satellites; it is therefore highly reliant on allies to provide space-sourced data, information and services. In addition, ensuring the security of space capabilities is mostly in the hands of the allies. This puts NATO into a position where its main option to protect capabilities of vital importance is to encourage allies to put effort into securing the space-based assets and foster cooperation in space-based systems cyber security. Space as a domain of operations? During the Brussels Summit in 2018, the Alliance recognised space as a ‘highly dynamic and rapidly evolving area, which is essential to a coherent Alliance deterrence and defence posture’ and on 27 June 2019, it approved new space policy. As claimed by NATO’s Secretary General, Jens Stoltenberg, the space policy gives guidance on opportunities and challenges and is not about militarising space, but about information sharing and increasing interoperability. The research paper suggests that, in addition to policy, NATO needs to agree upon space doctrine. While policy directs, assigns tasks and prescribes desired capabilities, doctrine provides principles of how operations should be planned, prepared, commanded, conducted, sustained, terminated and assessed.1 This suggestion becomes even more relevant when taking into consideration recent announcements by some NATO diplomats about NATO’s aims to recognise space as a domain of warfare during the London summit at the end of 2019. This indeed would be a big step towards focusing more on space-based assets and their vulnerabilities. Considering the current context, in which China and Russia are increasing their presence in space, this action by NATO is inevitable. Whether or not NATO claims space as a domain, adversaries will nevertheless develop their aggressive capabilities, from cyber operations to anti-satellite missiles. Therefore, it is prudent to update the approach towards space and space-based assets to face new challenges. Yet, claiming space to be a domain of warfare highlights legal considerations. The Chatham House research paper raises a question from the cyber perspective: whether a cyber attack on a space system has to have kinetic consequences in order to give grounds for collective self-defence according to the Washington Treaty. This can be supplemented with a question on whether causing kinetic consequences that result in debris breaches the responsibility not to cause widespread, long-term and severe damage to the natural environment, as stipulated in article 35 of Additional Protocol I to the Geneva Conventions of 12 August 1949.2 Another question raised is targeting dual-use space technology in international humanitarian law (IHL). The principle of distinction foresees the duty to distinguish between the civilian population and combatants and between civil and military objects. As in the case of cyber objectives,3 dual-use satellites should be counted as military objectives, but would be subject to the rule of proportionality and requirement to take precautions in attack.4 Conclusion The Chatham House research paper makes recommendations that more or less all stress the same things: NATO is highly dependent on space capabilities; space-based systems are vulnerable to cyber attacks and will become more and more appetising targets for adversaries; and NATO must foster cooperation and information sharing between member states. Overlooking these aspects could undermine the credibility of the information provided through the space-based systems, which would in turn affect deterrence and strategic liability. In the broader view, destabilising space-based assets would not only affect military conduct, but also have severe effects on civil infrastructures.

#### NATO coop key to deter Russia and China

**Raymond**, Chief of Space Operations @ US Space Force, **2021**

(General John W., “#SpaceWatchGLShare: NATO Space by Gen John W. Raymond,” SpaceWatch.Global, March 2021, https://spacewatch.global/2021/06/spacewatchgl-share-nato-space/, accessed 7/4/2022, gdi-tmur)

International cooperation in Space has never been more important than it is today. Chinese and Russian military Space activities present serious and growing threats to NATO’s security interests due to their development, testing, and destabilizing deployment of counterspace capabilities, along with their associated military doctrine for employment in conflict extending into Space. Although the broader strategic threats posed by China and Russia are different, each has weaponized Space as a means to challenge our freedom of operation in Space and reduce US and NATO military effectiveness. NATO’s Space strategy and doctrine should be poised to counter, respond to, and deter the full range of competition and military conflict, including hybrid threats and military activities that fall short of war.

#### Allied coordinated efforts key to reduce Sino-Russian technological advantages in space

**Raymond**, Chief of Space Operations @ US Space Force, **2021**

(General John W., “#SpaceWatchGLShare: NATO Space by Gen John W. Raymond,” SpaceWatch.Global, March 2021, https://spacewatch.global/2021/06/spacewatchgl-share-nato-space/, accessed 7/4/2022, gdi-tmur)

China and Russia continue to develop Space capabilities that reduce the technological advantage long enjoyed by NATO Allies. Failure to innovate, adapt, and become more agile may make the Alliance’s Space capabilities less relevant in the near future. In the worst case, disadvantage in Space can create vulnerabilities for Allied forces in multiple domains. Space Force establishment allowed creation of new organizations and processes to unify complementing Space functions and authorities, already resulting in enhanced security options. To promote greater efficiencies, NATO members could likewise coordinate activities such as cooperative Science & Technology and Research & Development efforts. Working in a coordinated manner, NATO can help ensure our Space capabilities and associate architectures are fully functional throughout the spectrum of peace, deterrence, and conflict.

### Internal link - NATO Cyber Coop Key – Legal Harmonization

#### Cooperation needed to harmonize NATO member legal frameworks for cybersecurity of space assets

Cesari et al 21 [Laetitia, Consultant at the UN Institute for Disarmament Studies, “Space as NATO’s Operational Domain: The Case of the Cyber Threats against GNSS,” 72nd International Astronautical Congress (IAC), Dubai, United Arab Emirates, 25-29 October 2021, <https://spacegeneration.org/wp-content/uploads/2022/04/IAC-21E927x66298_Space-as-NATOs-Operational-Domain-The-Case-of-the-Cyberthreats-against-GNSS_Paper.pdf>, accessed 07/04/22, GDI-JCR]

The first challenge for NATO in Outer Space is regulatory, while the increasingly congested, contested, commercial, and competitive nature of Space operations intensifies the need for legal clarity and harmonization, the development of national space law frameworks are at a different pace. The lack of clarity weakens the alliances options for deterrence, therefore, as Secretary General Stoltenberg highlighted [28] build on previous cyberattack declarations to issue a formal declaration stating the readiness to counter attacks on Allied Space assets, including an explanation of which assets fall within the scope of the Treaty [29]. As a result, following the collective commitment under Article 3 of the North Atlantic Treaty, to reduce vulnerabilities and ensure Allied militaries can effectively operate in peace, crisis and conflict, to strengthen interoperability and understand vulnerabilities, While the institutional development is rapid, member states’ legal development at different pace and adoption of different standards, can lead to the progressive dismantling of regulatory standards or, as NATO Officials used, to a ‘race to the bottom’, which could compromise the interoperability of the Space legal frameworks of the member states, and reduce the collective value of space assets and negatively impacts NATO’s Space power projection [29]. To this end, one of NATO's space policy priorities is to foster enhanced interoperability by fostering a common legal Space doctrine based on agreements on fundamental mechanisms, international standards, or norms of behaviour, in which Allies can collaborate using operational assets and national policies or frameworks. “NATO does not own satellites, but owns and operates terrestrial elements, such as satellite communications anchor stations and terminals. It requests access to products and services of member states – such as space weather reports and satellite overflight reports provided via satellite reconnaissance advance notice systems – but does not have direct access to satellites: it is up to individual NATO member states to determine whether they allow access”

### Internal link - NATO Cyber Coop Key – Attribution

#### Credible space attribution process key to successful deterrence and builds NATO cohesion

**Raymond**, Chief of Space Operations @ US Space Force, **2021**

(General John W., “#SpaceWatchGLShare: NATO Space by Gen John W. Raymond,” SpaceWatch.Global, March 2021, https://spacewatch.global/2021/06/spacewatchgl-share-nato-space/, accessed 7/4/2022, gdi-tmur)

A credible, trusted, and transparent Space attribution process – the ability to trace the origin of an action against Space architectures – underpins a successful NATO Space deterrence strategy. Inability to determine the origin or source of a hostile or malicious action undermines the expectation of a credible response.7 Space Domain Awareness (SDA) is a critical part of attributing threatening or malicious action against Space architectures. SDA encompasses the effective identification, characterization, and understanding of any factor associated with the Space domain that could affect Space operations.8 The United States has already crafted more than 100 agreements to share situational awareness to support safe satellite operations. SDA alone, however, may not be enough to enable Space attribution. We must go deeper in our understanding of the domain. We must develop the means to determine the source and pathway of an attack against Space architectures after such an attack has occurred.9 We need scientific methods to gather data and information from satellites, ground systems, and associated networks regarding actions that are non-kinetic or kinetic, and reversible or non-reversible. For hostile actions in Space, the attribution process may lead to a military response. Yet for less serious acts in Space, attribution may lead to prosecution through civilian courts or diplomatic admonishment. For the Space attribution process to be viable when needed, NATO Nations must prepare now to develop the requisite SDA and scientific capabilities, rehearse related intelligence collection and information sharing, and integrate trusted commercial partners. By rehearsing the attribution process – such as during combined Space exercises and wargames – it may be determined that additional SDA capabilities are needed. Working together and sharing intelligence and information will lead to increased transparency and build trust and confidence in the Alliance’s Space attribution process. This trust and confidence established in peacetime can result in additional countries joining the Alliance’s effort during times of crisis.

### Internal link - NATO Action Key – Follow On

#### Member states look to NATO when formulating national space security policy

Unal 19 [Beyza, senior research fellow with the International Security Department at Chatham House, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, “Cybersecurity of NATO’s Space-based Strategic Assets,” Chatham House Research Paper, July, <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>, accessed 07/04/22, GDI-JCR]

If capabilities remain in national hands NATO’s role in the space realm should be considered. It could have the following functions: 1. Intelligence; 2. Creating dialogue with the space components industry; 3. Operational planning; and 4. Coordination/liaison with the allies on personnel requirements, in order to improve alliance knowledge and capacity on the use of space technology in NATO operations. In many areas, NATO allies that have either not invested in space technology or do not have sufficient capability to protect their systems, look to NATO as an informative entity that could guide them towards the best approach for space security. If NATO’s role in the space realm were to be clarified as discussed above, this could help those allies to perform their obligations.

#### Plan solves – ensures NATO allies collaboratively take actions to enhance space domain stability and reduce miscalculation

**Raymond**, Chief of Space Operations @ US Space Force, **2021**

(General John W., “#SpaceWatchGLShare: NATO Space by Gen John W. Raymond,” SpaceWatch.Global, March 2021, https://spacewatch.global/2021/06/spacewatchgl-share-nato-space/, accessed 7/4/2022, gdi-tmur)

NATO provides a forum to discuss the development of international norms of responsible behaviour for the utilization of Space that consider the changing Space landscape and security implications. This is especially true given the expected growth in Space traffic management, on-orbit servicing assembly and manufacturing, and rendezvous and proximity operations. Collaboratively, the Allies should take actions that enhance Space domain stability and reduce the potential for miscalculations. NATO can promote norms of responsible behaviour in Space favourable to Alliance and key partners’ interests. This collaboration could contribute to enhancing the safety and stability of the Space environment to facilitate peaceful exploration, science, and commercial activities.

### Internal link - NATO Action Key – Spurs Private Sector

#### NATO action spurs private sector innovation and efficiency – this is key to our technological advantage

**Raymond**, Chief of Space Operations @ US Space Force, **2021**

(General John W., “#SpaceWatchGLShare: NATO Space by Gen John W. Raymond,” SpaceWatch.Global, March 2021, https://spacewatch.global/2021/06/spacewatchgl-share-nato-space/, accessed 7/4/2022, gdi-tmur)

Prudent risk-taking is inseparable from the concepts of innovation and agility. Military Space forces must be skilled at managing risk, always seeking mission accomplishment at the speed of relevance while recognizing that perfection is often the enemy of good-enough. Protracted acquisition processes can lengthen decision cycles and dilute the transformative potential of proposed innovations. Leaders must continually seek the proper balance between desired capabilities and fielding schedules, between rigour and efficiency, and between deliberation and action.6 A significant element of Space Force’s organizational transformation is creating both the organizational structures and a Service culture that help leaders at all levels balance these complex concerns while addressing an overall imperative for timely action. Furthermore, to ensure that NATO has the requisite capabilities to be relevant in the future, it is critical to incorporate the innovation experience of the commercial Space sector. The commercial sector – whether satellite operators, launch service providers, or the manufacturing supply base – should play a significant role in NATO’s operations and strategy. Commercial Space activities have expanded significantly in both volume and diversity, resulting in new forms of commercial capabilities and services that leverage commoditized, off-the-shelf technologies, and lower barriers for market entry. Together with civil Space agencies with whom we share a common industrial base, the Alliance can leverage innovation and costeffective investments driven by the private sector, presenting opportunities to develop novel capabilities with a more streamlined and responsive acquisition process. By incorporating the innovation experience of the commercial sector, NATO can implement more effective operations and deterrence strategies, especially as potential adversaries seek to outpace our technological advantage and Space-based capabilities.

### Internal link - Cyber key to effective NATO space capabilities

#### Security of space assets is fundamental to NATO’s capabilities across all domains – cyber security is mission critical

Unal 19 [Beyza, senior research fellow with the International Security Department at Chatham House, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, “Cybersecurity of NATO’s Space-based Strategic Assets,” Chatham House Research Paper, July, <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>, accessed 07/04/22, GDI-JCR]

Strategic space capabilities are generally composed of three elements: a space segment, a ground segment, and a user segment – also known as an uplink, a downlink and a crosslink – that transmit telemetry data.1 Military commanders, staff and senior decision-making cadres within NATO receive mission-significant data through products2 – e.g. space imagery and weather maps – and services3 – e.g. satellite communications and position, navigation and timing (PNT) data – provided by member states with space capabilities. Although emerging technologies such as artificial intelligence (AI) and the Internet of Things (IoT) could be force multipliers for space capabilities,4 increased prevalence of cyber means may also challenge the integrity of data carried through these technologies. Most countries either own satellites or have a stake in space-based assets for meteorological purposes and communications.5 The functioning of all satellites is dependent on cyber technology, including software, hardware and other digital components. Any threats that could impact a satellite’s controls, reliability, or bandwidth availability would pose a direct challenge to national critical assets.6 If cyberthreats are not effectively addressed, vulnerabilities in the strategic infrastructure could result in severe consequences for international security. Cyber vulnerabilities strike at the heart of the key technologies in strategic doctrines and military planning. In the event of crisis escalation, such as in Ukraine, the Middle East or in South Asia, the assumption is that weapons systems will perform as planned. But this should not be taken for granted. It is mission-critical for NATO to manage, preserve and protect space capabilities, inter alia, by means of agreements and policies. Understanding space vulnerabilities and ensuring that mitigation measures and redundancies are in place, will help to protect NATO’s space capabilities. NATO’s missions and operations are conducted in four areas: air, land, cyber and sea.7 Space-based architecture is fundamental to the provision of data and services to all domains. Therefore, any vulnerability in space infrastructure will likely spread to other domains.8 The critical interdependency between space and other domains increases the threat of cyber risks, which disproportionately affect mission assurance. Investing in mitigation measures and in the resilience of space systems are key priorities in protecting all domains.

#### Cyber vulnerability in NATO’s space-based architecture wrecks mission assurance, undermines deterrence, and increases the risk of miscalculation

Unal 19 [Beyza, senior research fellow with the International Security Department at Chatham House, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, “Cybersecurity of NATO’s Space-based Strategic Assets,” Chatham House Research Paper, July, <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>, accessed 07/04/22, GDI-JCR]

All satellites depend on cyber technology including software, hardware and other digital components. Any threat to a satellite’s control system or available bandwidth poses a direct challenge to national critical assets. • NATO’s missions and operations are conducted in the air, land, cyber and maritime domains. Space-based architecture is fundamental to the provision of data and services in each of these contexts. The critical dependency on space has resulted in new cyber risks that disproportionately affect mission assurance. Investing in mitigation measures and in the resilience of space systems for the military is key to achieving protection in all domains. • Almost all modern military engagements rely on space-based assets. During the US-led invasion of Iraq in 2003, 68 per cent of US munitions were guided utilizing space-based means (including laser-, infrared- and satellite-guided munitions); up sharply from 10 per cent in 1990–91, during the first Gulf war. In 2001, 60 per cent of the weapons used by the US in Afghanistan were precision-guided munitions, many of which had the capability to use information provided by space-based assets to correct their own positioning to hit a target. • NATO does not own satellites. It owns and operates a few terrestrial elements, such as satellite communications anchor stations and terminals. It requests access to products and services – such as space weather reports and satellite overflight reports provided via satellite reconnaissance advance notice systems – but does not have direct access to satellites: it is up to individual NATO member states to determine whether they allow access. • Cyber vulnerabilities undermine confidence in the performance of strategic systems. As a result, rising uncertainty in information and analysis continues to impact the credibility of deterrence and strategic stability. Loss of trust in technology also has implications for determining the source of a malicious attack (attribution), strategic calculus in crisis decision-making and may increase the risk of misperception.

#### Space assets key to NATO mission success and deterrence

Cesari et al 21 [Laetitia, Consultant at the UN Institute for Disarmament Studies, “Space as NATO’s Operational Domain: The Case of the Cyber Threats against GNSS,” 72nd International Astronautical Congress (IAC), Dubai, United Arab Emirates, 25-29 October 2021, <https://spacegeneration.org/wp-content/uploads/2022/04/IAC-21E927x66298_Space-as-NATOs-Operational-Domain-The-Case-of-the-Cyberthreats-against-GNSS_Paper.pdf>, accessed 07/04/22, GDI-JCR]

The advances within the space sector creates new opportunities and challenges. It has become an area essential to NATO’s deterrence and defence. “Space provides a number of critical military functions in peace time, as well as in crisis and conflict. NATO is increasingly reliant on space to navigate and track forces, to detect missile launches and to ensure effective command and control. For example, satellite imagery can play a significant role in NATO’s decision-making process” [1]. “Out half of the currently deployed active satellites are owned by NATO Allies - NATO relies on space to navigate and track forces, to have robust communication, to detect missile launch and to ensure effective command and control. each nation responsible for defending its space assets itself” [2]. “NATO’s missions and operations are conducted in the air, land, cyber and maritime domains. Space-based architecture is fundamental to the provision of data and services in each of these contexts. While the Alliance’s reliance on Space-based Data, Products, and Services (DPS) grows, members face a more contested Space domain with new kinetic and non-kinetic threats. The critical dependency on space has resulted in new cyber risks that disproportionately affect mission assurance. Investing in mitigation measures and in the resilience of space systems for the military is key to achieving protection in all domains” [3]. With the multiplication of cyber hostile operations targeting space systems and the increasing reliance on said space systems, the nexus between space and cyber is becoming one of pressing importance for collective security.

### Internal link - - NATO Space Key to Peacekeeping

#### Space assets key to all NATO activities, including peacekeeping and humanitarian assistance

Unal 19 [Beyza, senior research fellow with the International Security Department at Chatham House, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, “Cybersecurity of NATO’s Space-based Strategic Assets,” Chatham House Research Paper, July, <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>, accessed 07/04/22, GDI-JCR]

Space systems, which include both satellites and ground stations, as well as related space products and services, provide mission-critical information both for NATO’s member states and for the alliance as a whole. NATO relies on space-based assets for almost all of its operations and missions.29 Some of the critical missions that rely on space assets include: defence of NATO’s territory and the neighbouring regions; peacekeeping missions; humanitarian assistance and disaster relief; counterterrorism; and conflict prevention activities.

### Internal link - NATO Space Key to UAVs

#### Satellite vulnerability makes UAVs undependable

Unal 19 [Beyza, senior research fellow with the International Security Department at Chatham House, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, “Cybersecurity of NATO’s Space-based Strategic Assets,” Chatham House Research Paper, July, <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>, accessed 07/04/22, GDI-JCR]

Cyber vulnerabilities undermine confidence in strategic systems; they increase uncertainty in information and analysis, which impacts the credibility of deterrence and strategic stability. Loss of trust in technology also has implications for attribution and strategic calculus in crisis decision-making and may increase the risk of misperception. This dependency on space-based technology has major implications for the way NATO conducts warfare today, and how it will do so in the future. For instance, in order to conduct precision strikes or earth observation through the use of unmanned aerial vehicles (UAVs – such as military drones), systems rely on so-called ‘beyond-line-of-sight’ (BLOS) communication via satellites – especially in times of crisis and conflict, since ground-based line-of-sight communications are vulnerable to physical attacks. Yet, cyberattacks on space technology or on the UAVs may lead them to misinterpret commands, or to lose contact with the command centre and fail in operation.

### Internal link - NATO Space Key to Navigation

#### NATO depends on space assets for navigation and timing

Unal 19 [Beyza, senior research fellow with the International Security Department at Chatham House, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, “Cybersecurity of NATO’s Space-based Strategic Assets,” Chatham House Research Paper, July, <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>, accessed 07/04/22, GDI-JCR]

Position, navigation and timing (PNT) PNT is a vital part of any NATO operation. It provides forces with the necessary means to conduct timely and effective operations. Thus, the loss of PNT would leave forces vulnerable to attacks. NATO uses GPS for accurate timing and navigation in its PNT system. The accuracy of this data depends on the satellite geometry and the receiver system. In the tactical domain, alliance troops may not always have – or be able to rely on – space capabilities in conducting their missions. For instance, during a NATO exercise in Finland in 2018, Finland’s civilian air navigation services were disrupted through electronic means, which was later attributed to Russia.38 Loss of navigation capability was also reported in Norway at the same time. While these incidents were not cyberattacks, they illustrate the extent of NATO forces’ dependency on navigational signals, and the vulnerability of navigation systems to interference. In 2002, the EU initiated a European alternative to GPS, named Galileo,39 which is one of four existing Global Navigation Satellite Systems (GNSS). At the core of Galileo lies a European strategic determination to create a stand-alone system that is independent from but compatible with the US’s GPS system, thus providing much-needed resilience for both the US and Europe. At the very beginning of its development, the US claimed that Galileo would be superfluous to the already existing GPS capability and that it would rival the capabilities of the US by creating a reduced European security reliance on that country. Later, this policy was dropped as it became increasingly obvious that Galileo provided a necessary back-up system for GPS – a parallel route for space resilience, and therefore for trans-Atlantic security. There is a need for GPS/Galileo interoperability for NATO military capabilities that are dependent on space-based systems to ensure their reliability and integrity. Galileo has a civilian portion and a public regulated service (PRS), which is an encrypted navigation service, restricted to governments that use it mainly in military applications.40 PRS has anti-jamming and anti-spoofing capabilities, and is reserved for certain users within EU member states. The US needs to negotiate access to the PRS signals. When and if GPS fails to operate, Galileo is designed to provide civilian and military services for the US as well as for Europe. There is no interoperability issue between Galileo and GPS, as these points were discussed and solved in the framework of the EU–US agreement of 2004. The US needs to negotiate access to PRS signals. There is no agreement yet for Galileo to replace GPS in case of the latter’s failure.

### Internal link - NATO Space Key to Intelligence

#### NATO depends on space surveillance and reconnaissance – any loss would be dire

Unal 19 [Beyza, senior research fellow with the International Security Department at Chatham House, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, “Cybersecurity of NATO’s Space-based Strategic Assets,” Chatham House Research Paper, July, <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>, accessed 07/04/22, GDI-JCR]

Intelligence, surveillance and reconnaissance (ISR)41 ISR provides information and imagery intelligence to allied forces about specific targets. It is used in air, land and maritime domains in order to supply accurate and timely information to the relevant commander to support decision-making.42 NATO’s intelligence-led operations rely fundamentally upon space-based ISR capabilities, and the effectiveness of the alliance’s operations is based upon the availability of these systems. The imagery that ISR provides can be used both in conventional and nuclear weaponry command and control, and in targeting. ISR capability is composed of airborne imagery platforms, space-based assets and ground sensors. The information is collected through surveillance and reconnaissance sensors, which may be vulnerable to cyberattacks. Sensors could also be manipulated through physical or cyber means: this could even occur at the design stage within the manufacturing organization – a weakness all NATO countries should be aware of, especially if they rely on equipment sourced from non-NATO parties for the components of intelligence-gathering technologies. NATO is working to improve the interoperability of ISR capabilities. To this end, in 2011, nine NATO countries voluntarily joined the Multi-intelligence All-source Joint Intelligence Surveillance and Reconnaissance Coalition (MAJIIC-2) initiative, with the aim of increasing interoperability and information-sharing between each nation’s ISR capabilities.43 ISR technologies contribute significantly to national, regional and international security. Through surveillance systems, such technologies can observe and map adversary command, control and communication systems, thus providing invaluable strategic insights. Yet – as stated by a former battalion intelligence officer – collecting all the necessary information from multiple sources in a timely manner is not an easy task.44 That information may be received at different times from different outlets. Technology is an important factor in facilitating this analysis, and AI can overcome many existent analytical difficulties and analyse data in a compressed time frame. Any loss of ISR capability through cyberattacks would have dire consequences for strategic planning and policy.

### Internal link - - NATO Space Key to Missile Defense

#### Space assets key to NATO missile defense

Unal 19 [Beyza, senior research fellow with the International Security Department at Chatham House, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, “Cybersecurity of NATO’s Space-based Strategic Assets,” Chatham House Research Paper, July, <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>, accessed 07/04/22, GDI-JCR]

Missile defence relies heavily on early warning capabilities otherwise known as integrated threat warning and threat assessment (ITW/TA): US space-based infrared sensors detect the hot plumes of ballistic missile launches and communicate the information to the service component command. Theatre missile defence, which includes the Patriot missile defence system – a long-range surface-to-air missile system used by the US and NATO allies – and standard missile defence systems, and which is part of the naval component of the integrated Aegis weapon system, also serves as part of overall missile defence capability.45 The Aegis combat system operates in the maritime domain, using radar to track and guide weapons to destroy targets; its elements – which include a space tracking and surveillance system, the AN/SPY-1A radar, a command and decision system and a display system – could all potentially be exposed to cyberattacks. The US Department of Defense conducted an auditing exercise in 2018 for the internal controls of its ballistic missile defence systems (BMDS). The aim of the audit was to ensure that systems and programmes were functioning as intended. The findings indicated that there were ‘internal control weaknesses related to protecting networks and systems that process, store, and transmit BMDS technical information’.46 These weaknesses could be exploited through insider threat and/or cyber means. Missile defence systems may fail, or they may be activated due to false information sent from communication systems (such as ground-based radars) to the command unit. The Israeli anti-missile defence system Iron Dome, for example, is claimed to have a 90 per cent accuracy rate when intercepting targets. Yet there have been cases where a faulty response within the system has activated the launch of interceptor missiles erroneously, such as occurred in Gaza in March 2018, when it was triggered by machine gun fire.47 Thus the battle management and weapons control system was proved at that time to be unable to make proper threat assessments. Similar outcomes could result if the threat assessment control system is interfered with via cyber means; the consequences could be much higher, including the loss of civilian life. In the Israeli case, it was reported that Rafael Advanced Defense Systems, a supplier of technology to the Iron Dome system, together with Israel Aerospace Industries and the Elisra Group, both of which were also involved in the project, faced persistent cyberattacks during the period of October 2011 to August 2012. This resulted in the loss of sensitive data that was believed to include the specifications of the Arrow 3 missile, developed jointly by the US and Israel.48 Vulnerability to cyberattacks within the supply chain is not unique to NATO, and NATO and its allies should address this type of risk. Supply chain integrity (in terms of both hardware and software) is imperative for reliable military systems. One of the core elements of a missile defence system is that it relies on the reception of near real-time information by a command centre to be able to identify and project the trajectory of an incoming missile. Through automated response it calculates the speed, velocity and location of the target in order to be able to intercept the incoming missile in a short time frame. Any deliberate interference with the information, for instance from the radar, could mean that the defence missiles fail to intercept an incoming threat, or could lead to a faulty decision based on falsified or spoofed information. Thus, for example, a defence missile could fail to hit the correct target and strike well beyond the intended target zone. In order to detect deliberate interference or cyber intrusion, it is important to put preventive measures in place. One such measure could be to conduct organized, simulated cyberattacks on a system to assess its performance: this is known as penetration testing. In the future, detection of anomalies could be possible through ML and AI, especially in closed networks.49

### Internal link - NATO Space Key to Environmental Monitoring

#### Key to environmental monitoring

Unal 19 [Beyza, senior research fellow with the International Security Department at Chatham House, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, “Cybersecurity of NATO’s Space-based Strategic Assets,” Chatham House Research Paper, July, <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>, accessed 07/04/22, GDI-JCR]

An area often neglected in discussions of space-dependent capabilities is the environmental monitoring of Earth: this process provides weather forecasting, geospatial and oceanographic information. Environmental monitoring is equally important during peacetime and during conflict. This capability supports mission planning, flight trajectories and targeting. For instance, in the context of NATO operations, environmental monitoring could supply information on flooding trends in a specific region, which a commander could access, allowing the latter to plan a mission accordingly. Weather information is also crucial to air defence planning and to the deployment of security against the use of chemical, biological, radiological and nuclear (CBRN) agents. Real-time weather data is vital for missile launches and accurate targeting. NATO does not itself supply data or equipment for the provision of weather-related information. Instead, information about environmental conditions – and their potential impact on SATCOM and sensor accuracy – is provided to NATO by the US, through the meteorological and oceanographic (METOC) community.55

### Impact – Nuclear Escalation

#### Satellite disruption poses a unique risk for nuclear escalation – entanglement of nuclear and nonnuclear systems means conventional conflict provokes nuclear response

Acton 18 [James, Jessica T. Mathews Chair and co-director of the Nuclear Policy Program at the Carnegie Endowment for International Peace, “Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War,” *International Security*, <https://www.mitpressjournals.org/doi/full/10.1162/isec_a_00320>, accessed 8/20/19, JCR]

In issuing this threat, the Nuclear Posture Review illustrates that nonnuclear attacks on nuclear forces and C3I capabilities could be highly escalatory, even to the point of directly sparking a nuclear war. A key challenge in managing these escalation risks is that attacks on an opponent's nuclear forces or their C3I capabilities (whether they belong to the United States or another state) might not be deliberate. Since the late 2000s, scholars have warned about the possibility of escalation in a U.S.-China conflict resulting from so-called crisis instability generated by actual or threatened U.S. nonnuclear operations that were intended to suppress China's conventional forces but inadvertently degraded its nuclear forces or associated C3I assets located in the theater of operations, thus leading Beijing to fear it was being disarmed.3 Similar, if more infrequent, scholarly warnings have been voiced about a U.S.-Russia conflict.4 Such escalation would be inadvertent because it was the result of military operations or threats that were not intended to be escalatory.5 This article's thesis is that the risks of inadvertent escalation are even more serious than these warnings suggest and are likely to increase significantly in the future. Driving these risks is the possibility that Chinese, Russian, or U.S. C3I assets located outside—potentially far outside—theaters of operation could be attacked over the course of a conventional conflict. These assets include satellites used for early warning, communication, and intelligence, surveillance, and reconnaissance (ISR); ground-based radars and transmitters; and communication aircraft.6 Such assets constitute key nodes in states' nuclear C3I systems, but they are also “entangled” with nonnuclear weapons in two ways.7 First, they are typically dual use; that is, they enable both nuclear and nonnuclear operations. Second, they are increasingly vulnerable to nonnuclear attack—much more vulnerable, in fact, than most nuclear-weapon delivery systems. Entanglement could lead to escalation because both sides in a U.S.-Chinese or U.S.-Russian conflict could have strong incentives to attack the adversary's dual-use C3I capabilities to undermine its nonnuclear operations.8 As a result, over the course of a conventional war, the nuclear C3I systems of one or both of the belligerents could become severely degraded. It is, therefore, not just U.S. nonnuclear strikes against China or Russia that could prove escalatory; Chinese or Russian strikes against American C3I assets could also—a possibility that scholars have scarcely even considered since the end of the Cold War.9 Two escalation mechanisms that have not been previously discussed in the academic literature are largely responsible for the increasing risk. First, the target might interpret nonnuclear attacks against its dual-use C3I assets that were motivated by conventional warfighting goals as preparations for nuclear use. It might respond to such “misinterpreted warning,” to coin a term, by trying to deter the nuclear strike it believed might be coming or to mitigate its potentially calamitous consequences. Such efforts, which might include provocative nonnuclear operations to protect remaining C3I assets (such as strikes against anti-satellite weapons deep within the adversary's territory) accompanied, perhaps, by nuclear threats, could prove highly escalatory. These escalation pressures could arise even if the recipient of misinterpreted warning were not concerned about the survivability of its nuclear forces—a key distinction from crisis instability. Second, a state with a damage-limitation doctrine would rely on sophisticated C3I capabilities to locate and destroy its opponent's nuclear forces and conduct missile defense operations. If these dual-use enabling capabilities were subject to attack in a conventional conflict—or even if their possessor feared they might be—the state could worry that its window of opportunity for conducting effective damage-limitation operations might have closed by the time the war turned nuclear. In this case, the state might take escalatory measures to protect its C3I system or even initiate counterforce operations preemptively. This escalation mechanism, which might be termed the “damage-limitation window,” is distinct from crisis instability because it is driven by the state's desire to hold an opponent's nuclear forces at risk, not to protect its own. It is distinct from misinterpreted warning because it could operate even if the state did not believe that nuclear use by an adversary might be imminent; the state would only have to believe that such escalation was possible later on. An additional implication of C3I entanglement is that the risks of crisis instability are more serious than portrayed in the academic literature. Scholarly warnings about crisis instability have focused on the potential for U.S. nonnuclear operations to degrade Chinese nuclear forces, but have also identified the risk of inadvertent threats to China's nuclear C3I capabilities located in the theater of operations.10 These threats have received particular attention since the United States acknowledged, in 2013, that it seeks to defeat potential adversaries' antiaccess/area-denial capabilities by holding relevant C3I assets at risk as part of the concept formerly known as AirSea Battle (which was renamed, in 2015, as the Joint Concept for Access and Maneuver in the Global Commons and has since been further developed).11 If overlap exists between the communication systems for China's land-based nuclear and nonnuclear missiles, as some analysts have suggested, China could mistake U.S. strikes designed to disable its nonnuclear missiles as an attack against its nuclear forces.12 Entanglement, however, has created other potential triggers for crisis instability. The United States, for example, has—or could develop—incentives to launch nonnuclear kinetic attacks against existing and probable future dual-use Chinese or Russian early-warning capabilities, including over-the-horizon radars, ballistic missile early-warning radars (BMEWRs), and early-warning satellites, that are located outside the theater of operations.13 (Kinetic weapons, which often use explosive warheads, aim to damage or destroy targets by transferring kinetic energy to them through physical contact; non-kinetic weapons include directed energy and cyber capabilities.) Moreover, Russian strikes on the United States could precipitate crisis instability if U.S. communication aircraft (currently, the United States' most survivable means to communicate with its nuclear forces) become vulnerable. Entanglement could catalyze escalation in any major U.S.-Chinese or U.S.-Russian conventional conflict, irrespective of its origins. That said, for the sake of concreteness, the kind of U.S.-Chinese conflict that forms the backdrop to this article would most likely begin with a Chinese attempt to reunify with Taiwan by force (either unprovoked or because the government of Taiwan had declared independence), followed by U.S. intervention on behalf of Taiwan. The most probable cause of a major U.S.-Russian conflict would be the invasion and occupation of one or more of the Baltic states by Russia, followed by a U.S.-led counterattack to liberate them. In both cases, fighting could spread from the theater in which it started. There would, of course, be important differences between the escalation dynamics in a U.S.-Chinese and U.S.-Russian conflict. Nevertheless, there would also be important similarities that help illustrate the general nature of the risks stemming from entanglement. In particular, entanglement could not only precipitate the use of nuclear weapons directly, but could also frustrate efforts to manage nonnuclear escalation, thus raising the risk of nuclear use later on. Early in a conflict, for example, to emphasize its limited war aims, the United States might refrain from conducting nonnuclear strikes beyond a certain distance into an adversary's territory. Subsequently, if the United States became worried that key C3I satellites were at risk, it might believe that it had to attack Chinese or Russian anti-satellite (ASAT) weapons located further beyond the border.

### Impact – Russia

#### Risk of cyber escalation with Russia is massive and goes nuclear – prioritize this impact because cognitive bias underestimates it, and deterrence can’t solve it.

Beebe 19 [George, VP and Director of Studies at the Center for the National Interest, a nonpartisan think tank, former head of Russia analysis at the CIA, “We’re More at Risk of Nuclear War With Russia Than We Think,” October 7, *Politico*, <https://www.politico.com/magazine/story/2019/10/07/were-more-at-risk-of-nuclear-war-with-russia-than-we-think-229436>, accessed 07/04/22, GDI-JCR]

Today, that old dread of disaster has all but disappeared, as have the systems that helped preclude it. But the actual threat of nuclear catastrophe is much greater than we realize. Diplomacy and a desire for global peace have given way to complacency and a false sense of security that nuclear escalation is outside the realm of possibility. That leaves us unprepared for—and highly vulnerable to—a nuclear attack from Russia. The most recent sign of American complacency was the death, a few weeks ago, of the Intermediate-Range Nuclear Forces Treaty—a pivotal 1987 agreement that introduced intrusive on-site inspection provisions, destroyed an entire class of dangerous weaponry, and convinced both Washington and Moscow that the other wanted strategic stability more than strategic advantage. The New START treaty, put in place during the Obama administration, appears headed for a similar fate in 2021. In fact, nearly all the key U.S.-Russian arms control and confidence-building provisions of the Cold War era are dead or on life support, with little effort underway to update or replace them. Meanwhile, U.S. officials from both parties are focused not on how we might avoid nuclear catastrophe but on showing how tough they can look against a revanchist Russia and its leader, Vladimir Putin. Summit meetings between White House and Kremlin leaders, once viewed as opportunities for peace, are now seen as dangerous temptations to indulge in Munich-style appeasement, the cardinal sin of statecraft. American policymakers worry more about “going wobbly,” as Margaret Thatcher once put it, than about a march of folly into inadvertent war. President Donald Trump’s suggestion that the United States and Russia might explore ways to manage their differences diplomatically has produced mostly head-scratching and condemnation. In my more than 25 years of government experience working on Russia matters, I’ve seen that three misguided assumptions underlie how the United States got to this point. The first is that American policymakers think that because neither side wants nuclear war, then such a war is very unlikely to occur. Russia would be foolish, we reason, to cross swords with the powerful U.S. military and risk its own self-destruction, and many Americans find it hard to imagine that modern cyber duels, proxy battles, information operations and economic warfare might somehow erupt into direct nuclear attacks. If the Cold War ended peacefully, the thinking goes, why should America worry that a new shadow war with a much less formidable Russia will end any differently? But wars do not always begin by design. Just as they did in 1914, a vicious circle of clashing geopolitical ambitions, distorted perceptions of each other’s intent, new and poorly understood technologies, and disappearing rules of the game could combine to produce a disaster that neither side wants nor expects. In fact, cyber technologies, artificial intelligence, advanced hypersonic weapons delivery systems and antisatellite weaponry are making the U.S.-Russian shadow war much more complex and dangerous than the old Cold War competition. They are blurring traditional lines between espionage and warfare, entangling nuclear and conventional weaponry, and erasing old distinctions between offensive and defensive operations. Whereas the development of nuclear weaponry in the Cold War produced the concept of mutually assured destruction and had a restraining effect, in the cyber arena, playing offense is increasingly seen as the best defense. And in a highly connected world in which financial networks, commercial operations, media platforms, and nuclear command and control systems are all linked in some way, escalation from the cyber world into the physical domain is a serious danger. Cyber technology is also magnifying fears of our adversaries’ strategic intentions while prompting questions about whether warning systems can detect incoming attacks and whether weapons will fire when buttons are pushed. This makes containing a crisis that might arise between U.S. and Russian forces over Ukraine, Iran or anything else much more difficult. It is not hard to imagine a crisis scenario in which Russia cyber operators gain access to a satellite system that controls both U.S. conventional and nuclear weapons systems, leaving the American side uncertain about whether the intrusion is meant to gather information about U.S. war preparations or to disable our ability to conduct nuclear strikes. This could cause the U.S. president to wonder whether he faces an urgent “use it or lose it” nuclear launch decision. It doesn’t help that the lines of communication between the United States and Russia necessary for managing such situations are all but severed.

#### Russia prioritizing cyber capabilities to counter space assets

DIA 22 [Defense Intelligence Agency is an external intelligence service of the Department of Defense and the United States Intelligence Community, it produces approximately one fourth of the intelligence content that goes into the President’s Daily Brief, “Challenges to Security in Space,” https://www.dia.mil/Portals/110/Documents/News/Military\_Power\_Publications/Challenges\_Security\_Space\_2022.pdf, accessed 07/05/22, GDI-JCR]

Cyberthreats. Since at least 2010, the Russian military has placed a priority on the development of forces and capabilities, including cyberspace operations, for what terms “information confrontation”—a holistic concept for ensuring information superiority. The weaponization of information is a critical aspect of this strategy and is employed in times of peace, crisis, and war. Russia considers the information sphere, especially space-enabled information collection and transmission, to be strategically decisive and has taken steps to modernize its military’s information attack and defense organizations and capabilities.453

#### Cyber ASAT attacks escalate to conventional war

**Tepper**, research coordinator and lecturer for space governance at Laval University, **2022**

(Eytan, “The First Space-Cyber War and the Need for New Regimes and Policies,” Center for International Governance Innovation, Policy Brief No. 173, May 2022, https://practicesource.com/wp-content/uploads/2022/05/apo-nid317939.pdf, accessed 7/4/2022, gdi-tmur)

Many dubbed the Gulf War of 1991 the “first space war” due to the US Armed Forces’ extensive use of satellites (Anson Bt and Cummings 2008). The current war in Ukraine might be remembered as the first space-cyber war. It is demonstrating the potential and temptation of targeting space assets during an armed conflict. The cyberwar in Ukraine is mostly secret, playing out in the shadows, as inconspicuous as it is insidious. However, we already know that on the day of the Russian invasion of Ukraine, Viasat, a US-based provider of high-speed satellite broadband services, suffered an outage, which disrupted the internet services it provides to the Ukrainian armed forces, intelligence service and police (Rid 2022). In addition, Russia allegedly jammed GPS signals locally in Ukraine, disabling the ability of Ukrainians to determine their location or navigate and guide weapons to their targets (Hitchens 2022). Moreover, Dmitry Rogozin, the head of the Russian space agency Roscosmos, said that Russia will treat any hacking of its satellites as a casus beli (Reuters 2022) — justification for war. This provides a stark demonstration of the explosive potential of the space-cyber nexus: launching a cyberattack on space assets can trigger a response in the form of conventional warfare. This Russian statement may become a new customary norm, as it builds on previous statements and actions regarding cyberattacks in general. In 2011, the United States released its “International Strategy for Cyberspace,” which declared it would “respond to hostile acts in cyberspace as it would to any other threat to our country” (The White House 2011, 14). Israel was the first country to take this type of action: in 2019, it attacked a building in Gaza from which Hamas hackers allegedly launched or tried to launch cyberattacks against Israeli targets (Israel Defense Forces 2019).

#### Russia will use cyber – not physical – ASATs

**Tepper**, research coordinator and lecturer for space governance at Laval University, **2022**

(Eytan, “The First Space-Cyber War and the Need for New Regimes and Policies,” Center for International Governance Innovation, Policy Brief No. 173, May 2022, https://practicesource.com/wp-content/uploads/2022/05/apo-nid317939.pdf, accessed 7/4/2022, gdi-tmur)

Commercial space companies have also become embroiled in the war in Ukraine. After Google Maps marked the traffic jam that was the invading Russian army, it turned off live traffic updates in Ukraine that might be used to target troops or refugees (Meaker 2022). Satellite imagery from commercial companies is used to shed light on the unfolding events and situation on the ground, including destruction of targets, as exemplified by Maxar Technologies’ satellite images of the 40-mile Russian military convoy en route to Kyiv (Sky News 2022). Moreover, commercial companies’ satellite imagery is also used by the Ukrainian army. MDA, a Canadian commercial space company, provides the Ukrainian government with satellite imagery, which the Ukrainian military uses to pinpoint Russian troops (Wark 2022). SpaceX’s Starlink announced the provision of space-based internet service in Ukraine (Jin 2022), amid problems faced by traditional suppliers, and, after having its satellite signal jammed (Swinhoe 2022), declared a new focus on cyber defense (Malik 2022). What this war did not yet see, and is less likely to see, is the physical destruction of satellites, although Russia has such capabilities, as revealed again by its anti-satellite test in November 2021 (Gohd 2021), as do the United States, China and India. Indeed, the Ukraine war demonstrates that cyberattacks are the main contra-space mode of warfare.

### Impact – China

#### Statements by the PLA and key military experts prove China will prioritize counterspace tactics in the event of conflict with the US

Cheng 18 [Dean, Senior Research Fellow for Chinese Political and Military Affairs at the Heritage Foundation, formerly with the Chinese Studies Division at the Center for Naval Analysis, a federally funded research and development center, analyst with the US Congress Office of Technology Assessment in the International Security and Space Division, “Space and Information Warfare: A Key Battleground for Information Dominance,” *Outer Space; Earthly Escalation? Chinese Perspectives on Space Operations and Escalation*, ed. Nicholas Wright, <https://apps.dtic.mil/dtic/tr/fulltext/u2/1066706.pdf>, accessed 07/04/22, JCR]

Throughout the 1990s, even as the Chinese view of future warfare and the role of information was evolving, the PLA was also developing its views on space warfare. Assessing other peoples’ wars, the Chinese concluded that future wars would include space warfare as an integral part of operations. This was not so much because of the importance of space systems—due to their growing role in providing the information support necessary for the successful conduct of future local wars—but more because of their performance and requirement under modern, high-technology conditions or informationized conditions. Indeed, PLA assessments of American and Russian military operations, beginning with the use of space in the first Gulf War, concluded that space-based information played an outsize role. Therefore, in the event of a conflict, the PRC must strive to deny an adversary the ability to use space freely. In particular, the PRC’s shift towards joint operations, which began in the 1990s, highlighted the importance of space. As envisioned by the PLA, joint operations would involve multiple services operating together across significant distances. The Gulf War, for example, sprawled across some 140 million square kilometers, and included forces ranging from armored units to aircraft carriers and long-range bombers (Wang & Zhang, 2000, p. 400). The ability to coordinate such diverse forces spread across a variety of domains would therefore require not only extensive communications, but also precise navigation and positioning information, both for units and for the growing plethora of precision munitions. Joint operations were therefore seen as requiring the ability to command and control operations across not only the traditional domains of land, sea, and air, but increasingly outer space. In this light, space capabilities were recognized as playing an essential role in any effort to wage a “local war under modern, high-tech conditions.” According to PLA estimates, the 70 satellites that were ultimately brought to bear against Iraq provided the US with 90% of its strategic intelligence, and carried 70% of all transmitted data for Coalition forces (Gao, 2001, p. 54). Indeed, these assets were the first to be employed, since they were essential for the success of all subsequent campaign activities. As one Chinese analyst observed, “Before the troops and horses move, the satellites are already moving” (Gao, 2005). PRC writings from the mid-1990s through the early 2000s reflect a steady evolution from seeing space as important to seeing it as decisive (See PLA Encyclopedia Committee, 1997, 2002). Given the importance of such support from space systems, victory in future “local wars under modern, high-technology conditions” was already recognized as requiring not only one’s own unfettered access to space, but also the denial of the same ability to the adversary. By preventing the enemy from obtaining the amount of information they required, it would be far more difficult for them to coordinate their forces and operations. As important, by preventing them from operating in the manner to which they were accustomed (and had trained), they would be far less efficient and flexible, and therefore more vulnerable to Chinese actions. In effect, by degrading adversary space capabilities, the enemy would suffer from a slower OODA (observe-orient-decide-act) loop. Space information support was therefore increasingly seen as complemented by offensive space operations (which somewhat aligns with Western concepts of counter-space operations). This shift may also have been a reflection of the ongoing development of Chinese concepts of future warfare. As part of the PLA’s “new historic missions,” Hu Jintao in 2004 made clear that the PLA must secure China’s interests in outer space, as well as the electromagnetic spectrum (2004). The incorporation ofthe space domain into the specific range of PLA responsibilities reflected the steadily growing emphasis placed upon establishing space dominance, as part of the larger effort to secure information dominance. Indeed, as the PLA shifted from preparing to fight “local wars under modern, high-technology conditions” to fighting “local wars under informationized conditions,” space was increasingly seen as part of those “informationized conditions.” As PLA writings note, “informationized conditions” did not simply refer to computers and cyberwarfare. Instead, it involves the acquisition, transmission, and exploitation of all forms of information. Space plays a central role in all these tasks. In the 2006 edition of The Science of Campaigns, it is specifically stated that “the space domain daily is becoming a vital battle-space…. Space has already become the new strategic high ground” (Zhang, 2006, p. 87). Similarly, in the 2013 edition of The Science of Military Strategy, space is deemed the “high ground in wars under informationized conditions,” tied to the struggles in networks space and the electromagnetic spectrum as key future battlegrounds (Academy of Military Science Military Strategy Research Office, 2013, p. 146-147).In the Chinese conception, space is important for the advantage it confers with regards to the ability to collect, transmit, and exploit information, rather than for its own sake. As other Chinese analysts conclude, “space operations will be a core means of establishing information advantage” (Yuan, 2008, p. 324). Chinese military planners are therefore preparing to undertake a range of space actions, should that be necessary. That readiness is facilitated by the reality that the PLA runs China’s space facilities.12 These include a range of anti-satellite tests in 2007, 2010, and 2013. This last test is especially notable, as it is assessed as demonstrating an ability to threaten targets as far as the geosynchronous belt, over 26,000 miles away (Weeden, 2014). This is the first time that any nation has tested a weapon explicitly intended to hold satellites in that orbit at risk. The ability to hold at risk the entire range of orbital regimes is tied to the Chinese emphasis on establishing “information dominance” in order to win future conflicts. Chinese analysts have long recognized, since at least the first Gulf War twenty-five years ago, that space is a key means of providing information support to terrestrial forces. Consequently, the emphasis upon establishing space dominance, as part of the struggle for information dominance, has become more explicit. Chinese authors believe that without space dominance, one cannot obtain information dominance and aerial dominance, and therefore one cannot achieve land or maritime dominance. Space will therefore inevitably be a battleground, if only in order to deny an adversary the ability to use it freely (Ye, 2007, p. 154). Consequently, the space arena will be one of the very first scenes of conflict, as the two sides struggle for control of space. Neither side can afford to neglect this theater, as it will be a central determinant of who will secure information dominance (Chi & Xiao, 2005, p. 38-39). Space dominance entails not only the ability to provide information support to the PLA, but also to deny an adversary the ability to exploit space to gain information. The American reliance on space systems, in particular, has been remarked upon in various Chinese military writings. Nor is American dependence upon space unique, in the Chinese view. PLA writings indicate that they are also closely observing other nations’ space developments. Russian space developments in particular seem to garner heavy Chinese attention. The Chinese military textbook Military Astronautics discusses Russian as well as American aerospace forces (Chang, 2005, p. 219-220). The 2013 edition of The Science of Military Strategy observes that Russia has made space a major focus of its military refurbishment effort, and that Moscow has increased its investments in the space sector as the Russian economy has improved (Academy of Military Science Military StrategyResearch Office, 2013, p. 180).

#### China emphasizes offensive cyberspace capabilities in military strategy against space-based assets

DIA 22 [Defense Intelligence Agency is an external intelligence service of the Department of Defense and the United States Intelligence Community, it produces approximately one fourth of the intelligence content that goes into the President’s Daily Brief, “Challenges to Security in Space,” https://www.dia.mil/Portals/110/Documents/News/Military\_Power\_Publications/Challenges\_Security\_Space\_2022.pdf, accessed 07/05/22, GDI-JCR]

Cyberthreats. The PLA emphasizes offensive cyberspace capabilities as a major component of integrated warfare and could use its cyberwarfare capabilities to support military operations against spacebased assets.239,240 For example, the PLA could employ its cyberattack elements to establish information dominance in the early stages of a conflict to constrain an adversary’s actions or slow its mobilization and deployment by targeting network-based command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR); logistics; and commercial activities. The PLA also conducts cyberespionage against foreign space entities, consistent with broader state-sponsored industrial and technical espionage, to increase its level of technologies and expertise available to support military research, development, and acquisition. The PLA unit responsible for conducting signals intelligence has supported cyberespionage against U.S. and European satellite and aerospace industries since at least 2007.241,242

#### China will first strike our satellite systems with cyber attacks at the start of conflict

Lewis 18 [Bruce, Senior Vice President and Program Director at CSIS, formerly worked at the Departments of State and Commerce as a Foreign Service Officer, “‘Bottom Line Thinking’ about the ‘Commanding Heights’,” *Outer Space; Earthly Escalation? Chinese Perspectives on Space Operations and Escalation*, ed. Nicholas Wright, <https://apps.dtic.mil/dtic/tr/fulltext/u2/1066706.pdf>, accessed 07/05/22, JCR]

China’s concepts of future warfare calls for operational and tactical offense in the context of strategic defense. Should China decide to engage in armed conflict, it will attempt to use a combination of strike weapons, submarines, anti-satellite, and cyber-attacks to quickly overwhelm opponent forces in the theater of operations. China’s military prefers to strike first—preemptively and without warning. The ambiguity and reinterpretation of China’s “No First Use” policy reflects this. If the intent is to overwhelm an opponent rapidly, then piecemeal deployment and gradual escalation undercut the chances for success. In the event of conflict, early attacks on American space assets would be central to China’s rapid escalation. China (like our other opponents), believes the US military is dependent on space services and China has developed means to damage or cripple reconnaissance, communications, and navigation using both kinetic and non-kinetic attacks. Having crossed the use-of-force threshold, the next escalatory threshold will be whether to attempt to geographically limit conflict or to strike the American homeland, actions that may produce retaliatory risk that is disproportionate any military benefit such attacks may provide. Chinese strategists are concerned with “war termination,” e.g. ending armed conflict in ways that advance China’s interests, but finding a way to terminate a war with the US on favorable terms may present them with unsolvable problems. While the opening phase conflict might see China gain swift local advantage, this would be attractive only if China assumes that any American response will be limited and of short duration, and this assumption makes sense only if there was a collapse of US political resolve. A short, sharp, regional conflict could follow China’s timetable for successful conflict termination, but it is a bold assumption that the US would not continue any conflict until it had inflicted significant losses on Chinese forces and regained military advantage. While “gray zone’ efforts by China can circumvent America military power, open conflict would bring this power into play in ways that would put Chinese naval, air and space assets at considerable (and at least for now, unacceptable) risk. Chinese space activities to date have been demonstrations of prowess and national strength while developing operational capabilities, including anti-space capabilities targeted at the United States. China will continue to develop anti-satellite capabilities (and other advanced military capabilities) to narrow the scope for US action and to decrease the likelihood ofUS success if conflict arises. However coercion in space has been difficult to manage and the use of force in space will occur only when China has decided upon armed conflict, something it will for now try to avoid. Space (and cyberspace) challenge efforts at controlling escalatory risk through geographic limitations to conflict. Chinese writings refer to space as the “commanding heights in strategic competition,”11 one of the new technologies that (along with cyber) have expanded the domain for conflict. Space occupies an anomalous position, with American space assets providing tempting and vulnerable targets whose destruction would provide real operational advantage, but that also bring the risk of making any conflict “strategic” rather than the limited war China would prefer. An attack on an American space asset orbiting over China, producing no casualties or dramatic photos, may seem ideal as a demonstration of nationalist resolve. A demonstration of the ability to inflict harm in space without damaging a satellite may be even more attractive as a warning to potential opponents about the danger of conflict with China. However, the experience of the 2007 anti-satellite test, which was badly coordinated within the Chinese government, provoked an unexpectedly hostile global reaction, and led to a US counter-demonstration, show the limits of coercion in space.

#### The US would interpret Chinese ASAT use as preparation for nuclear strikes

Acton 18 [James, Jessica T. Mathews Chair and co-director of the Nuclear Policy Program at the Carnegie Endowment for International Peace, “Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War,” *International Security*, <https://www.mitpressjournals.org/doi/full/10.1162/isec_a_00320>, accessed 07/05/22, JCR]

That said, the United States could still interpret Chinese attacks against its early-warning system as preparations for limited nuclear strikes intended to terrify the United States into terminating a conflict on terms not too unfavorable to Beijing. Fairly or not, Washington does not have complete confidence in the reliability of China's no-first-use pledge.51 In particular, skeptics typically argue that Beijing would be most likely to abandon this pledge if China were in danger of losing a war over Taiwan—an outcome that could jeopardize the continued rule of the Chinese Communist Party.52 If, in this circumstance, China attacked critical U.S. early-warning assets—satellites, in particular—in an effort to help its conventional ballistic missiles penetrate U.S. defenses, Washington might conclude that desperate Chinese leaders were preparing limited nuclear strikes, against either the United States or regional targets.53 Again, much would depend on context. The likelihood of misinterpreted warning would probably increase if, in addition to attacking dual-use U.S. enabling capabilities, China had dispersed or alerted nuclear-armed missiles. Although this step could be a standard defensive precaution to protect the missiles' survivability in a major conflict, it might also exacerbate concerns in Washington about the possibility of Chinese first use. Some nuclear-armed medium-range DF-21A ballistic missiles appear to be targeting U.S. assets in the West Pacific.54 The alerting of these missiles could be seen by the United States, therefore, as preparations for regional nuclear strikes. The alerting of China's ICBM force, meanwhile, could be interpreted as an attempt to threaten the U.S. homeland and so deter nuclear retaliation to Chinese first use against regional targets. The escalation pressures might be more serious still if China had conducted extensive attacks against U.S. ISR assets, denying the United States contextual information that might be helpful in interpreting Chinese intentions correctly.

### Impact – GNSS

#### Attack on the Global Navigation Satellite System ripples across sectors, sparks panic

Cesari et al 21 [Laetitia, Consultant at the UN Institute for Disarmament Studies, “Space as NATO’s Operational Domain: The Case of the Cyber Threats against GNSS,” 72nd International Astronautical Congress (IAC), Dubai, United Arab Emirates, 25-29 October 2021, <https://spacegeneration.org/wp-content/uploads/2022/04/IAC-21E927x66298_Space-as-NATOs-Operational-Domain-The-Case-of-the-Cyberthreats-against-GNSS_Paper.pdf>, accessed 07/04/22, GDI-JCR]

The Global Positioning System was originally designed as a military system, to meet tactical and strategic needs on the battlefield, during the Cold War Era. The term traditionally refers to the North American global positioning system, or satellite positioning system, while GNSS refers to the International Multi-Constellation Satellite System. Therefore, GNSS as an umbrella term typically includes GPS, GLONASS, Baidu, Galileo, and any other constellation system. GNSS and GPS work together, however the GNSScompatible equipment can use navigational satellites from other networks beyond the GPS system, which is the main difference from GPS, and more satellites means increased receiver accuracy and reliability. The GNSS can be targeted by cyberattacks via the command connection or ground station, since an unencrypted command link can expose the satellite's capabilities to an opponent, or a ground station could be hacked directly, allowing the ground station to influence satellite control or data. The ITU, while recognizing that “Member States retain their entire freedom with regard to military radio installations” [44] these installations must, so far as possible, take measures to prevent harmful interference [45]. Therefore, when assessing the interference risks associated with conflict zones or planning military exercises, ITU invites Member States to consider that the use of satellite-based systems can potentially be impacted beyond that zone, and therefore, an enhanced civilmilitary coordination is required. NATO’s ballistic missile defence capability is being built around a command-and-control system that enables five key functions: planning, monitoring, informationsharing, interception and consequence management 12 . The security of the system relies on three key elements, confidentiality, integrity and availability. industrial security is paramount (inc also supply chains)” [2]. The consequences of cyber-attacks on space missions are aggravated because of component satellites’ augmented connectivity and use of Internet of Things (IoT) devices in contemporary space systems. The potential impacts of an attack on a communication satellite can endanger national security by generating widespread disruptions to communication channels, not only national level, but also across widespread geographies, cross countries, and cause panic. The attacker can infiltrate the network without being detected and remain undetected. Cyber threats may target different components of a space mission: the ground segment, the space segment, and the link segment. The vulnerabilities stem from the ground segments; mostly generated from network components and the receivers (which receive the data from the satellite). The threats may also target hardware of satellites in the supply chain, and compromise ground units at a later stage [46]. “Cyber vulnerabilities undermine confidence in the performance of strategic systems. As a result, rising uncertainty in information and analysis continues to impact the credibility of deterrence and strategic stability. Loss of trust in technology also has implications for determining the source of a malicious attack (attribution), strategic calculus in crisis decision-making and may increase the risk of misperception” [47] Ground stations - how can we prevent threats? Preventive method and time-based method. Previous attack on ISS. GNSS are specifically vulnerable to hostile cyber operations because of the very low power of their signals and services and constitute potential primary targets in future wars because of their importance not only for military operations, but also for critical national infrastructure and key economic sectors. Unlike physical attacks they are not likely to cause major damages to the satellite navigation system. Recent cyber operations against GNSS were jamming and spoofing [48] although other types of attacks such as hacking or eavesdropping of communications satellite systems, are also technically possible.

#### Disruption of the GNSS system would instantly destroy the global economy and gut virtually every critical infrastructure sector

Graff 18 edited for language [Garrett, editor-in-chief of Washingtonian magazine, instructor at Georgetown University in the Masers in Professional Studies, Journalism, and Public Relations program, former deputy national press secretary for Howard Dean’s presidential campaign, “The New Arms Race Threatening to Explode in Space,” *Wired*, 6/26/18, <https://www.wired.com/story/new-arms-race-threatening-to-explode-in-space/>, accessed 07/05/22]

For decades, America’s satellites had circled Earth at a largely safe remove from the vicissitudes of geopolitics. An informal global moratorium on the testing of anti-satellite weapons had held since 1985; the intervening decades had been a period of post–Cold War peace—and unquestioned American supremacy—high overhead. During those decades, satellites had become linchpins of the American military apparatus and the global economy. By 2007, ships at sea and warplanes in the air had grown reliant on instant satellite communications with ground stations thousands of miles away. Government forecasters relied on weather satellites; intelligence analysts relied on high-­resolution imagery to anticipate and track adversaries the world over. GPS had become perhaps the single most indispensable global system ever designed by humans—the infrastructure upon which the rest of the world’s infrastructure is based. (Fourteen of the 16 infrastructure sectors designated as critical by the Department of Homeland Security, like energy and financial services, rely on GPS for their operation.) Now, Shelton feared, all those satellites overhead had become so many huge, unarmored, billion-dollar sitting ducks. In the decade since China’s first successful anti-satellite missile test, Shelton’s premonition has largely come true: Everything has changed in space. A secretive, pitched arms race has opened up between the US, China, Russia, and, to a lesser extent, North Korea. The object of the race: to devise more and better ways to quickly cripple your adversary’s satellites. After decades of uncontested US supremacy, multinational cooperation, and a diplomatic consensus on reserving space for peaceful uses, military officials have begun referring to Earth’s orbit as a new “warfighting domain.” On the ground, the military is starting to retrain pilots, ship captains, and ground troops in fail-safe forms of navigation that don’t rely on GPS—like celestial navigation. The US military must relearn how to fight “unwired” and defend itself in space. “We knew how to do that, and somehow we forgot,” General John E. Hyten, the head of US Strategic Command, said in 2015. When former director of national intelligence James Clapper left office at the end of the Obama administration, he told me that the increasing sophistication of America’s adversaries in space was one of the top three strategic threats he worried about. Clapper’s successor, Dan Coats, warned last spring that “Russia and China remain committed to developing capabilities to challenge perceived adversaries in space, especially the United States.” Since he took office, President Trump has dropped numerous hints of the warnings he’s evidently getting from military and intelligence leaders. During a spring livestream with astronauts aboard the International Space Station, he alluded, obliquely and without context, to the “tremendous military applications in space.” And he has repeatedly floated the idea of creating a new branch of the armed forces specifically for celestial combat—culminating last week with a speech out-and-out ordering the Joint Chiefs of Staff to begin developing plans for a new “Space Force.” But if space is indeed becoming a war-­fighting domain, it’s important to understand the stakes, not just for America’s strategic standing but for the species. A Russo-Sino-American space war could very well end with a ~~crippled~~ [wrecked] global economy, inoperable infrastructure, and a planet shrouded by the orbiting fragments of pulverized satellites—which, by the way, could hinder us all on Earth until we figured out a way of cleaning them up. In the aftermath of such a conflict, it might be years before we could restore new constellations of satellites to orbit. Preparing for orbital war has fast become a priority of the US military, but the more urgent priority is figuring out how to prevent it. GROWING UP IN Oklahoma City, William Shelton dreamed of becoming a pilot. He got as far as the Air Force Academy before he discovered his eyes weren’t good enough. So instead he became an astronomical engineer. In 1976 he began serving as a launch facility manager at Vandenberg Air Force Base, the military’s oldest space and missile launch base, perched on the California coast north of Santa Barbara. He arrived just as the Air Force was beginning to understand how crucial space would be to its future: The nation’s first early-warning satellites had been put in orbit with the intention of tracking Soviet missile launches, and satellite imagery was becoming increasingly critical to intelligence gathering. Shelton’s poor eyesight, it turned out, had led him to the center of the Air Force’s new frontier. In August 1990, Shelton, then a young lieutenant colonel, took command of the 2nd Space Operations Squadron in Colorado. When he arrived at his post, the Air Force was busy building a new constellation of satellites—launching new ones from Cape Canaveral in Florida every few months to help fill out what he was told would ultimately be a global system aimed at helping the US improve its navigation and increase the precision of its bombs and missiles. This was the new Global Positioning System, and one of Shelton’s first duties at “2Sops” was to build support and enthusiasm for the new effort. To impress visitors (including the brass), he carried around a demo GPS unit that weighed 10 pounds, cost $3,000, and could tell America’s soldiers, sailors, airmen, and Marines exactly where they were on the surface of the planet. The power of the new system that 2Sops ran was proven faster than anyone imagined. The Gulf War caused a rush of final preparations to get GPS ready for battle. Around 2:30 am on January 17, 1991, GPS-equipped helicopters snuck into Iraq, using the technology to guide themselves through the darkened desert and knock out air defense radars. The first bombing campaign of the war had begun. Reporters marveled at precision-­guided bombs zeroing in on their targets and cruise missiles appearing to turn street corners to hit the right buildings. Shelton had a front-row seat to this transformation. As the technology has improved, so has the precision of GPS. The system originally provided accuracy to within 17 yards; with it, you could pinpoint a specific copse of pine trees. Today, if you’re using a smartphone, it can generally locate an object to within five yards—a resolution fine enough to locate a pair of pine trees within that copse. Soon it could be able to zero in on a pine cone: Research from UC Riverside has demonstrated that the latest tech is reliable to within an inch. And research has shown that 1-millimeter accuracy might be eventually possible—which means that the system could locate an individual seed inside that pine cone. Today, troops on the ground use GPS to navigate foreign streets; drone pilots can program a flight plan from thousands of miles away. And because GPS satellites also house America’s detection system for nuclear detonations, we rely on them to tell us if North Korea launches a nuclear weapon, and to tell our missiles and bombs where to find their targets. “When you look at our American way of war, the strategy is largely underpinned by space assets—navigation, early warning, timing,” Shelton says. And that’s just the military. The creators of GPS probably never intended for the system to become the backbone of daily life, but it has. I visited Colorado while reporting this story and tried to keep tabs on everything I did that relied on GPS. There were the obvious navigational moments—my Uber ride to the airport, my American Airlines flight to Denver, my own Google Maps–guided drive in a rental car to Schriever Air Force Base, outside Colorado Springs. But there were also less obvious instances, like the phone calls I made along the way (cellular networks rely on GPS data to keep their stations synchronized), my stop at the ATM (banks use GPS to track deposits and withdrawals), and the fill-up at the gas station (the credit card system also relies on GPS). Moreover, GPS is no longer the world’s sole geolocating mechanism. Russia, China, and the European Union have now all either deployed or begun working on their own full constellations of navigation satellites, ensuring that they won’t have to rely on the US system. It also means that, in the early moments of a war, it’s a fair bet that satellites—the other guy’s satellites—could be among the first targets. DURING THE COLD War, a US army mountain outpost in the Fulda Gap, the shortest route between East and West Germany, served as an early warning trip wire for a Soviet invasion of Europe. If Russian tanks ever made a surprise attack, NATO planners knew that the soldiers there would likely be the first to find out. Today, the members of 2Sops play a similar role. Deep inside the squat, beige, windowless Building 400 at Schriever Air Force Base—the destination I had plugged into Google Maps during my trip to Colorado—10 people at a time remotely operate the heavenly constellation of GPS satellites that guide Tomahawk cruise missiles to their targets, deliver Lyft passengers to their destinations, and help farmers cultivate their crops. They also watch out for any shocks or attacks on the system. The average GPS operators are in their mid-twenties. During one recent shift, the entire Global Positioning System was being operated by two 19-year-old airmen (who, the Air Force emphasizes, are rigorously trained). Their commander, US Air Force lieutenant colonel Peter Norsky, is in his mid-thirties. Together, they watch over the roughly three dozen GPS satellites, troubleshooting the geolocation system and minding the quirks of each orbiting craft—this one’s damaged solar panels, that one’s balky communications links—as if they were remotely tending a stable full of temperamental horses. As integral as GPS is to daily life, the way it actually works is little understood by most people outside of Schriever Air Force Base. Fundamentally, the function of GPS is to provide the globe with a shared clock. GPS satellites allow phone companies to keep their systems in sync, battleships to chart open waters, and ATMs to time-stamp their transactions by triangulating signals from overhead and measuring how long it takes those signals from different satellites to reach a GPS receiver. The system works by making daily calculations, employing Newtonian physics and Einsteinian relativity, to minutely tweak the time broadcast from each GPS satellite as it moves through space—the high-tech version of tuning your grandfather clock to within 100-­billionths of a second. Time is, after all, relative; as of January, the time in space was 18 seconds ahead of Earth’s “Coordinated Universal Time,” since space doesn’t recognize the leap seconds that scientists add to terrestrial time to account for the planet’s slowing rotation. Additionally, the time-keeping device on each satellite gives a subtly different reading, the result of variations in their atomic clocks, which tell time by measuring the precise oscillations of an atom. (Some GPS satellites use rubidium atoms, which are highly accurate day to day; some use cesium, which is more accurate over long stretches.) Any malfunction in the GPS system threatens to plunge the global economy into chaos. Fortunately those glitches are rare, but they’re not unheard of. On January 25, 2016, one of 2Sops’ flight commanders, Captain Aaron Blain, was awoken by a call from work in the middle of the night. User reports from around the country suggested that the system’s precision had “wobbled,” making measurements increasingly inaccurate. Blain raced to Schriever in his Ford pickup and found that the constellation’s timing was off by about 13 microseconds. It was an infinitesimal number—over 25,000 times shorter than the blink of an eye—but for the finely tuned GPS it was a yawning crevice. Left uncorrected, the glitch could have ricocheted through the global economy, corrupting not just driving directions but stock trades too.

### AT: Economy bad now

#### Inflation on the decline – but new shocks can stop the positive trends

**Carlsson-Szlezak , 2022**

[Philipp, global chief economist of BCG, “[Weighing the Risks of Inflation, Recession, and Stagflation in the U.S. Economy” Harvard Business Review, June 10 2022 https://hbr.org/2022/06/weighing-the-risks-of-inflation-recession-and-stagflation-in-the-u-s-economy](Weighing%20the%20Risks%20of%20Inflation,%20Recession,%20and%20Stagflation%20in%20the%20U.S.%20Economy) accessed 7/7/22 GDI-TM]

Covid inflation has been an unusual confluence of extremely high demand, driven by enormous stimulus, and simultaneous supply bottlenecks in product, commodity, and labor markets. It was more persistent than widely expected because new shocks kept coming. Initially, it was harmless “bounce” inflation from low prices at the start of the pandemic. Later came the supply bottlenecks; then the energy surge of last year; an enormous scramble for labor; the unexpected war in Ukraine; and the economic lockdown in China this spring. Inflation will remain hard to predict — those who warned against inflation early did not do so because they anticipated this sequence of shocks. **While it’s not over, the period of maximum stress is likely behind us. Demand is cooling. Inventories have been rebuilding healthily. Workers are returning to the labor force. This will allow inflation figures to moderate throughout the rest of the year. Another signal of moderating inflation is firms’ waning pricing power.** Firm profits grew strongly in 2021 — microeconomic proof of inflation since firms were clearly able to pass through price pressures to consumers. But that is less and less likely to persist. Consider that firms usually face a tradeoff between raising prices and losing market share. As the economy reopened, that tradeoff was suspended because of high demand and low supply. But as demand slows and inventories rebuild, pricing power is likely to wane. Big retailers, such as Walmart and Target, recently exhibited such dynamics when they showed shrinking margins. That said, moderating inflation is not the same as vanquishing inflation. Realistically, inflation, while declining, will stay above the target rate of 2% through all of next year and plausibly beyond — and upside risks remain. There could be new, unexpected shocks.

### AT: recession risk now

#### Recession risks limited – trending in the right direction

**Carlsson-Szlezak , 2022**

[Philipp, global chief economist of BCG, “[Weighing the Risks of Inflation, Recession, and Stagflation in the U.S. Economy” Harvard Business Review, June 10 2022 https://hbr.org/2022/06/weighing-the-risks-of-inflation-recession-and-stagflation-in-the-u-s-economy](Weighing%20the%20Risks%20of%20Inflation,%20Recession,%20and%20Stagflation%20in%20the%20U.S.%20Economy) accessed 7/7/22 GDI-TM]

As the chance of recession comes down to the balance of moderating inflation vs. a slowing economy, we should also ask how much stress the economy can absorb. If a 2023 recession is avoided, it will be because U.S. consumers and firms are still in robust health. Household balance sheets are strong, and the labor market is booming. Encouragingly, we see some cooling of inflation pressures (such as falling durable goods prices and easing wage growth) without macroeconomic weakness. And though firms’ margins will decline from here, they’re coming down from exceedingly strong levels. Yet, it’s easy to point to the economy’s vulnerabilities. Deteriorating business sentiment can weigh on investment rapidly, robbing the economy of momentum. And despite the strong labor market and strong household balance sheets, consumer confidence has been depressed for a while, likely driven by energy prices. Add to that the fact that wobbly financial markets shrink household wealth — a problem that would get bigger if the housing market were to turn — and the cycle looks vulnerable. That said, if a recession hits in 2023, there are good reasons to expect it to be mild because the drivers of the most damaging types of recession are less likely today. Banks are well capitalized, profitable, and unlikely to drive a structural overhang in recession. This leaves the prospect that demand could return quickly and that labor markets remain tight, which would keep a recession mild.

## Supply Chain

### Squo - Attacks Increasing

#### Supply chain attacks have been small, but massive escalation is coming

Higgins 21 [Kelly, Executive Editor of Dark Reading, award-winning technology & business journalist, named one of the Top 10 Cybersecurity Journalists in the US by Onalytica, “Why Supply Chain Attacks Are Destined to Escalate,” 08/05/21, <https://www.darkreading.com/vulnerabilities---threats/why-supply-chain-attacks-are-destined-to-escalate/d/d-id/1341588>, accessed 07/04/22, GDI-JCR]

The epic software supply chain attacks over the past year, including the high-profile breaches of SolarWinds, Microsoft Exchange Server, Kaseya, and Codecov, were only the beginning. "Supply chain attacks are only just starting, and mostly with pretty small vendors that most people had not heard of beforehand," said Corellium COO Matt Tait, in a live conversation via video with Black Hat founder Jeff Moss. But what happens when these attacks get bigger and affect larger vendors and more of their customers? Tait – who also delivered the prerecorded keynote, which was streamed on multiple large screens in a ballroom at the Mandalay Bay Conference Center in Las Vegas yesterday – said in the live portion of the event that the relative impact of these high-profile attacks could have been much worse given they were mostly targeted. He warned there will be more and they could well wreak more extensive and widespread damage to more organizations if the attackers hit larger targets with massive customer bases, such as the recent theft of source code from gaming giant EA Games. "It's likely to start to escalate in the coming months and years," he said. "And when something really big happens ... everything else will look like complete peanuts" in comparison, he said. When a nation-state or cybercrime organization makes that leap and infiltrates more victims, it will no longer be a "sustainable" situation.

### Internal link - NATO Key to Supply Chains

#### NATO is central to the protection of global supply chains

Granger 22 [Euan, Materials & Supply Chain Manager at Soil Machine Dynamics Ltd, “The Role of NATO in Protecting our Supply Chains,” 05/17/22, <https://www.procurious.com/procurement-news/author/euan-granger>, accessed 07/04/22, GDI-JCR]

NATO plays an active role in global peacekeeping, has built up the concept of co-operative security, and is a deterrent for illegal and terrorist activities. And it is in this role that we see the link between its activities and its importance to global supply chains. Protecting the Supply Chain Current events such as the war in Ukraine and global COVID restrictions, as well as the ongoing threat of terrorist activity has highlighted the importance of stability and continuity in the supply chain. For example, while Ukraine may not be a member of NATO, the NATO countries are using integrated logistics and supply routes to move arms, vehicles and aid into the war zone. Through its actions in the past, as well as actions it is taking now and for the future, NATO is providing support and protection for global supply chains. Here are three key ways that demonstrate the importance of the organisation to the global community: 1. Protection of Key Infrastructure – Energy Security Energy and key utilities, such as oil and gas, are critical for almost every aspect of global supply chains. Disruption to sources or supplies of energy could easily undermine the security of countries and continents, leading to situations where global production is halted, and supply of everything from electronic components to food and drink is disrupted. Vulnerabilities exist not only in infrastructure (oil/gas pipelines; power stations), but also in the systems used to control and manage them, especially in light of the increasing threat of cyber attacks. NATO members have been working since 2008 on energy security programs to help protect key infrastructure and ensure continuity of supply for both nations and the military. 2. Counter Piracy Operations and Protection of Sea Lanes Piracy continues to be a major threat to supply chains and freight in key shipping lanes around the world. While it would seem that the threat of piracy has lessened due to fewer serious incidents reported in the press in recent years, it remains a problem for shipping companies. NATO has in the past assisted in operations such as Operation Shield, an international cooperation to combat piracy of the east coast of Africa. Though this operation has since ended, NATO continues to work with countries and global partners to assist further anti-piracy efforts. Without the protection that NATO affords in conjunction with national navies and governments, there is the potential for disruptions to ships and cargo that would have lasting impacts on global supply chains. 3. Crisis Management including Relief Supplies in event of Natural Disasters NATO plays a key role in crisis and disaster management, both within its member countries and outside of this region. For this, NATO actually forms part of the global supply chain, ensuring that aid, equipment and personnel are able to reach areas affected by natural disasters. This can take the form of physically shipping goods on behalf of its member nations, as well as ensuring that requests for assistance from members or other countries are conveyed to the correct areas of government. While we may not see the work that NATO does as part of, or to support, global supply chains, its importance cannot be overemphasised. Without its efforts since its inception over 70 years ago, the global supply chain would look very different to how it does now.

### Impact – Economy

#### With supply chains stretched thin, disruption would be economically catastrophic – there’s zero buffer. EU simulations prove.

Murray 22 [Brendan, Trade Tsar at Bloomberg LP, “Cyber Threat Adds Another Curveball to Shipping Outlook,” 2/15/22, <https://www.bloomberg.com/news/newsletters/2022-02-15/supply-chain-latest-cyber-risk-adds-curveball-to-shipping-outlook>, accessed 07/04/22, GDI-JCR]

Jensen recalled a major cyber event in 2017, when shipping giant Maersk was among thousands of companies that shut systems down to assess the data damage. The Copenhagen-based container carrier’s estimate of the cost was around $300 million. Back then, port operators were among those with the most tangible consequences. While goods were moved, the process was slowed as terminals reverted to manual or backup operations. Still, the global economy absorbed the shock without much wider damage. With supply chains stretched to their limits, that’s unlikely to be the case now. No Buffer “In 2017 we could essentially lose the largest carrier in the world for a week and it didn’t cause any major problems,” Jensen said. “Sure, if you had your cargo on board one of those ships it got delayed maybe a week or two and that was annoying, but from a global perspective it was a non-event in terms of disturbing the supply chain. There was plenty of buffer capacity — of ships, terminals, everything. Right now we have zero, as in literally zero, buffer capacity.” Four of the world’s top five container lines are headquartered in western and northern Europe, and at least one has been hit with a cyber attack since the start of the pandemic. Marseille, France-based CMA CGM said in September 2020 that a breach hit services and affected bookings. Days later, the International Maritime Organization, a United Nations agency that serves as the industry’s regulatory body, said it suffered “a sophisticated cyber attack” affecting its public website and internal systems. In mid-January, European Union governments took part in large-scale simulation of a cyber intrusion affecting multiple member countries. The six-week exercise was expected to model attacks on supply chains and some spillover socio-economic effects in other countries. “If they have done their jobs well, they have a good backup plan,” Jensen said. “In the current environment, taking just one major port out of action for two, three, four days on top of what we’re already dealing with — that will have major ramifications on the supply chain.”

### Impact – Economy

#### Economic downturn and fragmentation of world economy challenge LIO – and harms ability to deal with existential threats like climate change

**Georgieva, IMF Managing Director, 2022**

[Kristalina “Facing Crisis Upon Crisis: How the World Can Respond” IMF, April 14, 2022 [https://www.imf.org/en/News/Articles/2022/04/14/sp041422-curtain-raiser-sm2022 accessed 7/7/22](https://www.imf.org/en/News/Articles/2022/04/14/sp041422-curtain-raiser-sm2022%20accessed%207/7/22) GDI -TM]

In economic terms, growth is down and inflation is up. In human terms, people’s incomes are down and hardship is up . These double crises—pandemic and war—and our ability to deal with them, are further complicated by another growing risk: fragmentation of the world economy into geopolitical blocs—with different trade and technology standards, payment systems, and reserve currencies. Such a tectonic shift would incur painful adjustment costs. Supply chains, R&D, and production networks would be broken and need to be rebuilt. Poor countries and poor people will bear the brunt of these dislocations. This fragmentation of global governance is perhaps the most serious challenge to the rules-based framework that has governed international and economic relations for more than 75 years, and helped deliver significant improvements in living standards across the globe. It is already impairing our capacity to work together on the two crises we face. And it could leave us wholly unable to meet other global challenges—such as the existential threat of climate change. It is a consequential moment for the international community. The actions we take now, together, will determine our future in fundamental ways. It reminds me of Bretton Woods in 1944 when, in the dark shadow of war, leaders came together to envision a brighter world. It was a moment of unprecedented courage and cooperation. We need that spirit today, as we face bigger challenges and more difficult choices.

### AT: Economy not great now

#### See space section

# Aff – solvency mechanisms

## Cyber Policies - General

### US NATO cyber key

#### US and NATO proactive and continuous responses needed to enhance deterrence and defend in great power war competition with Russia and China

**Kramer et al, Atlantic Council, 2020**

[Franklin, “NATO needs continuous responses in cyberspace“ New Atlanticist

December 9, 2020 <https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-/responses-in-cyberspace/> accessed 7/7/22 GDI-TM]

President-Elect Joe Biden’s transition team has declared cyber threats as “one of the defining challenges of our time.” In its early days, the incoming US administration must take on cybersecurity threats as one of its key priorities. Nowhere will that effort be more important than with the United States’ closest Allies at NATO, a cornerstone for Western security. Today, NATO’s security is threatened by Russia’s and China’s continuous cyberattacks on the Alliance and its members. To accomplish its mission of deterrence and defense, NATO needs to implement a strategy of proactive, continuous responses to China and Russia in cyberspace, where great power competition is playing out in real time.

### US led efforts key

#### Resiliency, active cybersecurity, sustained interventions to reduce China and Russia cyber capabilities should be focus of NATO cyber shift – US leadership necessary

**Ahlawat, 2021**

[Urjasvi, Jindal School of International Affairs and Research Intern at the Centre for Security Studies, “NATO: CYBERSECURITY AND CYBER COALITION“CSS ISSUE BRIEF, January 2021, https://jgu.s3.ap-south-1.amazonaws.com/jsia/Urjasvi+-+NATO+Cybersecurity.pdf accessed jcp-tm 6/9]

THE UNITED STATES ASPECT

Being the influential and dominant member, the United States did not consider NATO or cybersecurity to be of great importance, however, the dynamics are likely to change post- 2020 Presidential elections. Joe Biden, the President-elect, declared cyber threats as “one of the defining challenges of our time.” He believes that in today’s time, Russia and China impose a threat to NATO’s security by continuously attacking the Alliance and its members. To equip with protection from the aforementioned threats, Biden under the US believes that NATO has to adopt a policy of constructive, ongoing responses to China and Russia in cyberspace to achieve its mission of deterrence and security, where great power rivalry is taking place in real-time. NATO’s central focus should be on cybersecurity, for which the following three key actions are to be followed.

First, NATO should mandate that resilient cybersecurity architectures, the powers of its members and its main essential infrastructures be built and enforced by itself. Primary elements of a robust infrastructure could include the use of cloud technologies in the private sector; zero confidence architecture for successful access management; creation of stable hardware capabilities; and cyber defences increased by deep learning and artificial intelligence. To achieve this, the architecture framework suggested needs to be flexible to adapt to the rapidly developing and emerging technologies. However, the barrier arises as it is a challenge for NATO to itself build the suggested architecture. Using the NATO Defence Planning Process (NDPP), procurement processes, requirements and goals, and Allied Command Transition strategy to promote a robust research and development initiative, it should stress their necessity and require its members to do so.

NATO must agree that one size would not fit all when determining specifications for these resilient architectures. Not only will requirements differ among military, government, and critical infrastructures operators, but, as has been shown in the development of autonomous vehicles and space capabilities, there are a variety of different approaches that may prove effective.10

Second, **NATO should conduct active cybersecurity in cooperation with its nations**. Due to technological loopholes or human error, even the best exclusionary technologies in a cybersecurity resilient design may fail. As a result, even after an attacker has abused cybersecurity, the alliance requires "active cyber defences'' that will create durability. These features impact only certain networks where they have been built by providers and owners and are not for offensive purposes. In its Active Cyber Defence11, the US National Security Agency illustrates how the key elements of active defence capacities include “real-time communication, sense-making analytics to understand the current state and automated decision-making to decide how to react to current state information.’’[10]

NATO must be capable of searching for potential enemies within electronic networks vital to security as a core aspect of successful cyber defence. By removing malware and closing redundant **ports, the Alliance could build highly competent specialist hunting teams to review device operations, identify irregularities, and combat intruders**. NATO Standing Cybersecurity Hunt Teams should also be working with the cooperation and active collaboration of national governments and operators of infrastructure networks. These hunting teams will perform in- depth technological assessments of live networks to detect unnoticed risks, according to the US Department of Homeland Security. Standing Cybersecurity Hunt Teams will broaden the capacities of NATO's existing Cyber Rapid Response teams, which are small in size and work reactively, with an emphasis on aggressive protection.

Third, NATO should strategize a sustained intervention policy aimed at reducing Russian and Chinese interventions to undercut the cyberspace alliance. US Cyber Command developed the idea of sustained commitment, but the reasoning still extends to NATO, arising from the need to tackle the current cyber attack campaigns emanating from Russia and China. Persistent engagement includes monitoring enemies, recognising their objectives, evaluating the instruments used for attacks, and taking steps to degrade their ability to blunt current attacks or stop potential attacks. As a core aspect of its deterrence and security, the Alliance wants a sustained commitment cyber policy.

NATO should exploit its intelligence and defence preparation resources to build a framework for allies to actively control cyberattacks from Russia and China to ensure sustained participation successfully in the Alliance. NATO can collect information through its Intelligence and Security Branch, attacking allied vital assets, strategic capabilities, or democratic structures. Using this material, the Cyberspace Operations Center (CYOC) of NATO could outline ways to decrease the capacity of Russia and China to carry out such attacks. The CYOC should share its analyses with pre-designated Allies who would work with targeted countries and employ their cyber effects against the identified threats12. In support of NATO operations, nine NATO nations have already pledged to make those results possible. The aforementioned cyber-capable allies will be responsible, based on NATO guidelines, for persistently undermining the cyber operations of adversaries. This model will make the CYOC of NATO a strategy platform with an approach to persistent interaction around the Alliance. It will allow NATO to encourage its members to take individual or multilateral measures against hybrid cyberspace operations by adversaries.

### NATO comprehensive policy – solvency

#### Revised policies for NATO collective cyber defense and offense under Article 5 necessary - multifaceted unified policy solves

. NATO must plan to protect the infrastructure and key resources of member states as a unified effort, not a piecemeal operation undertaken by a few nations. In order to do this, NATO must identify and prioritise infrastructure for protection, as well as criteria and policy for action

**Klipstein and Japaridze, 2022**

[Michael and Tinatin, Associate Research Scholar, Arnold A. Saltzman Institute of War and Peace Studies, Columbia University and Vice President of Business Development and Strategy, The Critical Mass; “Collective cyber defence and attack: NATO’s Article 5 after the Ukraine conflict” Commentary European Leadership Network 16 May 2022 <https://www.europeanleadershipnetwork.org/commentary/collective-cyber-defence-and-attack-natos-article-5-after-the-ukraine-conflict/> accessed 6/8/22 JCP-TM]

With the Russian invasion of Ukraine on February 24, 2022, US and Western European pundits predicted devastating and crippling cyber effects predicating kinetic warfare. However, over the past weeks, numerous Russian actions in cyberspace have largely flown beneath the radar due to actions by the cyber-security industry, or so-called “patriotic hackers”, who have taken it upon themselves to counter Russian cyber aggression and attack Russian cyber infrastructure. In light of developments such as these, the North Atlantic Treaty Organisation (NATO) should consider and create policy for collective cyber defence, and potentially offense, under Article 5 of the NATO Charter.

Cyberspace has proliferated across the globe, particularly in critical infrastructure, as technology has eclipsed traditional definitions of computing. Non-traditional computers reside in pockets, are able to make phone calls, and, increasingly, take high-resolution photographs. These non-traditional computers also maintain proper food temperatures in kitchens, give directions in cars, and track movement and health on people’s wrists. But more importantly, these non-traditional computers reside in critical infrastructure centres displaying data for operators in the form of large screen monitors on walls, showing the physical environment through closed circuit television cameras. Many of these devices, which frequently lack anti-virus protection and utilise vulnerable protocols, exist within critical infrastructure, either natively or brought into these environments by employees. Electrical power generation and distribution, telecommunications, finance, and water treatment and distribution are some examples of critical infrastructure that are managed by computer-controlled systems. Compounding the problem, the internet does not abide by national boundaries, making forensic investigation and attribution difficult. Critical infrastructure sectors rely heavily on automation, and thus online control, as described in the U.S. National Strategy for Maritime Cybersecurity.

Recent state activities demonstrate how cyberoperations can have physical consequences. In the summer of 2020, Iranian hacking of Israeli water treatment facilities came close to over-chloritizing the water, changing faucets into poison dispensers. More recently, in February 2022, in an attempt to cut communications within Ukraine, Russian cyberattacks on Viasat satellite networks disrupted German windmill electricity generation and distribution. Additionally, Russia has in the past—and continues in the current war as recently as April 2022—to target electrical power generation and distribution systems with cyber effects and to harm Ukrainian civilian and military infrastructure. As the above examples show, cyber attacks are not limited to online locations but their impact can be felt in the physical world. As a result, NATO must prepare for these activities to grow and expand.

Following the shortcomings of the 2015 United Nations Group of Governmental Experts report on information and telecommunications in the context of national security, a lack of consensus continues to exist on the severity of cyberspace operations targeting critical infrastructure requiring collective and even national responses. Individual nations constructed individual criteria and response actions, utilising diplomacy, information, military, or economic action. They largely did so alone or in combination with other states. NATO, however, did not formulate a coherent analogous response and as a result, lacks publicly acknowledged policy addressing cyberspace activities that would constitute a necessary collective response under Article 5. In order for NATO to maintain its relevance in the present moment and sustain it through the coming years, this paradigm must change.

NATO must adjust its thinking regarding methods of warfare as cyberspace operations—both destructive attacks and disinformation—continue to grow in complexity and in certain areas even replace traditional kinetic operations. To fulfill this role in kinetic as well as non-kinetic realms, NATO must be prepared for hybrid forms of warfare and present slated to join the alliance a cohesive and tailored response to transgressions. This is increasingly important as Russia continues to threaten potential future NATO members such as Finland and Sweden, who are slated to join the alliance in the coming months. Russia has overtly stated that the invasion of Ukraine was, in part, a response to NATO’s eastward expansion. Although Russia has deemed NATO expansion into former Soviet states to be problematic since the collapse of the USSR, recently, Moscow has also begun to denounce potential expansion beyond its perceived immediate sphere of influence. For example, on April 14, 2022, Russian Minister of Foreign Affairs Sergei Lavrov cautioned that the inclusion of Finland and Sweden into the military alliance would have dire consequences, including Russia reinforcing nuclear weapons in the Baltic Sea region.

Considering the increased emphasis and relevance of the transatlantic alliance leading up to and during Russia’s invasion of Ukraine, it is imperative for the organisation’s member states to identify and agree upon more pronounced “triggers” or “red lines” that determine what constitutes a sufficiently egregious action in cyberspace for Article 5 to be discussed, and if need be, potentially invoked. Furthermore, in enhancing its preparedness in cyberspace, specific policies must be crafted that delineate synchronised actions taken collectively by members to prevent Russian malign activities in the cyber domain under Article 5 to allow for a rapid and coordinated response. The dominance of the US, the UK, Australia, Canada, and New Zealand, known in government as the FVEY, or Five-Eyes, highlights the urgent need for the alliance to develop policy addressing the collective defence of NATO members. Effective policy for NATO should address collective and coordinated cyberspace operations, both offensive and defensive. Currently, NATO, as a military institution, lacks “rules of engagement” for cyberspace and individual member states lack a standardised threshold or response guidance. Therefore, NATO must define the activities, “red lines”, and threshold incurring response, as well as what a coordinated kinetic/cyber response would entail. The interconnectedness of European critical infrastructure, as illuminated by the Russian ViaSat communications attack impacting German wind power generation and distribution, highlights the requirement for NATO to address cyberspace as the critical domain it is. As a result, we recommend:

In the event of adversarial cyberspace actions warranting Article 5 action, the NATO Commander becomes the commander and coordinator for all cyberspace activities, both defensive and offensive, by NATO nations within the area of hostilities.

NATO identifies, establishes, prioritises, and continually refines critical infrastructure and key resources within member nations, as well as criteria for what constitutes necessary action for collective responses.

NATO identifies limits of activity, or “red lines” resulting in Article 5 response discussions.

NATO members present the NATO Commander intelligence identifying indications, warnings, and attribution of cyberspace attacks, both for response action and, where applicable, public consumption.

NATO members present legal constraints and capabilities of nations to the NATO commander allowing maximisation of nations’ capacity and capability.

NATO must recognise cyberspace for what it is—an interlocutor of networks and devices from control systems for critical infrastructure to seemingly anonymous devices operating in the background of our lives. This interconnectedness by an invisible thread of information, however, is the critical vulnerability in the stability of societies. NATO must plan to protect the infrastructure and key resources of member states as a unified effort, not a piecemeal operation undertaken by a few nations. In order to do this, NATO must identify and prioritise infrastructure for protection, as well as criteria and policy for action. Russia’s recent invasion of Ukraine and the Kremlin’s increased aggression, not solely in kinetic but also in non-kinetic realms, is a stark reminder that the alternative to further delay of the inevitable recognition of cyberspace for what it is will, ultimately, prove to be all the more costly.

### NATO tech innovation key

#### \*\* NATO ahead on tech now – gap closing with Russia, China and non-state actors. NATO investment in tech capacity and innovation necessary to keep gap in capabilities

Magula and Alvarez-Couceiro, 21

[Justin, Army Strategist serving in the Strategic Landpower and Futures Group at the U.S. Army War College, and Paula, graduate of Strategic Studies at the Johns Hopkins University School of Advanced International Studies, "Mainaining and Improving NATO's Technological Edge", Wavell Room, 9/30/21, https://wavellroom.com/2021/09/30/maintaining-improving-natos-technological-edge-technology/, accessed 7/4/22, GDI-cc]

What happens when an alliance’s competitors quickly improve their technology and capabilities to place the alliance at increased risk? The North Atlantic Treaty Organization (NATO) addressed this dilemma during a recent summit in Brussels.  At the summit, the North Atlantic Council built upon[NATO’s 2030 strategic outline](https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf) and presented targets for increased technological collaboration to counter growing threats from Russia, China, and non-state actors. While NATO’s scientific and technical superiority has historically allowed it to outpace competitors, its adversaries are quickly closing the gap.

NATO members still hold advantages in their development of [new technologies](http://wavellroom.com/podcast/technology-and-the-future-of-land-warfare/). According to the Global Innovation Index, seven of the top ten[most innovative countries](https://knowledge.insead.edu/entrepreneurship/the-worlds-most-innovative-countries-2020-15076) globally are part of NATO, while the other three are key NATO partners. Even so, NATO can do more to harness the alliance’s combined technological prowess to better compete and win in a future conflict. As China seeks to become the[world’s innovation leader](https://www.businesschief.asia/leadership-and-strategy/china-aims-be-global-innovation-leaders-next-15-years) and Russia continues to undermine the alliance’s security, NATO will need to out-innovate its competitors and prepare for an uncertain future.

Four areas where NATO can focus on improving its competitive edge are developing its formal organizations, increasing public and private sector collaboration, harnessing and countering Emerging Disruptive Technologies (EDTs), and improving conventional military equipment. NATO must maintain its relative lead in technology sectors to defend its people and enhance its long-term strategic position. Improving science and technology (S&T) innovation will increase alliance collaboration, strengthen public and private sector cooperation, counter hybrid threats, deter adversaries, and harden defenses against attacks. NATO’s effectiveness in the future will heavily depend on its ability to maintain and improve its science and technology capabilities.

#### EDT innovation key to check Russia and China threat

**Becker et al.**, affiliated with the Centre for Security, Diplomacy and Strategy at the Vrije Universiteit Brussels, **2022**

(Jordan, academy professor and director of the Social Science Research Lab at West Point academy, “DON’T LET RUSSIA DOMINATE THE STRATEGIC CONCEPT,” War on the Rocks, JUNE 28, 2022, https://warontherocks.com/2022/06/dont-let-russia-dominate-the-strategic-concept/, accessed 7/3/2022, gdi-tmur)

A significant strategic concern for NATO allies is to avoid precipitating a Russian-Chinese authoritarian alignment. While Russia and China face distinct strategic challenges of their own and their “unlimited partnership” has appeared to stumble upon some limits, their continued pursuit of emerging, disruptive technologies and their authoritarian models of governance present significant risks to NATO allies. These models, coupled with Russia and China’s shared willingness to undermine national and international institutions in the trans-Atlantic community, mean that the most daunting threat NATO faces may be to its foundational values. Incorporating these core values into strategy and policy will be a key task for the 2022 Strategic Concept.

New Domains

Whether in coordination or not, China and Russia will undoubtedly continue to challenge allies in domains like space and cyber using emerging and emerged technologies. Dealing with such challenges is core NATO business — grounded in Article 3 of the Washington Treaty and resting primarily with national authorities. The new Strategic Concept should aim to integrate these relatively new domains while responding to disruptive technologies as well. Allies must endeavor to reach a “pre-crisis” consensus on what space and cyber actions would constitute an “armed attack” in accordance with Article 5. This kind of crisis decision-making is a core function of NATO’s political and military headquarters. Such agreement, when paired with improved national capabilities, would contribute to deterrence by communicating resolve to adversaries. Improved capabilities themselves will only arise through public-private partnership to maintain a technological edge. A common strategic culture of innovation, much of which arises from the private sector, is a key advantage that NATO has — and should retain — over its adversaries. Such innovation has been on display in the Russo-Ukrainian war and will doubtless be essential in future conflicts.

## Cyber defenders

#### NATO cyber defenders increase cyber defense – new partnerships and tech key

**Ackerman 20**

(Robert Ackerman, Retired Editor in Chief, SIGNAL Magazine, and Senior Director, SIGNAL Media; former war correspondent at AFCEA International, graduated from Boston University in communications, “NATO Expands Cybersecurity Activities” Signal Magazine, May 2020, Proquest, accessed 6/29 GDI- TMK)

From partnerships with industry to dual-use Al cyber capabilities, the alliance is playing the field. NATO is doubling down on cyberspace defense with increased partnerships and new technology thrusts. Information exchanges on threats and solutions, coupled with research into exotic capabilities such as artificial intelligence, are part of alliance efforts to secure its own networks and aid allies in the cybersecurity fight. The threats the alliance networks face constitute relatively the same ones confronting other organizations. NATO faces the double challenge of securing its own networks and information assets, as well as helping its member nations improve their own national cyber resilience. In the past, NATO viewed cybersecurity as somewhat of a technical challenge. But that perspective evolved over time as the cyberscape underwent changes. This came less from choice and more of necessity as a result of the amount and content of malicious cyber activity, explains Christian Liflander, head of section, Cyber Defense, Emerging Challenges Division, NATO. NATO does not have any tanks, ships or aircraft, with a few exceptions such as the AWACS aircraft operated from Geilenkirchen Air Base in Germany. However, when it comes to cyber defense, NATO has its own capability that defends its networks and maintains their operation in the face of adversarial actions. Unlike combat forces, cyber defenders are all NATO staff members. This force is not dependent on individuals loaned from member nations. Instead, it staffs its own personnel to form a core of cybersecurity expertise. One constant over the next few years will be the need to remain resilient, Liflander states. NATO networks must be built and operated in ways that deny benefits to cyber attackers. This includes NATO being able to run networks in a degraded environment. Yet this is easier said than done, he offers. While NATO will continuously work to improve its cyber defense, its adversaries also will become more sophisticated and capable. "The changing threat landscape will continue to challenge us," Liflander says. "I don't really think there will be an endpoint where we can declare mission accomplished," he states. "It is a continuous task, a continuous mission, making sure that networks are well-defended." The alliance is looking to manage risk differently, he offers. "It's not only a technical risk that we're looking at; it's a risk to a mission." The alliance must be certain that an operational commander is able to operate in cyberspace with the same freedom of maneuver available on land, at sea and in the air. National cybersecurity resilience also presents the dichotomy of continuity and change. Member nations often face threats to their critical infrastructure or other soft elements in addition to hardened government networks. Attackers can be nation-states, organized criminals, individual hacktivists or even those working as proxies, although the vast majority of attacks are nonstate activities such as ransomware. "NATO's role in helping allies improve national resilience will become even more critical," Liflander offers. And NATO is no different in terms of potential threats to its networks. The alliance is looking at issues such as military supply chains, training and education, situational awareness and resourcing cyber defense. But Liflander emphasizes that NATO does not want to fall into the trap of viewing cybersecurity as simply a technology issue. This brings into play training and cyber hygiene, he notes. Neither the alliance nor its member nations have unlimited resources for cyber defense, so they must ensure that their resources are applied effectively, Liflander notes. NATO will serve as an important facilitator for allies as they develop their national cyber capabilities. "It starts with resources. If you're not spending resources, you're not going to improve," he declares. Liflander offers that NATO is one of the most sophisticated cyber actors among international organizations, and that comes from both its mandate and its partnered approach. "We have quite understood that no one, however powerful, can go it alone," he declares. "You need to cooperate. That's a prerequisite in order to do your job well."

## Cyber exercises – see also mil to mil

## Cyber force expansion

### SQuo – NATO increasing cyber force

#### Rapid response cyber force to combat growing cyber threat

**SC Media 22**

(SC Media Staff, SC Media is the essential resource for cybersecurity “NATO unveils plans against mounting cybersecurity threats,” SC Magazine, June 30th 2022, https://www.scmagazine.com/editorial/brief/threat-intelligence/nato-unveils-plans-against-mounting-cybersecurity-threats, accessed 7/3/22, GDI- TMK)

Growing cybersecurity threats have prompted NATO to reveal plans for a rapid response cyber force and expanded cyber defense aid for Ukraine amid its ongoing conflict with Russia, as well as an increased focus on Chinese state-sponsored attacks, CyberScoop reports. "We will significantly strengthen our cyber defenses through enhanced civil-military cooperation. We will also expand partnership with industry. Allies have decided, on a voluntary basis and using national assets, to build and exercise a virtual rapid response cyber capability to respond to significant malicious cyber activities," said NATO in its declaration. Such a declaration from NATO shows a stronger emphasis on cybersecurity, according to Chris Painter, who led cybersecurity at the State Department during the Obama administration. "Cyber is now part and parcel of both the threat and the response that NATO is looking at its no longer some foreign object. It is something that they have been building steadily since [the] Lisbon [NATO summit] many years ago, and it's become more and more prominent as time goes on. And thats appropriate," said Painter.

## Cyber norms [multilateral agreement]

### Multilateral explicit agreements solves – norm enforcement

#### Multilateral explicit agreements key to effective norm enforcement against IP theft

**Kim ‘22**

(Wonny K. Kim, Innovation and Information Operations Officer in the U.S. Army Reserve 75th Innovation Command, Master of International Affairs from Columbia University, Master of Science in Technical Intelligence from National Intelligence University, and B.A. in Philosophy and Psychology from Binghamton University, ““Explicit” Bargains are Essential to Forming Desired Norms in Cyberspace,” Cyber Defense Review, Spring 2022, JSTOR, accessed 6/30/22, GDI- TMK)

WHY CULTIVATING TRUE COOPERATION IS KEY

Criminal, non-state sponsored, activity withstanding, why would the PRC choose to violate an explicit bargain in the face of a credible threat of retaliation? Assuming a rational actor, it would be simply because the prospective marginal gains still outweigh the prospective mar- ginal costs. Though explicit bargains set the conditions for avoiding escalatory spirals, there must exist a viable and mutually beneficial solution which is attainable through the prospect of cooperation. Otherwise, both sides would be resigned to a future of escalatory standoffs or cost- ly competition. Notably, this is where the dynamics of counter-intelligence and norm develop- ment diverge. Namely, espionage and counterintelligence have no other prospective solutions outside of tacit bargaining, absent the possibility of an intelligence-sharing treaty like the Unit- ed Kingdom – United States of America Agreement (UKUSA), also known as the “Five Eyes.” Without such agreements, practitioners typically accept costly competition and retrospectively define the boundaries of acceptable action by triggering escalatory standoffs. Whether the So- larWinds hack is such a trigger or just becomes another aspect of costly competition remains to be seen. Either way, on norm development, it may be easier to build cooperation on economic issues as the market may have already provided the prospect for such regarding IP-theft.

In his seminal work, The Evolution of Cooperation, Robert Axelrod notes that the prospect of continued engagement enables cooperation to develop; inversely, a perception that the PRC or US would soon collapse undermines motivation for either party to cooperate. Instead, each would simply exploit the other for as much as it can steal from the other before the game ends. Assuming neither party is on the verge of collapse, in an environment in which continuous engagement is to be expected, for a strategy to be collectively stable—that is, able to resist the invasion of competing strategies—the strategy must offer a higher rate of return than a compet- ing strategy. In other words, an international normative behavior must essentially be self-rein- forcing. This requires two sequential conditions:

1) The reciprocal benefits of IP protections must be more beneficial amongst cooperating parties, e.g. the like-minded nations in the G-20, than for them to participate in IP-theft against each other

2) For (1) to be true, those who protect and respect IP must be prepared to retaliate collec- tively against those that adopt IP-theft, to deny, reduce, or otherwise render prohibitively costly the stolen IP.[61]

In essence, retaliation for violations of an international norm should be multilateral. Not only would a multilateral effort relieve the US of solely bearing the costs of enforcement, multilat- eral condemnation of IP-theft would provide even greater legitimacy to any punitive actions inside or outside cyberspace, raising the credibility and scope of potential punishment for violations while constraining the PRC’s freedom of action to retaliate in kind.

While effective retaliation may deter future transgressions, the ability to return to a mutually cooperative state is as important.[62] Pundits may argue that communicating on such intentions is impossible due to issues of trust, but the economic market for justice may well have already provided the tacit evidence necessary to move nations and other entities towards a cooperative cyberspace and away from IP-theft. As Fareed Zakaria put it,

That China engages in rampant theft of intellectual property is a widely accepted fact—ex- cept among U.S. companies doing business in China. In a recent survey of such compa- nies conducted by the U.S.-China Business Council, intellectual property protection ranked sixth on a list of pressing concerns, down from number two in 2014. …Why this shift from 2014? That year, China created its first specialized courts to handle intellectual proper- ty cases. In 2015, foreign plaintiffs brought 63 cases in the Beijing Intellectual Property Court. The court ruled for the foreign firms in all 63.[63]

Since then, the IP caseload has grown rapidly. “In 2018 alone, Chinese courts received 301,278 new IP cases in the first instance, of which 287,795 were concluded. These figures represent an increase of 41 percent and 42 percent respectively compared to those for 2017.”[64] These include cases involving myriad American, Chinese, and other international companies.[65] Interestingly, ~79% of the cases brought before the court were purely PRC domestic cases,[66] with the remainder having foreign interests represented. In those latter cases, the court ruled in civil cases ~68% of the time in favor of foreign interests over domestic parties.[67]

Historical evidence points towards potential cooperation on intellectual property rights as well. As Yukon Huang and Jeremy Smith from the Carnegie Endowment for International Peace argue,

In terms of outright theft of IP, China’s infractions are anything but unique: It is just one of 36 violators listed in the 2019 Special 301 Report by the Office of the U.S. Trade Repre- sentative (USTR). Historically, rapidly growing emerging market economies tend to be cited as they transition to higher income levels. For example, decades ago Japan, South Korea, and Taiwan were each perennial Section 301 violators until they reached a per capita GDP of about $20,000-$25,000.[68]

Given the PRC’s per capita GDP is roughly $17,000 as of 2020,[69] this hypothesis will likely be tested in the near future.

Others are less optimistic about China’s IP-theft, noting that the US Trade Representative cites numerous cases and complaints in the office’s 2018 report on PRC IP-theft.[70] And Za- karia does not consider that many affected US businesses may be unaware that they were victims of such theft.[71] However, Zakaria does highlight the convergence of PRC interests, US pressure, and desired normative behavior by stating that,

reforms…are often undertaken only in the face of Western pressure and, even then, be- cause they serve China’s own competitive interests—the largest filer of patents worldwide last year was the Chinese telecommunications giant Huawei. But it is also true that many Chinese economists and senior policymakers have argued that the country will modernize and grow its economy only if it pursues further reform.[72]

While it may not be immediate, there certainly appears to be a prospect of cooperation that benefits both parties as the marginal gains from reciprocal IP protection outweigh the marginal gains from IP-theft as China’s economy matures.

Some claim that this was a fait accompli, that the Chinese economy was essentially able to mature because of the IP-theft over these past decades. This is perhaps true and it may have been a strategic failure of the US for not timely countering. However, it was not a failure of the US to envision an operational approach to cyberspace; tacit bargains without explicit bargains are unlikely to have been helpful; and tacit bargains in support of the explicit bargain, though some may have been potentially successful, would still run the risk of an escalatory spiral absent a perceived prospect of cooperation. Additionally, a multilateral effort to collaborate on punishing IP-theft and protecting the value of cybersecurity cooperation is still lacking. How to resolve the issues of retribution for past transgressions is beyond the scope of this article, which seeks to highlight the dynamics at play and explain why explicit bargains, the prospect of cooperation, and multilateral coordination outside of the cyberspace domain are important keys to developing international norms within cyberspace.

#### International entanglement and norm setting offers effective deterrent for malicious cyber activity- Estonia policy approach proves

**Parnik 22**

(Piret Parnik, researcher at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), “Cyber deterrence: A case study on Estonia’s policies and practice,” The European Centre of Excellence for Countering Hybrid Threats, October 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211012\_Hybrid\_CoE\_Paper\_8\_Cyber\_deterrence\_WEB.pdf, accessed 7/4/2022, GDI- TMK)

Participating in international cooperation (and in doing so, ensuring Estonia’s leading position in international cybersecurity issues) is expected to strengthen deterrence through entanglement and norm-setting. The interdependence and entanglement of cyberspace actors can have deterrent effects.26 When many countries abide by “the rules of the road” – international law, cyber norms and confidence-building measures – and act responsibly in cyberspace, it creates trust and stability. Countries are interdependent in cyberspace. For example, if one country were to target a public core of the internet (such as terrestrial and undersea cables, internet exchange points, and domain name system), such an attack would also impose serious costs on the attacker. In this case, interdependencies in cyberspace are likely to contribute to cyber deterrence because a potential attacker has something valuable to lose. For countries whose economic growth and political regime are highly dependent upon the internet, the prevailing interest is to ensure the stability of cyberspace.27 International cooperation on cybersecurity increases entanglement. Similarly to entanglement, norms “can deter actions by imposing reputational costs that can damage an actor’s soft power beyond the value gained from a given attack”.28 The multilateralization of cyber norms helps to raise the reputational costs of irresponsible state behaviour in cyberspace.29 As a small country, Estonia stresses the importance of upholding value- and rule-based international order, including democratic freedoms and human rights in cyberspace, which support Estonian security policy objectives. Small countries in particular benefit from the existence of international rule-based order, and from the extension of the rule of law to cyberspace.30 Estonia’s objective is therefore to establish that international law applies to cyberspace, and states must adhere to global cyber norms. It sees international cooperation and cyber diplomacy as being fundamental to domestic defence and resilience.31 In the country’s view, when states violate norms, they must be held responsible for these actions through collective public attribution and the imposition of response measures. Legal consequences must be imposed upon cyber norm violators.32 Through international cooperation and cyber diplomacy efforts, states will understand that they are interdependent and that cyberspace stability benefits everyone. Hence, responsible state behaviour is in everyone’s interests, which contributes to deterrence by entanglement. An example of entanglement comprises Estonia’s efforts since 2007 to put cybersecurity on the agenda of international and regional organizations (the EU, NATO, UN, OSCE, the Council of Europe, and Baltic and Nordic inter-governmental and parliamentary cooperation formats) on a regular basis. Likewise, Estonia has contributed over many years to the cybersecurity capacity-building of many EU and NATO partners and beyond, believing that this assistance contributes to international stability in cyberspace, and consequently deters malicious cyberattacks. Estonia stresses that sharing cybersecurity information and best practices increases mutual trust and stability in cyberspace, strengthening deterrence and defence.33 For Estonia, multi- and bilateral international cooperation is a primary means of achieving entanglement and norms-related objectives through whole-of-society and multi-stakeholder approaches. Publishing the government’s positions on how international law applies to cyberspace is aimed at influencing other states to adhere to responsible state behaviour in cyberspace.34 To strengthen its cyber diplomacy capacity, Estonia established a position in 2018 for an ambassador-at-large for cybersecurity. Estonia is one of the leaders among the Baltic and Nordic countries when it comes to cyber diplomacy. It has been a member of the UN Group of Governmental Experts for many years, and is also a leader in cyber diplomacy education for foreign diplomats.35 As a member of the UN Security Council in 2020– 2021, in June 2021 Estonia organized for the first time in the Council’s history an open meeting on cybersecurity, where it raised the issue of state behaviour in cyberspace in the context of international peace and security.36 Since 2008, Estonia has hosted the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), which sponsors the publication of world-renowned scholarly works on international law applicable to cyberspace – the Tallinn Manuals 1.0 (2013), 2.0 (2017), and the forthcoming volume 3.0.37

#### Internal link solvency – ICT allows cyberattacks on CBRN facilities – only cooperation and harmonisation at a regional level like the plan solves

**Farnelli**, PhD and Senior researcher in international law at University of Bologna, **2022**

(Gian Maria, “Chapter 31: New Technologies and CBRN Events: International Obligations in the Cybersecurity Domain,” International Law and Chemical, Biological, Radio-Nuclear (CBRN) Events: Towards an All-Hazards Approach, it’s a book, edited by de Guttry et al., 2022, Koninklijke Brill NV, accessed 7/1/2022, gdi-tmur)

\*ICT = Information and communication technology

\*CBRN = Chemical, Biological, Radio-Nuclear

Building upon the consideration that ‘[t]he expanding use of ICTs in critical infrastructures and industrial control systems creates new possibilities for disruption’,86 the chapter at hand has presented the reasons why cybersecurity has been at the forefront of policymakers’ minds since the early 21st Century. States and international bodies have increasingly addressed the issue at hand, with a view to preventing malicious uses of ICT inconsistent with the collective interest in the maintenance of international peace and security.

The present analysis has also addressed the ongoing debate over the application of international obligations to activities in cyberspace. It is commonly accepted that existing international law applies in cyberspace without the need to develop a new legal instrument. However, technical difficulties in attributing conduct in cyberspace make the application of secondary rules on State responsibility difficult, leaving space for ‘malicious cyber operations without an author’.

Against this background, applying existing international due diligence obligations to ICT over which a State exercises jurisdiction appears reasonable. This would arguably mitigate the risk and the effect of malicious cyber activities targeting critical infrastructure, and provide the territorial State with legitimate reasons to exercise proportionate monitoring activities on data flows. Moreover, such approach would provide the victim State with a liable party from whom to seek compensation, absent a clear attribution of the cyber operation.

It has been argued that the application of existing obligations of due diligence, eg those stemming from the customary no harm rule, to highly ICT-dependent CBRN facilities requires the territorial State to exercise control over the appropriateness of the cybersecurity standards of any CBRN facility, irrespective of its private or public nature, with a view to fostering the prevention of CBRN events.

Following this line of reasoning, no new international legal instrument is necessary to require States to adopt cybersecurity regulations and strategies. Indeed, current international law concerning the prevention of harm and mitigation of consequences thereof may be easily construed as encompassing prevention of malicious cyber activities – ie cybersecurity. Moreover, the above line of reasoning would ground the assessment by existing compliance review mechanisms of the ‘appropriateness’ of States’ cybersecurity strategies and plans, insofar as their inadequacy could generate a harmful event triggering States’ liability under relevant international disaster, environmental or human rights law. However, the ‘transboundary nature’ of ICT implies that no State can tackle cyber-related issues alone. Initiatives aimed at fostering cooperation and harmonisation, in particular at a regional level,87 are surely desirable and called for.

### Tacit bargaining/informal norm development fails – escalation

#### Tacit bargaining and norm development risks escalatory environment and bad norms

**Kim ‘22**

(Wonny K. Kim, Innovation and Information Operations Officer in the U.S. Army Reserve 75th Innovation Command, Master of International Affairs from Columbia University, Master of Science in Technical Intelligence from National Intelligence University, and B.A. in Philosophy and Psychology from Binghamton University, ““Explicit” Bargains are Essential to Forming Desired Norms in Cyberspace,” Cyber Defense Review, Spring 2022, JSTOR, accessed 6/30/22, GDI- TMK)

WHY EXPLICIT BARGAINING IN CYBERSPACE IS NECESSARY

These new interactions, in the form of tacit bargaining, have become embodied in DoD’s 2018 Cyber Strategy as a way to contest malicious cyber activity. Countering “cyber cam- paigns threatening U.S. military advantage by defending forward to intercept and halt cyber threats and by strengthening the cybersecurity of systems and networks that support DoD missions.”[35] As Fischerkeller and Harknett explain it:

By describing persistent engagement, operationally, as continuously engaging and contest- ing adversaries and maneuvering for advantage below the threshold of armed conflict … it is reasonable to conclude that persistent engagement would support a strategic process of tacit bargaining adopted to develop mutual understandings with adversaries on accept- able/unacceptable behavior in agreed competition.[36]

Notionally, then, U.S Cyber Command (USCYBERCOM) would engage and contest adversar- ies conducting espionage in cyberspace for economic gain and thereby counter with conse- quences this unacceptable behavior. However, tacit bargaining in foreign networks, absent explicit bargains, risks establishing stable yet undesirable normative behavior.[37] Instead of the “open, reliable, and secure” cyberspace envisioned by the US strategy, this risks leaving the US vulnerable to costly escalatory spirals.

Escalatory Spirals

Escalatory spirals spawned by cyberspace actions have already occurred. Examples include Iran accelerating its cyber development and deployment following the attack on its uranium enrichment centrifuges (Stuxnet attack[38],[39]), and Russia’s claim that it was simply respond- ing in kind through cyber means to the Panama papers release.[40] Predicated on whether cy- berspace becomes truly offense-dominant or defense-dominant as the domain matures,[41] two types of escalatory spirals may occur in cyberspace:

1) A spiral that leads to a standoff with the potential to breach the limits of “competition short of armed conflict”[42]

2) A spiral that stabilizes as marginal costs eventually match marginal gains in a costly competition.[43]

In either case, at least in regards to IP-theft, both of these options are less desirable than a US-PRC agreement to reciprocate on IP protection and cooperate on combating the economic threat of cyber-crime which was the envisioned state of relations in the 2015 accord.

### Tacit bargaining/informal norm development fails – no enforcement

#### Enforcement of tacit norms fail – lack of consistent application and signaling means no behavior change and risks escalation

**Kim ‘22**

(Wonny K. Kim, Innovation and Information Operations Officer in the U.S. Army Reserve 75th Innovation Command, Master of International Affairs from Columbia University, Master of Science in Technical Intelligence from National Intelligence University, and B.A. in Philosophy and Psychology from Binghamton University, ““Explicit” Bargains are Essential to Forming Desired Norms in Cyberspace,” Cyber Defense Review, Spring 2022, JSTOR, accessed 6/30/22, GDI- TMK)

In lieu of an explicit agreement, consider if USCYBERCOM had engaged in tacit actions to punish and thereby compel the PRC to cease its IP-theft. US experience with economic sanc- tions has proven the importance of focusing efforts on the appropriate targets and communi- cate the desired behavior change.[44] As such, USCYBERCOM’s two likely targets would be

1) Those who authorize and conduct state espionage in cyberspace, as well as the abetting network infrastructure (PRC cyberspace state espionage)

2) Those that receive and exploit the stolen IP (IP-theft recipients).

Targeting PRC cyberspace state espionage

While disrupting or degrading the PRC’s IP-theft enabling infrastructure is appealing, this approach is likely to be unhelpful for norm formation because the US is faced with a “Cheap Talk” dilemma of its own. This is because the US is motivated to disrupt or degrade this target for counterintelligence against espionage writ-large.[45] Even if explanatory commu- nications accompany the counter-action and give IP-theft as the reason why it was imposed, there is no reason for the PRC to trust that these actions would end as the US benefits from the disruption. Furthermore, as the PRC would most likely not resume espionage from a network that is known to be compromised, there is no value proposition for the PRC to have the US cease its disruption or degradation activities. This is the antithesis for driving desired behavior change since it is necessary that the adversary sees both the prospect and value in the punishment ending when the egregious IP-theft behavior ends.[46] Tacit bargaining in this situation exacerbates the trust dilemma, not alleviates it. Instead, the US incurs ongoing manpower and resource costs to defend forward in order to suppress IP-theft, and the US and PRC are embroiled in an escalatory spiral in pursuit of marginal advantages over each other. As such, tacit bargaining, even with explanatory communications, contributes little to the development of the desired norm.

If the US could effectively disable all PRC espionage, that would eliminate IP-theft, but that is unrealistic. Again, the Iranian response to Stuxnet shows that an escalatory spiral is invariably in the offing given the low barrier to entry into cyberspace.[47] Even DoD acknowl- edges the futility of attempting to achieve total dominance.[48]

### Tacit bargaining/informal norm development fails – retaliation fails

#### Retaliation for IP theft absent explicit bargaining and agreement limited deterrent effect – minimize norm development and risk retaliation

**Kim ‘22**

(Wonny K. Kim, Innovation and Information Operations Officer in the U.S. Army Reserve 75th Innovation Command, Master of International Affairs from Columbia University, Master of Science in Technical Intelligence from National Intelligence University, and B.A. in Philosophy and Psychology from Binghamton University, ““Explicit” Bargains are Essential to Forming Desired Norms in Cyberspace,” Cyber Defense Review, Spring 2022, JSTOR, accessed 6/30/22, GDI- TMK)

Targeting IP-theft recipients

Turning to the second set of targets, the IP-theft recipients, the US has followed “a two-pronged approach to combat economic espionage: (1) reducing theft by educating and training the pri- vate sector how to improve security and safeguard secrets,[49] and (2) federally prosecuting offenders.”[50] This latter approach has yielded a mixed bag[51] with few convictions under the 1996 Economic Espionage Act,[52] none involving cyber espionage. Considering that IP-theft continues to plague the US at enormous scale,[53] prosecuting offenders does not seem to have effectively stemmed or deterred cyber-enabled IP-theft, anecdotal arguments to the contrary notwithstanding.[54] Whether US actions targeting non-cyber actors, including the Department of Justice’s recently concluded China Initiative,[55] are successful at reducing espionage is outside the scope of this article.

A potential third US option is to threaten US cyberspace retaliation against businesses that exploit stolen US IP. This is likely to have some deterrent effect on IP-theft recipients’ behavior. Examples of such potential punitive actions abound, from denial-of-service attacks against network infrastructure to malware akin to NotPetya[56] or high-profile ransomware attacks.[57] However, without an explicit bargain, these actions invite tit-for-tat reciprocal responses against US economic targets. Even if we assume that attribution for these actions makes them discernible from the background noise of cybercrime, without an explicit bar- gain, any US claim to legitimacy for its tacit actions is severely weakened, especially con- sidering these actions would be conducted on foreign networks outside of US sovereignty. This greatly diminishes the value to normative behavior formation and lowers the barrier for retaliatory PRC action. Absent the explicit agreement, the PRC can simply claim the US vio- lated their sovereign networks and reciprocate in kind. As such, prosecuting this target set with tacit actions in cyberspace also carries the potential for an escalatory spiral, not unlike the current US-PRC trade-war. The solution must include consideration for PRC domestic enforcement, which manifests in the prospect for cooperation discussed later herein.

### Explicit bargaining solves – behavioral convergence

#### Behavioral convergence around limitations only way to create sustainable cyber norms

**Kim ‘22**

(Wonny K. Kim, Innovation and Information Operations Officer in the U.S. Army Reserve 75th Innovation Command, Master of International Affairs from Columbia University, Master of Science in Technical Intelligence from National Intelligence University, and B.A. in Philosophy and Psychology from Binghamton University, ““Explicit” Bargains are Essential to Forming Desired Norms in Cyberspace,” Cyber Defense Review, Spring 2022, JSTOR, accessed 6/30/22, GDI- TMK)

Prospect of Punishment and Retaliation

Tacit bargains without explicit bargains risk escalatory spirals; explicit bargains need to be enforced. Had USCYBERCOM and other US agencies acted in defense of the 2015 U.S.– China Cyber Agreement by imposing punitive actions in response to PRC transgressions, this punishment would have helped to deter future transgressions.[58] Even Fischerkeller and Harknett support the dual importance of explicit and tacit bargains when they advocate for “an aligned application of them to the strategic realities the United States faces.”[59] They write further:

The success of a strategic framework for constructing cyber norms grounded in per- sistent engagement and tacit bargaining will depend, in part, on how well states commu- nicate their national interests in cyberspace. Behavioral convergence around definable limitations is how sustainable cyber norms can be constructed.[60]

Those communicated defined limitations are the basis for explicit bargains, which confer legitimacy on retaliatory action; the prospect of retaliatory action and ensuing escalatory spirals supports behavioral convergence. This is where we see the convergence of explicit and tacit bargains. Even in the relatively benign costly competition scenario, the level of competition tacit bargaining will spawn will always be less desirable than a cyberspace characterized by cooperation. The US’s failure to respond to PRC violations unfortunately, but predictably, emboldened PRC exploitation. However, while it becomes evident that ex- plicit bargains and tacit enforcement are both necessary, this argument also leads to another question in the shadow of a potential escalatory spiral: what happens if the PRC reciprocates in kind against punishment, despite an explicit bargain? This question highlights the impor- tance of the prospect of cooperation.

### AT norms can’t be enforced

#### Explicit frameworks enable enforcement – lack of explicit bargaining reason for SQuo failures – 2015 China Agreement proves

**Kim ‘22**

(Wonny K. Kim, Innovation and Information Operations Officer in the U.S. Army Reserve 75th Innovation Command, Master of International Affairs from Columbia University, Master of Science in Technical Intelligence from National Intelligence University, and B.A. in Philosophy and Psychology from Binghamton University, ““Explicit” Bargains are Essential to Forming Desired Norms in Cyberspace,” Cyber Defense Review, Spring 2022, JSTOR, accessed 6/30/22, GDI- TMK)

The 2015 U.S.–China Cyber Agreement states that “the United States and China agree that neither country’s government will conduct or knowingly support cyber-enabled theft of intel- lectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.”[18] The par- ties also pledged to investigate and mitigate malicious cyber activities emanating from their respective territories, and to support development of “appropriate norms of state behavior in cyberspace.”[19] Post-accord, similar agreements were made between the PRC and other G-20 members.[20] Yet the PRC’s active theft of IP have since continued.[21]

Continued IP theft has led Dr. Michael P. Fischerkeller of the Institute for Defense Analyses and Dr. Richard J. Harknett of the University of Cincinnati to argue that explicit bargaining, which involves “international conference or bilateral diplomacy and treaty negotiations,”[22] has significant limitations in the cyber domain because participants would not “trust the other to any agreement explicitly reached.”[23] They write:

Consider, for example, the 2015 agreement Presidents Obama and Xi, which committed that neither country would conduct or knowingly support cyber-enabled theft of intellectu- al property for commercial gain. … This explicit agreement failed not because of any deficit in U.S. diplomatic bargaining skills, but because the bargaining process itself was not ap- propriate for the strategic competitive space to which it was applied.[24]

Instead, Fischerkeller and Harknett urge the use of tacit bargaining to develop normative be- havior in cyberspace. Tacit bargains are defined by Schelling as “informal agreements.arrived at ‘not by verbal bargaining, but by maneuver, by actions, and by statements and declarations that are not direct communication to the enemy.’”[25]

It is important to recognize that these two processes are not mutually exclusive. If the US had responded to violations of the U.S.–China Cyber Agreement[26] with more than mere words,[27],[28],[29] for example, with palpable actions against IP-theft recipients, the accord may have established an international norm and deterred future transgressions. Moreover, respons- es would not have had to be constrained to cyberspace: threat of economic sanctions is what compelled the PRC to enter into the accord in the first place.[30] Failure of the explicit bargain was not due to any structural realities of cyberspace, but, rather, to “Cheap Talk;”[31] the un- derlying potential payoffs for the PRC decision calculus ran counter to the explicit agreement. Xi had reason to convince Obama that it was in the PRC’s interests and intentions to respect IP, yet the PRC’s benefits from violating the agreement outweighed the prospective marginal cost, particularly if the prospect of US follow-through on the threat of sanctions diminished. As US enforcement of the agreement lagged,[32] the prospect of punishment diminished, and the calculus shifted in favor of IP-theft. Alternatively, the PRC may have perceived the prospective value of economic cooperation diminishing, given difficult trade negotiations throughout 2017- 2018.[33] Either way, if actors are believed to be rational, trust in the agreement failed because interests were no longer aligned. The take away lesson should have been to enforce agree- ments, not necessarily that new interactions[34] in cyberspace are required to develop norms.

## Cyber signaling

### Cyber signaling – de-escalation

#### Cyber actions provide accommodative signaling that de-escalates conflict – limited effects and ambiguous responsibility allows actions to demonstrate resolve without escalation

**Lonergan**, assistant professor at the Army Cyber Institute at the US Military Academy, and **Lonergan**, senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers, **2022**

[Erica and Shawn, “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises”, Security Studies, 18 Feb 2022, Taylor and Francis, accessed July 1, 2022, JCP-LL]

Signaling is a core element of international crisis bargaining and coercive diplomacy. To succeed in crises, states must convey to targets that they possess the capability to impose an advantageous outcome and that they are resolved to do so, while also managing the risks of unintended escal- ation and war.1 Much of the traditional signaling literature focuses on how to communicate resolve through costly signaling.2 Beyond resolve, states can also signal capabilities through brandishing them or conducting mili- tary demonstrations.3 Less studied in the signaling literature is how states can use signals to manage escalation risks or de-escalate crises. However, as Glenn H. Snyder and Paul Diesing note, even during crises where one side seeks to maximize its strategic objectives, it will also seek to reduce escal- ation risks.4

Despite the prevalence of cyber operations in contemporary international crises, there is nascent theoretical and empirical work on how cyberattacks shape crisis dynamics and, in particular, the different ways such attacks could function as signals.5 In this article, we develop and test a theory of cyber signaling. We argue that, in some crisis contexts—particularly those where leaders are simultaneously managing domestic political pressure to take a harder stance and the desire to avoid escalatory actions—cyber oper- ations have a distinct utility for what Snyder and Diesing term “accommodative” signaling.6 This is due to two important characteristics. First, cyber operations generate limited effects relative to other capabilities, so their use could demonstrate a willingness to avoid more costly actions that increase escalation risks. Second, the plausibly deniable nature of cyber operations allows states to placate nationalist constituencies, typically through permitting proxy groups to conduct low-cost attacks, while exploit- ing ambiguities about state responsibility. In other words, cyber operations as accommodative signals work for many of the same reasons that they fail as coercive signals: they do not hurt and they are ambiguous.

To test our argument, we explore how states use cyber operations during international crises across five case studies that vary in the presence or absence, as well as the nature of, cyber operations during a crisis. We find strong evidence to support our claim that states sometimes choose to use cyber operations for signaling purposes and that certain types of cyber operations can act as accommodative signals. We also find that accommo- dative cyber signals are correlated with crisis de-escalation, although further research is needed to substantiate a causal link. Nevertheless, our analysis offers a plausible explanation for recent empirical findings that cyber oper- ations are not associated with escalation.7

### Cyber signaling – resolve and accommodation

#### Cyber actions signal resolve and accommodation – clear communication about consequences key

**Lonergan**, assistant professor at the Army Cyber Institute at the US Military Academy, and **Lonergan**, senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers, **2022**

[Erica and Shawn, “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises”, Security Studies, 18 Feb 2022, Taylor and Francis, accessed July 1, 2022, JCP-LL]

Signaling in International Politics

Signals involve statements (literal messages) or actions (military maneuvers) meant to shape the target’s image of the signaling state.8 Signals often rely on implied, mutual understandings about the meaning behind statements or actions; and actions in particular are often coupled with messages.9 Signaling is foundational to theories of coercion and crisis bargaining because it helps states shape the perceptions and, ultimately, behavior of an opponent. Successful coercion rests on clearly communicating to a target what the coercing state expects of it—if you do X, then Y will follow.10 And the target must perceive the message to be credible rather than merely “cheap talk.”11

The bulk of the signaling literature focuses on how states can make their signals credible through conveying resolve.12 However, we argue that cyber operations are often used as signals of accommodation—not just resolve. Moreover, to understand cyber signaling, the signaling literature on accom- modation and the role of secrecy is particularly important.13 Our theory of cyber signaling merges and builds on these to present a framework for how cyber operations could function as accommodative signals.

### Cyber signaling – de-escalation solvency

#### Mitigating the risks of war and de-escalation of future risk result from accommodative signaling – reinforces coercive signaling

**Lonergan**, assistant professor at the Army Cyber Institute at the US Military Academy, and **Lonergan**, senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers, **2022**

[Erica and Shawn, “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises”, Security Studies, 18 Feb 2022, Taylor and Francis, accessed July 1, 2022, JCP-LL]

Signaling for Resolve Versus Accommodation

Snyder and Diesing’s foundational work on coercive diplomacy emphasizes that almost all international crises contain elements of both coercion and accommodation.14 For accommodation, resolve is less imperative than more conciliatory signaling objectives, such as willingness to make conces- sions, compromise, save face, and avoid war.15 Crisis management, as Snyder and Diesing define it, entails ensuring a state can achieve its stra- tegic interests and mitigate potential risks of escalation. The challenge “is to find the optimum mix or trade-off between coercion and accommoda- tion in the particular crisis context, given the distribution of values and military power among the participants.”16

The distinction between coercion and accommodation rests on the rela- tive emphasis on “winning” versus mitigating the risks of war. Coercion weighs the former more heavily, whereas accommodation seeks to “reach some settlement that promises to defuse the issue as a potential source of future crises”—without making too many painful concessions.17 Nevertheless, each contains elements of the other; coercive strategies may include accommodative tactics meant to address controlling escalation risks, and accommodative strategies may include coercive tactics that seek to minimize losses.18 Characteristics of accommodative actions include demonstrating restraint, information sharing, clarifying shared expectations and norms regarding limits on conflict, or creating space for negotiations and diplomacy.19 Accommodative signaling is linked to crisis de-escalation because the former can enable the latter. Even a “controlled reprisal” that is less escalatory than the prior action could prompt both sides to de-escalate.20

### AT cyber signaling fails –lack of attribution

#### Secret signaling manages escalation -

**Lonergan**, assistant professor at the Army Cyber Institute at the US Military Academy, and **Lonergan**, senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers, **2022**

[Erica and Shawn, “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises”, Security Studies, 18 Feb 2022, Taylor and Francis, accessed July 1, 2022, JCP-LL]

Public Versus Secret Signaling

Much of the signaling literature assumes signaling occurs in the open to enhance its credibility, whereas private talk is “cheap talk.”21 However, secret signaling can also be an effective tool of escalation management. Synder and Diesing explicitly link the decision to signal in public or private with coercive versus accommodative strategies. Although they argue that public threats may enhance credibility, such threats also increase escalation risks through creating mutual public commitments and invoking prestige. Conversely, private threats enable risk avoidance because they are more deniable. Similarly, private communication increases the probability of a peaceful settlement but also reduces the chances that any one actor will maximize its own objectives.22 Therefore, Snyder and Diesing posit that private communication generally lends itself to accommodative strategies and public communication lends itself to coercive strategies.23 Recent research uncovers similar findings: privacy and secrecy can enable signalers to save face, avoid paying potential domestic costs, and reduce escal- ation risks.24

### Cyber signaling – secrecy solves

#### Secrecy of cyberspace action support accommodative signaling to de-escalate crisis

**Lonergan**, assistant professor at the Army Cyber Institute at the US Military Academy, and **Lonergan**, senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers, **2022**

[Erica and Shawn, “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises”, Security Studies, 18 Feb 2022, Taylor and Francis, accessed July 1, 2022, JCP-LL]

What Is Cyber Signaling Good For?

Academic research finds that cyber operations have limited utility for sig- naling resolve.25 However, there is little research on the role of cyber oper- ations as accommodative signals.26 Brandon Valeriano and Benjamin Jensen argue that cyber operations may provide “a means of signaling future escalation risk as well as a cross-domain release valve for crises. Rival states use cyber operations as a substitute for riskier military oper- ations.” Drawing on their prior empirical findings about the relative absence of meaningful escalation dynamics in cyberspace, Valeriano and Jensen suggest this could be because cyber operations “offer great powers escalatory offramps.”27 We build a theoretical framework for why and under what conditions signaling in cyberspace could serve accommodative purposes. Specifically, we argue that the same factors that make cyber oper- ations suboptimal as costly signals of resolve also make them good for sig- naling for accommodation, especially the relatively limited effects cyber operations cause and their plausibly deniable nature. Moreover, we contend that states can strategically leverage one of these important aspects of cyberspace—secrecy—to support accommodative strategies.

#### Attribution and plausible deniability allow states to choose to level of secrecy – opening up space for placating constituencies and negotiating

**Lonergan**, assistant professor at the Army Cyber Institute at the US Military Academy, and **Lonergan**, senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers, **2022**

[Erica and Shawn, “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises”, Security Studies, 18 Feb 2022, Taylor and Francis, accessed July 1, 2022, JCP-LL]

Implications of the Strategic Use of Secrecy for Signaling

However, the effects of cyber operations alone do not offer a complete explanation of how cyber tools could function as accommodative signals. We argue that, in addition to effects, how states choose to take advantage of opportunities for more or less secrecy and ambiguity surrounding their conduct of cyber operations also plays a signaling role. For this aspect of our argument, there are two types of audiences for the signal: the adversary regime and domestic constituencies observing the government conducting or permitting a cyber action during a crisis. Moreover, the deliberate manipulation of secrecy is dyadic—both the signaling state and the target make choices during a crisis about the visibility of the cyber operation itself and the extent to which it is linked to the government.

Secrecy can manifest in different ways in cyberspace. For instance, main- taining secrecy about the cyber operation itself can be a condition for its success. Revealing information about how a state has gained access to a tar- get, as well as a state’s tool kit (especially if highly tailored), prior to or during the course of an operation can negate its efficacy because it permits defenders to take concrete steps to render the threat inert.55 However, our argument focuses on a different form of secrecy: attribution and plausible deniability in cyber operations.56 In a technical sense, cyberspace enables actors to conceal their responsibility for cyberattacks because it facilitates the obfuscation of points of departure for attacks.57 These technical meth- ods could also be coupled with deliberate efforts to obscure command and control for cyberattacks, such as employing cyber proxies with varying degrees of connection to the state to conduct offensive operations on the latter’s behalf.58 How much direct control governments exert over cyber proxies varies. For instance, governments could co-opt unwitting proxy actors—for example, by distributing malware in patriotic hacker forums (as occurred during the Russian-Georgian conflict in 2008). Or they could establish more direct relationships with groups that knowingly act on their behalf (e.g., the relationship between Russian intelligence agencies and the group known as “Fancy Bear.”).59

In relatively rare instances, some states have taken responsibility for their own cyber operations. Examples include US Cyber Command acknowledg- ing in December 2021 that it had conducted operations to counter ransom- ware groups; the September 2017 leak by a senior official in the Trump administration that the US Cyber Command had conducted a sustained DDoS attack against North Korea’s Reconnaissance General Bureau; and, during the Obama administration, Secretary of Defense Ash Carter’s com- ments in a February 2016 press conference acknowledging a US role in cyberattacks against the Islamic State in Mosul.60

Avoiding attribution is a strategic choice, not an operational require- ment.61 Therefore, the extent to which states are public or private about their role in cyber operations has signaling implications. Whereas some lit- erature contends that the plausible deniability of cyber operations increases escalation risks, we hypothesize that the opposite is true.62 In this sense, our argument is a twist on prior theories positing that secret signaling can widen the bargaining space between states, allowing for crisis resolution. We argue that, distinct from perfect secrecy, the ambiguities of cyber oper- ations that straddle public and secret realms—visible, but with uncertainty about responsibility or command and control—create opportunities for states to simultaneously signal to multiple audiences (domestic publics and the adversary). This allows governments to be perceived at home as making some response to an adversary during a crisis while ensuring the adversary perceives that the action’s effects are relatively minor or proportionate to avoid further escalation. Moreover, this also presents the adversary with a choice to allow the ambiguous status quo to persist, or to ratchet up the crisis by directly calling out the opposing side. Table 1 depicts some hypothesized implications for crisis dynamics.63

As depicted in the top left cell of Table 1, during a crisis the target of a cyberattack may choose to preserve plausible deniability—even when it has some degree of confidence that its rival is responsible—to prevent further escalation. Adversaries can implicitly convey a mutual interest in maintain- ing stability. In other words, the strategic choice to not go public, or even to issue vague and ambiguous public statements in response to a cyberat- tack, can also act as an accommodative signal. This is especially likely if the target perceives political dynamics domestically or within the rival state (e.g., nationalist protests or hawkish veto players) that may increase the risks of unwanted escalation. Conversely, if one party goes public with attribution while the other seeks to maintain plausible deniability, it can be more difficult for the other side to offer concessions. Finally, if attribution is mutually made public, it is unlikely that cyber operations can act as accommodative signals because both sides will perceive less of an advantage in appearing to back down.

### Cyber signaling – limited effects solve escalation

#### Limited effects and secrecy make cyber signaling possible – de-escalates by signaling to adversary and domestic constituencies – secrecy provides choices for governments to signal accommodations

**Lonergan**, assistant professor at the Army Cyber Institute at the US Military Academy, and **Lonergan**, senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers, **2022**

[Erica and Shawn, “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises”, Security Studies, 18 Feb 2022, Taylor and Francis, accessed July 1, 2022, JCP-LL]

Characteristics of Cyberspace for Accommodative Signaling

There are two sets of audiences for accommodative cyber signaling: the adversary government and domestic constituencies on both sides. In this context, two core characteristics of cyber operations make them useful for accommodative signaling: their relatively limited effects and the role of secrecy.28 First, the relatively minimal effects of some types of cyber opera- tions can signal restraint to an adversary. Second, in crises where neither party seeks escalation but there is domestic political pressure for the gov- ernment to take a more aggressive stance, the plausibly deniable nature of some cyber operations allows leaders to placate hawkish domestic constitu- encies by responding while avoiding more strident actions that might trig- ger escalation. Moreover, ambiguity surrounding the level of state responsibility allows leaders to “test the waters” with the other side, assess- ing the adversary’s willingness to avoid assigning responsibility to the gov- ernment and therefore refraining from further stoking nationalist sentiments.

In this sense, our argument about secrecy differs from existing work on secret signaling. In cyberspace, there can be a middle ground between purely covert cyber actions that are only observed by the target (if at all) and public operations for which a government takes responsibility.29 It is precisely through these noisy, ambiguous, and low-cost cyberattacks that accommodative signaling can occur. In other words, in addition to a cyber operation’s effects, the level of secrecy surrounding a cyber operation is a choice states make; and the decision by both parties to maintain plausible deniability can signal accommodation.

#### Magnitude of cyber operations impact signaling – permanence, scope, criticality of target and level of harm determine

**Lonergan**, assistant professor at the Army Cyber Institute at the US Military Academy, and **Lonergan**, senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers, **2022**

[Erica and Shawn, “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises”, Security Studies, 18 Feb 2022, Taylor and Francis, accessed July 1, 2022, JCP-LL]

The Strategic Effects of Cyber Operations

Cyber operations encompass a range of activity that occurs in the digital realm, including gaining access to computer networks for the purposes of exfiltrating sensitive information (cyber espionage); disrupting, degrading, destroying, or manipulating data that resides in or transits through a net- work, or the system itself (cyberattacks); or weaponizing sensitive or private information to influence an audience’s perception (cyber-enabled information operations).30 In this article, we focus on cyberattacks and exclude cyber espionage and cyber-enabled information operations.31

We argue that the magnitude of the effects of cyber operations affects their signaling potential. Therefore, to measure the effects of cyber opera- tions, we identify four areas: the permanence of the effects; the scope of the operation; the criticality of the target; and the level of harm. We focus on strategic-level effects because these pertain to how cyber operations influence broader crisis dynamics.

We operationalize the permanence of effects as the target’s relative ease and speed of recovery. A related aspect is the reversibility of the effects of a cyber operation.32 The most straightforward type of impermanent cyber operation is a distributed denial of service (DDoS) attack, which disrupts a network’s functioning by overwhelming the target’s processing capacity (typically through jamming its bandwidth via the sheer volume of requests) but does not cause lasting damage.33 For example, the 2016 the Mirai Internet of Things (IoT) botnet launched a massive wave of DDoS attacks that infected six hundred thousand IoT devices but only caused a tempor- ary interruption in service.34

However, even beyond DDoS attacks, many cyber operations “produce relatively transient and/or reversible effects.”35 Even for operations that des- troy data, capabilities and functions can often be reconstituted within a relatively short period of time.36 After the North Korean cyberattacks against South Korean banks and Sony Pictures in 2013—both of which destroyed files and damaged computers—the targets “are still in business, and none spent more than an inconsequential amount of time recov- ering.”37 In contrast, some cyber operations produce longer-term or even permanent effects, such as the Stuxnet computer worm discovered in 2010 that caused permanent, physical damage to Iranian centrifuges.38

A cyber operation’s scope addresses the range of targets against which it delivers an effect. Some cyber capabilities may widely proliferate across net- works but only produce effects against the specific systems that are vulner- able to them.39 Because cyber capabilities are comprised of computer code written to produce some kind of effect against another computer, they can- not be employed against just any desired target.40 For example, although Stuxnet was discovered in computers around the world, it only caused destructive effects against the centrifuges in Natanz.41 In contrast, whereas the 2017 WannaCry ransomware attack, attributed to North Korea’s Lazarus Group, only affected systems running a version of Windows 7, the scope was nevertheless wide, as it affected hundreds of thousands of com- puters globally across a range of industries that were running the older software.42

The criticality of the target, at the strategic level, is a function of how vital the government perceives that target to be. In the most extreme case this could be regime survival, but it also includes core national and eco- nomic security interests. How a particular government defines criticality for specific entities varies. For instance, the infrastructure that enables authori- tarian governments to control data that ingresses and egresses across sover- eign digital borders and to surveil domestic populations may be a critical target for those regimes but is less relevant for open societies.43

Finally, an essential aspect of cyber operations’ strategic effects is the level of harm to the target. Most malicious cyber activity to date has not risen to a threshold of significant harm, violent effects, or loss of life.44 This is especially the case when compared to other military capabilities.45 That said, there are different ways to operationalize level of harm. One potential metric is loss of life. To date, no one has reportedly died as a dir- ect result of a cyberattack, despite over thirty years of recorded cyber oper- ations.46 Even in hypothetical catastrophic scenarios, the cost in terms of human casualties is relatively low compared to other military capabilities. For instance, a common worst-case scenario is a cyberattack on a power grid.47 However, the 2015 Russian cyberattack against Ukraine’s power grid, the first known example of an offensive cyber operation targeting a state’s power grid, did not lead to any reported casualties.48

It is also possible to measure the harm cyber operations inflict in treas- ure rather than blood. According to this metric, the financial or economic costs of cyberattacks are significant. For example, the total cost of the most expensive cyberattack in history, the 2017 NotPetya attack, is estimated at $10 billion.49 However, governments have largely avoided characterizing these operations as crossing an “act of war” or “use of force” threshold.50 While still of strategic consequence, cyber operations (especially absent physical violence) appear to be perceived differently than other military operations.51

### Cyber signaling – alternative to kinetic attacks

#### Cyber effects provide alternative to kinetic physical attacks – and de-escalate conflicts

**Lonergan**, assistant professor at the Army Cyber Institute at the US Military Academy, and **Lonergan**, senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers, **2022**

[Erica and Shawn, “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises”, Security Studies, 18 Feb 2022, Taylor and Francis, accessed July 1, 2022, JCP-LL]

Given different approaches, we chose to measure level of harm in terms of the target state’s perception of a cyber operation’s national security con- sequences. Perception may not perfectly align with the objective human or economic costs. For instance, the SolarWinds supply chain breach, revealed in December 2020, compromised many US federal government and private sector networks but did not cause loss of life.52 Nevertheless, the US gov- ernment chose to activate the response process outlined in Presidential Policy Directive 41, which applies to cyber incidents that rise to a certain level of significance.53 This example illustrates how the perceived level of harm ultimately is a political or strategic assessment, rather than an object- ive measure of calculatable damage.

Taken together, the strategic effects of most cyber operations are rela- tively limited when compared to other types of military operations. That said, different types of cyber operations vary in their level of effects. These two points have implications for accommodative signaling. Specifically, in the context of an international crisis, the relative effects of a cyber oper- ation inform how the adversary perceives the intent behind the signal.54 In this sense, the key audience for a cyber operation’s effects is the adversary government. Because cyber operations lack the physical violence and per- manent destruction associated with other military capabilities—and may even be less painful than some economic instruments, such as sanctions— they could signal restraint relative to other options. Moreover, the choice of a disruptive cyber operation that has temporary effects, in comparison to a destructive cyber operation with longer-term effects, could also send an accommodative signal. The sequencing of the cyber operation could also inform its interpretation. For instance, if a cyberattack follows a kinetic one, it could be perceived as a de-escalatory choice.

### Prodict – Lonergan and Lonergan methodology

#### Methodology for case studies

**Lonergan**, assistant professor at the Army Cyber Institute at the US Military Academy, and **Lonergan**, senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers, **2022**

[Erica and Shawn, “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises”, Security Studies, 18 Feb 2022, Taylor and Francis, accessed July 1, 2022, JCP-LL]

Case Studies

We evaluate the conditions under which states choose to employ cyber operations for signaling purposes during international crises, as well as the differences between cyber operations for accommodative signaling or for resolve or deterrence, across five crises: the 2012 Senkaku/Diaoyu Islands dispute between China and Japan; the 2015 crisis between Turkey and Russia after Turkey downed a Russian jet during the Syrian civil war; the 2019 crisis over the Strait of Hormuz between the United States and Iran; the crisis precipitated by China’s 2013 declaration of an Air Defense Identification Zone (ADIZ); and the 2018 crisis between Russia and the United States when proxy forces affiliated with the Russian government attacked American forces in Syria.

To select these cases, we reviewed four datasets comprising hundreds of cyber incidents from 1999 through June 2020 to identify those where cyber operations occurred during a geopolitical crisis. We also examined major think tank reports, policy reports, and news media pertaining to cyber inci- dents.65 We specifically looked for crises where a contested political issue was present (e.g., a dispute over territory or a perceived political threat to a regime) that raised the risk that military hostilities may take place and where the trigger of the crisis was not a cyber event but, rather, a broader political issue.66 The vast majority of observed cyber behavior associated with nation-states occurs outside of the context of international crises.67

### AT: cyber operations escalate

#### Cyber operations in a crisis do not lead to escalation – either reciprocal action or de-escalation – cases prove effects and secrecy levels differentiate accommodative signaling versus signaling resolve

**Lonergan**, assistant professor at the Army Cyber Institute at the US Military Academy, and **Lonergan**, senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers, **2022**

[Erica and Shawn, “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises”, Security Studies, 18 Feb 2022, Taylor and Francis, accessed July 1, 2022, JCP-LL]

A few patterns stand out. Cyber operations during crises generally did not lead to escalation; they were typically followed by a reciprocal cyber operation and/or the de-escalation of the crisis. Additionally, most of the cases involved relatively low-cost cyber operations, such as website deface- ments and DDoS attacks perpetrated by proxy groups or patriotic hackers, rather than highly sophisticated operations that targeted adversary critical infrastructure or had lasting destructive effects. There were two exceptions, both of which reportedly involved the US government (rather than a proxy group) as a cyber actor: the Strait of Hormuz crisis between the United States and Iran in June 2019, and the Abqaiq-Khurais attack that led to a crisis between the United States/Saudi Arabia and Iran in September 2019.68 Therefore, we chose to examine one of those cases—the Strait of Hormuz crisis—in greater detail as a point of comparison.

The five cases vary according to the presence or absence of cyber opera- tions during the crisis; and, of the cases involving cyber operations, the operations vary in their type and role in the crisis. Although there is an inherent logic to the argument that cyber operations as accommodative sig- nals could facilitate crisis de-escalation, the overwhelming tendency of most crises, particularly those involving nuclear powers, to resolve short of major escalation makes it more difficult to empirically establish a causal relation- ship between the former and latter—or to find cases with meaningful vari- ation across escalation outcomes. Therefore, the case studies are meant to serve two purposes. First, given that cyber operations take place in some crises but not others, the cases aim to validate our argument that some cyber operations are deliberate signals rather than superfluous noise. Thi is particularly true for closed regimes, which monitor (and in some cases control) online activity within their cyber borders. Therefore, during a cri- sis, parties may surmise that cyberattacks originating from a closed state likely occur with some level of the central government’s implicit permis- sion.69 Second, **variation across the cases in the types and characteristics of cyber operations sheds light on the various ways states use cyber operations during crises, providing a means of distinguishing between cyber opera- tions as accommodative signals versus those meant to serve as signals of resolve or deterrence.**

In two of the case studies—the 2012 crisis between China and Japan and the 2015 crisis between Russia and Turkey—the crises triggered domestic nationalist sentiments, and private back channels failed to resolve the issues at hand. In this context, low-level, disruptive cyber operations carried out by hacktivist groups or proxies loosely affiliated with the government func- tioned as accommodative signals. There were two audiences for these cyber signals: nationalist or hawkish domestic constituencies and the adversary government. These attacks’ limited effects, coupled with their highly visible nature and tenuous connection to the government, enabled leaders to man- age domestic sentiments while avoiding more aggressive action that could further escalate the situation. In response, the targets avoided publicly link- ing the cyberattacks with the adversarial government.

In contrast, in two of the three cases that did not produce significant nationalist sentiments—the 2013 ADIZ crisis and the 2018 crisis between the United States and Russia in Syria—no cyber operations took place and the crises resolved through a combination of diplomacy and military maneuvers, both public and private. The absence of cyber operations in these instances demonstrates that the choice to conduct or allow cyber operations in some cases but not others is deliberate, providing inherent plausibility to our argument that cyber operations could be signals.

Finally, one case—the 2019 crisis between the United States and Iran over the Strait of Hormuz—involved a cyberattack in conjunction with the absence of major nationalist mobilization. However, unlike the first two cases containing cyber operations, in this instance government forces reportedly conducted a cyberattack directly and covertly, tailored it to a specific adversary intelligence organization, and degraded adversary capabil- ities for a sustained period. This is suggestive of a cyber signal of resolve, rather than accommodation.

Altogether, the five cases illustrate the characteristics of cyber operations as signals of accommodation versus resolve. They also suggest the condi- tions under which the former are more likely to be observed: in crises where leaders strive to balance nationalist domestic sentiments while avoid- ing actions that would exacerbate the situation, and where other forms of private communications may not be as viable. Table 2 depicts a summary of the cases and the core findings.

## Military to military exercises – general

### Expand military to military exercises

#### Solvency - expand cooperation and military to military exercises like Baltic Ghost

**Maigre, 2022**

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

Action Plan for the Next Five Years

To make NATO future-proof, it must be cyber-secure and operational. But is it doing enough to address the complex and evolving challenges of cyberspace? NATO’s strategic challenge is to blend its successful conventional deterrence functions with a new strategy for cyber action. NATO’s ability to send a collective message of resistance and to establish a credible threat response is its most valuable asset on the cyber-security front.

Four sets of actions for NATO are proposed. First, denying covertness by attribution: NATO should persuade opponents that they cannot be clandestine in their cyber actions. NATO and its members need to demonstrate that it is difficult or impossible to act covertly and be clear about attributing responsibility for cyberattacks.

Until recently, governments did not publicly release details on cyber incidents. But since 2018, public disclosures of cyberattacks by several Western powers indicate a new multinational policy of state transpar- ency. The growing relevance of attribution is partially due to states becoming better at attributing cyber operations.1 Greater public knowledge of cyberattacks heightens awareness of cyber conflicts and leads to greater public acceptance of cyber countermeasures.

Ultimately, what matters is that states engaging in unlawful actions using cyber means will face conse- quences. With attribution, policymakers show that they know what is happening in these networks and can investigate incidents. It also clearly spells out unacceptable behavior and can help create state prac- tice. The best way to implement the international norms is by calling out behavior and having conse- quences when these norms are breached. Attribu- tion will make clear to the malicious actor that their actions will be seen and addressed. It is the basis, under international law, for countermeasures and self-defense.

When should states publicly attribute cyberat- tacks? Effective public attribution requires a clear understanding of the attributed cyber operation and the cyber-threat actor, but also the broader geopo- litical environment, allied positions and activities, and the legal context. The public attribution frame- work put forward by Max Smeets and Florian Egloff in March 202127 distinguishes four factors that act as enablers or constraints in public attribution. These factors are intelligence, incident severity, geopolitical context, and post-attribution actions. The combina- tion of these four components enables consistent deci- sion-making about whether to publicly disseminate information about an adversary’s actions, privately tell the adversary, or restrict knowledge of the intrusion to the government and potentially other partners.

Collecting and processing intelligence—infor- mation about foreign countries and their agents— provides a technical basis for attribution. How could allies improve intelligence sharing to conduct more rapid attribution and enable a response to adver- sary cyber activity? During the Nordic-Baltic foreign ministers meeting in Tallinn in September 2020, a 90-minute tabletop exercise was organized28 to test the ministers’ ability to respond to and attribute an esca- lating cyberattack. They answered multiple-choice questions on communication of and possible diplo- matic countermeasures to the attack. The minis- ters learned through first-hand experience that a timely exchange of technical intelligence can be key in attributing any cyberattack. “The shared view [of the countries involved]—especially when it comes to complicated issues—is crucial,” said Urmas Reinsalu, Foreign Minister of Estonia.29

Attribution is only as good as the information that allies are willing to share. NATO’s value can be in becoming the preferred platform for sharing cyber information. General Paul Nakasone, who heads US Cyber Command, told the House Armed Services subcommittee on intelligence that “in 35 years” he has never seen a better sharing of accu- rate, timely, and actionable intelligence than what has transpired with Ukraine.30 Sharing information and intelligence with allies “builds coalitions” and can “shine a light on disinformation” campaigns, like the one Russia used to lay the groundwork for their invasion of Ukraine.

As the second course of action**, NATO should use the current crisis to accelerate the progress with setting up NATO’s own cyber command and sharpen allied responses to malicious cyber actions**. Overall, this would give more credibility to its cyber defense. In February 2019, allies endorsed a set of tools to respond to cumulative cyber activities, but not much has happened to take it forward. It is now time to build upon this set and develop concrete steps at the political, military, and technical levels to model alli- ance behavior according to the threat landscape. This means a sharper focus on future responses to high- and low-end cyberattacks along with concrete deter- rence actions and tools for individual sectors and target types. Much of this is based on the high-end cyber capabilities of select individual allies called “volunteer sovereign cyber effects,” where cyber- capable nations deliver voluntarily offensive cyber effects on a target designated by an operational-levelcommander. The NATO Cyber Command would be responsible for matching military needs with the willingness and capabilities of the nations potentially able to deliver such effects.31 **The alliance should clarify which allies are responsible for offensive cyber operations against certain targets and the informa- tion-sharing and notification requirements.**

**A good plan requires practice. The scenarios of cyber responses that are under the Article 5 threshold should be regularly practiced, and the NATO Cooper- ative Cyber Defense Centre of Excellence (CCDCOE) Locked Shields exercise is a good way to do so**. Orga- nized since 2010, it enables cyber-security experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. The focus should be on realistic scenarios simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects. Locked Shields is a unique opportunity to encourage experimentation, training, and cooperation among allies in an authentic but safe training environment.

NATO should also make more use of its Cyber Range, a platform for NATO exercises and training in Estonia operated by the Estonian Ministry of Defense. The Cyber Range already facilitates NATO’s flagship annual cyber defense exercise Cyber Coalition, and NATO CCDCOE has based Locked Shields on Cyber Range for over a decade. The versatility and computing power of the platform allows a different, complex scenario to be simulated every year for an increasing number of participants. The technical, red-teaming exercise CrossedSwords, organized by NATO CCDCOE, tests the capabilities and skills needed when executing a full-spectrum cyber operation in real life, focusing on experimentation with integrating kinetics and offensive cyber operations in the context of a modern battlefield. More operational- and technical-level joint activ- ities should be practiced among allies and with like- minded partners in order to contribute to imposing costs to malicious actors in cyberspace**. Given that NATO’s cyber response teams are stretched thin due to protecting NATO’s own networks, bi- and multilateral collaboration enables countries to share best practices and, in the event of an emergency, provide mutual rapid assistance in crisis response.**

The cyber exercise Baltic Ghost originated from a series of cyber defense workshops in 2013 and should be expanded to include all NATO battlegroups in the Baltics and Poland. Currently it is facilitated by the United States European Command with the objective to develop and sustain cyber partnerships between Estonia, Latvia, Lithuania on one end, and the Mary- land, Michigan, and Pennsylvania Army National Guards on the other end. Building on the success of Baltic Ghost, regular cyber exercises should take place in multinational NATO battlegroups, led by the United Kingdom, Canada, Germany, and the United States, in Estonia, Latvia, Lithuania, and Poland. Future exercises should regularly support NATO enhanced forward presence forces and train participants to respond to aggression in a contested, degraded, and denied cyberspace environment.

### Military to military exercises - Signaling

#### Military cyber exercises produces the analysis of cyber issues needed to respond to current threats

**Achberger and Smeets, 2022**

[Brita, Research Assistant specializing in international cybersecurity politics, and Max, Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich and Director of the European Cyber Conflict Research Initiative, "The Opportunities and Challenges of Military Cyber Exercises", Council on Foreign Relations, 3/24/22, https://www.cfr.org/blog/opportunities-and-challenges-military-cyber-exercises, accessed 6/30/22, GDI- CC]

CCDCOE started organizing Locked Shields in 2012–preceded by the Baltic Cyber Shield, a one-off exercise in 2010. In 2021, Locked Shields had over two thousand participants. Thirty countries have participated so far, including a NATO alliance team and non-NATO member states Australia and Japan. Over the past decade, military exercises have increasingly focused on cyber-related scenarios, which present unique opportunities and challenges for military planners. The main opportunities of military cyber exercises lie in the collection and analysis of data and the signaling of operational capability. The challenges to military cyber exercises stem from difficulties defining an appropriate ruleset and the resources required to create a realistic training environment with realistic timeframes and dynamics.

Military cyber exercises come in various shapes and forms: from specific, nationally oriented exercises such as Operation Eligible Receiver, organized by the U.S. Department of Defense in 1997, to more general, internationally oriented exercises like Cyber Coalition, organized annually by NATO. Some exercises are more offense-oriented, such as Crossed Swords, while other games lay the emphasis on defense, like Locked Shields.

Military cyber exercises are generally run in a virtual environment. The benefit of which is the organizer’s ability to collect data as the activities of different teams can be more easily recorded. Whilst traffic logs and other data are not always easy to digest, it often creates the opportunity for more granular analyses of moves ex post facto.

Signaling cyber capability is notoriously difficult. However, military cyber exercises can be used as a means of signaling capability and willingness to conduct or respond to cyber operations. “You cannot parade computer code on the streets of Moscow”, but you can create a scenario in which you successfully mitigate simulated malicious code in Moscow’s transportation infrastructure.

### Resiliency

#### Cyber exercises key in establishing a resilient society in an age of cyber threats – they build awareness and test responses

**Gafic et al, 2022**

[Melisa, Junior Researcher in the Department of Computer Science and Security at the St. Polten University of Applied Sciences, “Cyber Exercises in Computer Science Education”, ICISSP, Proceedings of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022) https://www.scitepress.org/Papers/2022/108458/108458.pdf, accessed 7/1/22, GDI-CC]

During COVID 19-crisis the security and resilience of critical information system have been more important than ever before. Breaches and cyber security incidents impressively highlighted the importance of cyber security and especially incident response (ENISA, 2020). In order to ensure resilience of systems, and to prepare for a such unpredictable cyber threats, it is necessary to continuously train people how to purposefully react on these threats and to communicate within the team under difficult circumstances (Wilhemson and Svensson, 2014). Therefore, exercises especially cyber exercises, play a central role in establishing a resilient society.

Cyber exercises have gained a lot of attention throughout recent years, especially in the cyber security sector, as an important tool for security training, awareness-building and testing incident response. The EU emphasizes the importance of this field in its strategy for the digital decade (European Commission, 2020). Large exercises, that make it to the news, such as CyberStorm (Cybersecurity & Infrastructure Security Agency (CISA), ), Locked Shields (The NATO Cooperative Cyber Defence Centre of Excellence, 2021) or Cyber Europe (ENISA, 2021), represent only a small fraction of the exercises carried out. Conducting cyber exercises also has an educational value. Through interactive activities, such as simulations and scenarios, exercise participants apply knowledge in practical situations using techniques and tools they are familiar with, thereby deepening their understanding of a particular type of incident (Dewar, 2018).

### SSA

#### cybersecurity exercises key to enhancing cyber operator readiness and situation awareness

**Pihelgas** **and Kont**, **2021**

(Mauno, Technology Branch @ NATO CCDCOE, and Markus, Research and Development @ Stamus Networks, “Frankenstack: Real-time Cyberattack Detection and Feedback System for Technical Cyber Exercises,” NATO Cooperative Cyber Defence Centre of Excellence, 2021, https://ccdcoe.org/library/publications/frankenstack-real-time-cyberattack-detection-and-feedback-system-for-technical-cyber-exercises/, accessed 6/29/2022, gdi-tmur)

Cybersecurity exercises (CSXs) are key to enhancing cybersecurity operator readiness while also improving situation awareness (SA) in the cyber domain. Crossed Swords (XS) [1] is an annual interdisciplinary CSX directed at training participants for responsive cyber-kinetic operations. Although NATO nations have begun acknowledging the necessity of both defensive and offensive cyber capabilities, there are few exercises that tackle such a controversial subject. XS is organized by the NATO CCD COE in the NATO Cyber Range and utilizes a hybrid approach between cyber-physical and simulated infrastructure.

Cyber-exercise-specific SA systems are designed to improve SA during cyber exercises. While traditional SA systems are oriented toward cyber defenders, CSX-specific SA systems have been designed to provide situation awareness feedback not only to cyber defenders, but all participating teams alike.

### US contributions key to effective cyber exercises

#### \*Supreme Allied Commander Europe and NAC should increase cyber exercises

**Ahlawat, 2021**

[Urjasvi, Jindal School of International Affairs and Research Intern at the Centre for Security Studies, “NATO: CYBERSECURITY AND CYBER COALITION“CSS ISSUE BRIEF, January 2021, https://jgu.s3.ap-south-1.amazonaws.com/jsia/Urjasvi+-+NATO+Cybersecurity.pdf accessed jcp-tm 6/9]

FUTURE: ACTIONS TO STRENGTHEN CYBERSECURITY

As the Cyber Coalition demonstrates the actions taken by NATO, this segment will further elaborate on more aspects that can be covered in the aforementioned exercises. The core of NATO cybersecurity efforts lies at the member-state level.7 The size and severity of today's cyber-attacks involve a new approach to political, military, and civilian responses. NATO should take a few effective steps in the organisation to establish a quick decision-making mechanism while confronting a cyber-attack. The solution towards more secure cyberspace lies in the functioning and accountability of member states; currently, no mechanism exists to ensure that the member states are adhering to the Cyber Defence Pledge taken in the Warsaw Summit of 2016. NATO can discuss and provide expertise, however, there is no apparatus to enforce that expertise on the member, and the efficiency of the cyber defence efforts depend on the implementation by the members.

The first action can be taken concerning the decision making of NATO, which is divided into NATO as an organisation and its members. In the former aspect, the resource allocation to NATO should be increased as it will help in not only detecting and indicating hostile cyber activities but will allow better use of the civil and military intelligence units. Furthermore, **the powers of the Supreme Allied Commander Europe should be increased by the North Atlantic Council, along with which the CCDCoE should increase cyber defence activities and exercises as it will increase efficiency**. The focus of these exercises should be on dynamic and challenging cyber crisis-conflict situations, fast decision-making processes. Concerning the members’ role, identifying and sharing information about any potential threats to any of the members should be shared; the national intelligence services should supply and exchange such information. Allies and willing partners should continue to work on improving and updating threat assessments, and facilitating closer intelligence cooperation.8 Cyber challenges arrive in the form of networks and to defeat these threats involves an equally well-organized network of multinational and cross-sector collaboration. CC20 did deal with the aspect of decision making, however, as explained above, this aspect has a greater potential to secure the member states of NATO from the cyber threats.

## MOU

### MOU solvency – coordinated cyber policy

#### Sustained ally coordination key to learn from different contexts for policy development – memorandum of understanding on cyber solves

**Smeets 2021**

(Max Smeets,, Max Smeets is Senior Researcher at the Center for Security Studies, Zurich; Director of the European Cyber Conflict Research Initiative; and an affiliate at Stanford's Center for International Security and Cooperation, “NATO allies’ offensive cyber policy: A growing divide?” THE FUTURE OF EUROPEAN STRATEGY IN A CHANGING GEOPOLITICAL ENVIRONMENT: CHALLENGES AND PROSPECTS edited  Michiel Foulon, and Jack Thompson Hague Centre for Strategic Studies, August 1st, 2021, JSTOR, GDI- TMK)

Where to go from here? The divergence in cyber policy across NATO member states is problematic. Allies disagree on both the goals of cyber policy and the ways and means to achieve them. This can cause tension between allies, especially when it comes to the necessity and legitimacy of operating on each other’s national systems and networks. Some may argue that these differences result from differences in maturity. Some states simply have not caught up with the latest developments, goes the argument. This assumes a single path to cyber maturity or that the dynamics of cyberspace pull all states in the same direction. It suggests that – even without major policy coordination – allies’ cyber policies will converge over time. But a more persuasive understanding of the current trend is that even though states can learn from each other’s institutional progress, differences do not merely stem from states “lagging behind.” These states are on a different policy path. This means it requires dedicated and sustained policy attention to, at a minimum, coordinating the different policies of states – and potentially bring them closer together.

What can be done to ensure that this divergence in cyber policy does not cause further friction between allies?11

I have previously proposed a NATO Memorandum of Understanding (MoU) to reduce discord among the allies; the goal would be to enhance trust, transparency, and confidence between allies and to improve the

effectiveness of disrupting and deterring adversaries’operations in cyberspace.12 The main purpose of the MoU would be to reach an agreement on the equities involved in permitting signatories to conduct cyber effect operations in each other’s networks—and the relative weight of those equities.

## Multilateral international framework

### International framework key

#### Legal framework necessary to facilitate NATO’s adaptation to cyber attacks

**Păunescu, 2021**

[Dragoș-Mihai, PnD in International relations at the Carol I National Defence University, “NATO’S ENCOUNTERS IN THE CYBER DOMAIN”, 11/9/2021, https://revista.unap.ro/index.php/XXI\_FSA/article/view/1274/, accessed 6/29/22, GDI- CC]

NATO’s potential adversaries are developing offensive cyber capabilities to exploit ridges and  vulnerabilities in order to confuse and undermine the Alliance’s reaction in future conflicts. The  constant technological adaptation of the NATO and national security forces to the current strategic  scenarios is essential to maintain a reliable defense posture.

The EU and NATO are targeted by similar cybersecurity threats that undermine, in various  degrees, all operational environment factors, political, military, economic, social, information,  infrastructure, and their cooperation is leading to common or complementary defense solutions.

By constantly adapting its structure and posture, NATO is able to face new emerging threats  and to increase its reediness and responsiveness in all operational domains. The Alliance’s  adaptation process comprise also the development of policies and capabilities for the cyber domain  designated to improve the understanding of different threats and risks and its ability to react in order  to achieve NATO’s ambitions for the cyberspace.

Given that, over the past few years, the frequency and complexity of the cyber-attacks and  their potential to generate instability grew substantially, the need to achieve consensus for a an  worldwide recognized legal framework in the cyber domain should become a high priority for  international organizations.

#### Explicit bargaining over international agreement necessary to delineate what constitutes acceptable cyber espionage and violations

**Kim ‘22**

(Wonny K. Kim, Innovation and Information Operations Officer in the U.S. Army Reserve 75th Innovation Command, Master of International Affairs from Columbia University, Master of Science in Technical Intelligence from National Intelligence University, and B.A. in Philosophy and Psychology from Binghamton University, ““Explicit” Bargains are Essential to Forming Desired Norms in Cyberspace,” Cyber Defense Review, Spring 2022, JSTOR, accessed 6/30/22, GDI- TMK)

INTRODUCTION

As the United States (US) endeavors to estab- lish international norms in cyberspace, it is critical that it delineate which behavioral norms it supports, how it plans to establish them, and to what ends the norms serve. These con- siderations are particularly timely as the current US administration builds its cybersecurity team and con- siders pressing issues in cyberspace. In January 2021, President Joe Biden appointed National Security Agen- cy Cybersecurity Director Anne Neuberger as Deputy National Security Advisor (DNSA) for Cyber and Emerg- ing Technology in the National Security Council.[3] As reported then, “Neuberger will be responsible for coordinating the federal government’s cybersecurity efforts, with a likely emphasis on responding to a mas- sive cyberespionage campaign carried out last year by suspected Russian hackers [referencing SolarWinds], which the government is still struggling to unravel.”[4] She has since been joined in the administration by Chris Inglis, National Cyber Director, and Jen Easterly, Director of Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).[5]

Although the SolarWinds breach was extensive, af- fecting roughly 100 companies and a dozen govern- ment agencies,[6] the breach itself was not a violation of international norms as the operation did not esca- late beyond espionage.[7] As the US devises its cyber policy, it is imperative to distinguish between actions taken for counterintelligence purposes and actions taken to develop international norms in cyberspace. Espionage is not a violation of an international norm, and the US does not appear inclined to establish it as such. Espionage and counter-espionage are estab- lished behaviors that participants have tacitly agreed to undertake and assume their associated costs. Yet some espionage-associated behavior in cyberspace fall outside these bounds; for example, the US takes exception to espionage conducted “with the intent of providing competitive advantages to companies or commercial sectors.”[8]

Current literature advocates for tacit bargaining, that is, behavioral actions and counter-actions, in developing normative behavior in cyberspace.[9] The dynamics of the 2015 U.S.–China Cy- ber Agreement, however, indicate two important considerations: first, the necessity of explic- it bargains, such as international agreements, to support the formation of desired norms that help avoid costly escalatory spirals. Second, how a viable prospect of cooperation underpins the success of norm development. Furthermore, the potential impact of actions taken outside of cyberspace must be taken into account as they did lead to the cyber accord and at least the temporary cessation of the People’s Republic of China (PRC) offending activity in cyber- space.[10] These are critical considerations for the US cybersecurity team as they develop US cyber policy: ideally, one directed towards a robust US-led multilateral, whole-of-government approach to the development of norms in cyberspace.

## Offensive cyber operations

### Squo – NATO lacks offensive cyber

#### Uniqueness – NATO lacks coordination on offensive cyber capabilities

**Smeets 2021**

(Max Smeets,, Max Smeets is Senior Researcher at the Center for Security Studies, Zurich; Director of the European Cyber Conflict Research Initiative; and an affiliate at Stanford's Center for International Security and Cooperation, “NATO allies’ offensive cyber policy: A growing divide?” THE FUTURE OF EUROPEAN STRATEGY IN A CHANGING GEOPOLITICAL ENVIRONMENT: CHALLENGES AND PROSPECTS edited  Michiel Foulon, and Jack Thompson Hague Centre for Strategic Studies, August 1st, 2021, JSTOR, GDI- TMK)

NATO allies have made slow but steady progress when it comes to crafting policy to deal with cyber security challenges. Yet this progress has not always been made in a collaborative fashion. Especially when it comes to the development and deployment of offensive cyber capabilities, NATO allies are increasingly diverging in policy. This is a worrying development and deserves more attention than it has so far received.

### Squo – lack of transparency offensive cyber capabilities

#### Lack of transparency and clear definition of offensive cyber weapons risks inadvertent escalation of cyber conflicts and prevents effective negotiations

**Faesen, et al Hague Centre for Strategic Studies, ‘22**

(Louk, Hague Centre for Strategic Studies, HCSS conducts research and provides advice on geopolitical and defence & security issues to governments, international institutions and businesses, “Cyber Arms Watch: An Analysis of Stated & Perceived Offensive Cyber Capabilities,” May 2022, JSTOR, accessed 6/29/22, GDI- TMK)

Conflict between states has taken on new forms, and cyber operations play a leading role in this increasingly volatile environment, earning them a top spot among states’ most critical security concerns. According to the Council on Foreign Relations, 34 states are suspected of sponsoring cyber operations since 2005.1 Despite the high level of activity, relatively little is publicly known about the offensive cyber capabilities of states. This is despite the widely held concern in diplomatic circles that tensions in cyberspace are escalating, and the likelihood of a catastrophic cyber exchange between nation states continues to rise. Such a calamity could well happen by accident. Avoiding “inadvertent escalation” – or accidental war – remains the most significant challenge between states in cyberspace. A major contribution to this uncertainty is the lack of transparency of offensive cyber capabilities. Unlike other military systems, they are largely treated as dark secrets from the espionage world. Traditional arms control efforts have depended upon the ability to count weapon systems, like tanks and missiles, to regulate their deployment. But there is no common understanding of what “cyber weapons” are, or indeed even “cyber forces”. States are left guessing as to the overall capability of another state (albeit at widely varying degrees of detail) without, for the most part, being able to detail the exact order of battle, table of equipment, tactics, techniques, procedures or other basic information – unless the intelligence assessment is very complete.2 This secrecy has implications not only for intelligence and national security assessments, but more so for both the institutional dialogues and the wider public discussion on international peace and security in cyberspace, by foreclosing any common language on offensive cyber capabilities and intent. Because of the lack of transparency, intergovernmental, track 1 and track 2 discussions often lack any basis for common exchange. It frustrates meaningful progress for predictability, confidence-building measures (e.g. within regional organisations such as ASEAN and the OSCE), norms of responsible state behaviour (e.g. within the United Nations), and other stability measures. The lack of transparency also impacts and limits the wider public discussion: the general absence of information means that much of the public, media, and academic discussion is not in sync with reality and risks becoming irrelevant.

### Squo – lack of focus on offensive capabilities

#### Limited investment in offensive cyber – need more focus

**Strucl, 2022**

[Damjan, researcher in the Strategy Branch at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), “Comparative study on the cyber defence of NATO Member States”, CCDCOE, 4/21/22, https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf, accessed 7/1/22, GDI-cc]

\*CD = cyberdefense

\*CS = cybersecurity

\*ICT = information communication technology

To implement effective CS and CD, the proper cyber capabilities are needed; that is to say, a combination of personnel, technologies and organisational attributes. From the collected data, we found that states are building cyber capabilities primarily by investing in technology and knowledge. It is very positive that most states have an integrated in-house education system, while at the same time using training and exercises within NATO and the EU. Such a combination of knowledge acquisition is particularly important in terms of exchanging good practices and testing interoperability at national and international levels.

It is also positive that most states use outsourcing and (commercial) think tank/laboratory organisations, but less than half of the states have a competency certification system in place. Some do not have offensive cyber capabilities or do not even intend to build them. Possession of offensive cyber capabilities does not affect the state's posture or does not mean that the state's posture is offensive. Offensive cyber capabilities allow the state to actively defend itself, while at the same time allowing it to better understand the attacker. The same is true in all other components of the military as states not only develop defence capabilities but are also offensive and they also train offensively, which does not mean that they will unnecessarily act offensively or pose a threat to international peace. Cyberspace, as one of the operational domains or as a cross-domain, is no different and so the same approach to ensuring national security is needed. Building cyber capabilities by upgrading ICT alone is not enough for effective CD. It is also necessary to build offensive cyber capabilities that will allow states to develop, among other things, tactical and technical procedures of CD that will stop an attacker from carrying out a cyber attack or operation. Therefore, it is not a question of whether an offensive cyber capability is needed, but how big and how trained it should be or, as Limnéll said, ‘cyber capabilities are essential for the nation-states and the armed forces that wish to be treated as credible actors’. 134

#### Offensive cybersecurity – NATO needs development

**Ahlawat, 2021**

[Urjasvi, Jindal School of International Affairs and Research Intern at the Centre for Security Studies, “NATO: CYBERSECURITY AND CYBER COALITION“CSS ISSUE BRIEF, January 2021, https://jgu.s3.ap-south-1.amazonaws.com/jsia/Urjasvi+-+NATO+Cybersecurity.pdf accessed jcp-tm 6/9]

The third factor is about the consideration of offensive cybersecurity. NATO acknowledges Article 5 a potential cyber-attack trigger. The doctrine and crisis management requirements are established in the cyber policy of NATO, however, the emphasis is only on a defensive stance. As such, cyber is not regarded by the Alliance as a power generator that may be of value to member states of NATO’s defence; as mentioned above, the integration of NATO and cybersecurity was only in 2008. In 2016 it was considered as an important domain; as of now, it was not considered to be important. On the contrary, Russia views aggressive cyber capability as an important part of its military strength and, in particular, as a way of compensating for its relative lack of conventional forces compared to NATO. The growth of networking, the proliferation of smartphones, cloud computing, the development of software, and other technical developments open new opportunities for attackers and compel defenders to protect a rising range of fields. The defensive strategy of NATO is not viable in the long term. There are valuable cyber capabilities worth attaining, including the ability to conduct reconnaissance and surveillance, intercept communications, or deny resources and access.9

### Squo – US Cyber Command unilateral shift

#### Uniqueness - US Cyber Command shift in policy to superiority through persistence – alters the scope of US military actions

**Smeets,** ETH Zurich, Center for Security Studies, **2020**

[Max “U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection” Intelligence and National Security vol 35, 2020 – Issue 3, Taylor and Francis Online accessed 7/5/2022 GDI-TM]

The 2018 U.S. Cyber Command vision and the Department of Defense Cyber Strategy embody a fundamental reorientation in strategic thinking.i Based on the recognition that adversarial behavior below the threshold of armed attack could nevertheless be strategically meaningful, U.S. Cyber Command seeks to achieve “superiority through persistence”, that is constantly engaging with the adversary - wherever they maneuver.ii

Much has already been written about the implications of U.S. doctrinal change. The strategic shift has, in particular, led to numerous critical remarks about the risks of escalation between the U.S. and its main adversaries in cyberspace.iii Early on, Healey voiced concern that the change in strategy would trigger the “new forever war in cyberspace”.iv In a more recent article, Healey analyzes the implied causal chain of “persistent-engagement stability theory,” and addresses how certain feedback loops could potentially amplify or dampen cyber conflict.v Others have argued that persistent engagement deepens the cyber security dilemma - especially between the U.S. and China.vi

The degree to which persistent engagement can help with the establishment of cyber norms has opened a second line of debate. According to some proponents, persistent engagement is a form of norms setting through practice, leading to a “comprehensive strategic great power competitive space with its own distinct structural features.”vii Others are less positive that the strategy can create a new normative area of competition - especially if it is not combined with other elements of competitions in the economic, diplomatic, informational and military spheres.viii

In addition, the shift in U.S. strategy together with a set of notable legal changes - particularly to the authorisation and oversight architecture - has led scholars and practitioners to write more prolifically about U.S. legal underpinnings of out-of-network operations.ix As a workshop report on military cyber operations clarifies, three changes are most prominent: “Firstly, the changes confirmed that the [DoD] has authority to operate in the cyber domain outside of the context of defending its own networks. Secondly, they clarified when the executive can decide on the undertaking of operations outside US territory without Congressional authorisation. […] Thirdly, Congress explicitly articulated that the activity conducted by U.S. Cyber Command does not constitute “covert action” as defined by US domestic law.”x Overall, scholars have concluded that U.S. Cyber Command can now operate more swiftly as it is no longer required to undertake the interagency process as before.xi

#### US strategy of persistent engagement and defend forward promotes stronger defense across alliance

**Smeets,** ETH Zurich, Center for Security Studies, **2020**

[Max “U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection” Intelligence and National Security vol 35, 2020 – Issue 3, Taylor and Francis Online accessed 7/5/2022 GDI-TM]

**\*the strategy refers to US Cyber Command shift to persistent engagement**

Less systematic attention, however, has been devoted to the strategy’s implications for the alliance and intelligence collection. The purpose of this paper is to conduct a benefit-risk assessment of the US strategy on this issue.xii The assessment of this article takes place in five steps. Section I notes that, historically, allied states operate in each other’s systems or networks in at least two ways: as an observer, gathering intelligence on adversarial activity in others’ networks; and as a passerby, transiting through allied systems and networks to access a certain adversarial target. It is argued that, with the change in strategy, the U.S. now also seeks to be a disrupter, seeking to cause friction for an adversary’s operation within an ally’s network or system. Section II addresses the benefits of this activity and efforts of the U.S. to more closely collaborate with allies in this space. It suggests US strategy of persistent engagement and defend forward can promote a stronger defense as a whole - and for states with limited cyber capability in particular.xiii Section III subsequently discusses the four avenues of how the strategy could lead to negative implications for the alliance: i) loss of trust due to offensive cyber effects operations in allied systems or networks; compromise of allied intelligence operations and capabilities; iii) exploitability of the strategy by adversaries; and iv) the implementation (and justification) of persistent engagement by other countries. The final section concludes and provides a potential proposal to move forward.

### Squo – US divergent policy undermines cohesion

#### National cyber policies developing, revealing disparities and differences in cyber capabilities and policies – US persistent engagement policy created divergence in allies’ cyber policies

**Smeets 2021**

(Max Smeets,, Max Smeets is Senior Researcher at the Center for Security Studies, Zurich; Director of the European Cyber Conflict Research Initiative; and an affiliate at Stanford's Center for International Security and Cooperation, “NATO allies’ offensive cyber policy: A growing divide?” THE FUTURE OF EUROPEAN STRATEGY IN A CHANGING GEOPOLITICAL ENVIRONMENT: CHALLENGES AND PROSPECTS edited  Michiel Foulon, and Jack Thompson Hague Centre for Strategic Studies, August 1st, 2021, JSTOR, GDI- TMK)

Steady progress

Member states agree on the critical need for a coherent cyber policy. Almost all NATO allies have developed both a cyber security strategy and a cyber defense strategy.1 Some states have published updated versions over the years to reaffirm cyber security as an issue of national security importance, to tweak institutional responsibilities, or to articulate changes in the threat landscape. In addition, since 2018, most NATO allies have established a military cyber organization (either a command or unit) with a mandate to conduct cyber effect operations – that is, cyber operations intended to disrupt, deny, degrade and/or destroy.2 There is also shared recognition that international law applies in cyberspace, although allies have yet to spell out the legal procedures for operating in this new “domain of warfare.”

These developments have been both reflected in, and aided by, policy progress made at the inter-governmental level. At the Prague Summit in 2002, NATO for the first time recognized that the Alliance should “Strengthen our capabilities to defend against cyber attacks.”3 In 2008, at the Bucharest Summit, there was another milestone development, when NATO adopted a “Policy on Cyber Defense,” aiming to “protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack.”4 In the same year, the Cooperative Cyber Defence Centre of Excellence – a NATO accredited international research institution – was established in Tallinn, Estonia. In 2016, at the Warsaw Summit, cyberspace was officially recognized as a “domain of operations” and allies made a Cyber Defense Pledge to enhance their cyber defenses.5 The 2018 Brussels Summit and 2020 London Summit reiterated NATO’s commitment to implement the Cyber Defense Pledge and operationalize the Cyber Operations Center, responsible for situational awareness and the centralized planning of cyber operations and missions.6 In January 2020, the Allied Joint Doctrine for Cyberspace Operations was published “to plan, execute and assess cyberspace operations (CO) in the context of allied joint operations.”7

Steady divergence

Yet when it comes to the direction of allies’ cyber policy, growing differences are apparent – especially in the development and deployment offensive cyber capabilities. First, even though most states now have – or are in the process of – establishing a cyber command, operational capabilities vastly differ across states.

Whereas some governments are increasingly allocating significant resources to conduct cyber operations – and are now starting to benefit from these investments – the majority of allies still run their cyber commands on a budget of a few million a year –an amount that is insufficient for effective operations in the cyber domain.

Secondly, until a few years ago, NATO members’ strategic visions were largely aligned. National cyber strategies shared a common threat focus on operations that could potentially cause major societal havoc, such as taking down the power grid. Allies’ national strategies were also largely unified in their vision to address this threat, discussing the need for deterrence, resilience, and norms. However, this changed with the publication of the US Department of Defense’s strategy on Defend Forward and US Cyber Command’s vision on Persistent Engagement.8 The United States emphasizes the need to cause friction “wherever the adversary maneuvers,” operating “globally, continuously and seamlessly” (potentially) below the threshold of armed attack. “We must…maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries,” in the words of NSA director and Cyber Command head Gen. Paul Nakasone.9 **Whereas deterrence is about changing your adversary’s cost-benefit calculus, Persistent Engagement is about taking the opportunity away from the adversary to act.10**

Third, NATO member positions on how international law applies – particularly the obligations of states vis-a-vis sovereignty – are now more divergent than a decade ago. Whereas countries like the Netherlands and France are located on the side of the “sovereignty as a rule” camp, the United Kingdom has taken the position that a remote cyber operation by one state into another’s cyber systems or network does not violate the latter’s sovereignty.

### Offensive cyber operations – no integration now

#### NATO doesn’t include offensive cyber effects in mission planning and contributions voluntary – despite state and non-state adversaries attacking NATO members

**Iftimie,** Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business**, 2020**

[Ion, “NATO’s needed offensive cyber capabilities” NDC POLICY BRIEF No. 10 – May 2020 <https://www.ndc.nato.int/news/news.php?icode=1441#:~:text=This%20Policy%20Brief%20looks%20at,cyber%20capabilities%20into%20its%20operations> accessed 7/5/22 GDI-TM]

NATO’s adversaries in the cyber domain

Warfare in the cyber domain is already conducted against NATO member states by both state and nonstate actors. It is also conducted by NATO member states against these external threats. Within the Alliance, however, **offensive cyber effects are not yet part of the mission planning process and integration of national offensive cyber capabilities into joint NATO operations is voluntary.** Integrating these national offensive cyber capabilities into NATO operations, thus requires, not only a clear understanding of these capabilities, but also agreement on the cyber threat environment, characterized by the intent and capabilities of NATO’s current and/or potential future adversaries. State adversaries in the cyber domain include Russia, China and/or Iran. These are countries known to be building offensive cyber capabilities specifically for the purpose of using them against NATO memberstates.7 In Russia’s case, cyber attacks were conducted against the critical infrastructure of NATO member states and partner nations, as for example against US energy infrastructure in 2017 (including against a nuclear powerplant near Burlington, Kansas)8 or against the Ukraine power grid in December 2015. China has also been conducting persistent cyber espionage using offensive cyber capabilities against core military and critical infrastructure of NATO member states for years. For this reason, the US Secretary of Defense, Mark T. Esper, remarked at the 2020 Munich Security Conference that the 5G Huawei infrastructure is a serious threat to NATO.9 Lastly, Iran’s offensive cyber capabilities have also been observed during multiple attacks against the critical infrastructure of NATO partner nations in the Middle East. NATO adversaries in the cyber domain also include non-state actors, such as terrorist organizations. The US and the UK have conducted several successful offensive cyber operations against those entities. These offensive cyber operations had a significant force multiplier effect, in conjunction with conventional actions on the ground, at sea, in the air and from space, that contributed to the defeat of Daesh in both Iraq and Syria.10 Today, most Allies are building offensive cyber capabilities needed to deny adversaries the freedom of maneuver in the cyber domain.

#### Evolution of cyber means cyber emerging as offensive weapon to integrate into NATO missions

**Iftimie,** Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business**, 2020**

[Ion, “NATO’s needed offensive cyber capabilities” NDC POLICY BRIEF No. 10 – May 2020 <https://www.ndc.nato.int/news/news.php?icode=1441#:~:text=This%20Policy%20Brief%20looks%20at,cyber%20capabilities%20into%20its%20operations> accessed 7/5/22 GDI-TM]

At the 2016 NATO Summit in Warsaw, cyberspace was recognized as an operational domain in which NATO military forces must be able to maneuver as effectively as they do on land, at sea and in the air. Since then, Allies have conducted several successful offensive cyber operations1 against non-state adversaries, such as Daesh. Due to technological transformations in recent years, cyber is no longer viewed by NATO and its member states only as a hybrid threat, but also as a weapon in its own right and as a force multiplier2 in current military operations. Over the next two decades, NATO will look for new ways to integrate cyber weapons (or offensive cyber capabilities) into its operations and missions.3

This Policy Brief looks at the distinctions between cyber as a hybrid threat and cyber as a weapon, from theoretical, policy and practice perspectives, and proposes new ways in which NATO can integrate offensive cyber capabilities into its operations.

### Offensive cyber operations – solves deterrence

#### Offensive cyber operations provides A2/AD to prevent freedom to maneuver in cyberspace – integration of OCOs key to deterrence credibility

**Iftimie,** Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business**, 2020**

[Ion, “NATO’s needed offensive cyber capabilities” NDC POLICY BRIEF No. 10 – May 2020 <https://www.ndc.nato.int/news/news.php?icode=1441#:~:text=This%20Policy%20Brief%20looks%20at,cyber%20capabilities%20into%20its%20operations> accessed 7/5/22 GDI-TM]

The use of area denial weapon systems in the cyber domain

Anti-Access/Area Denial (A2/AD) weapon systems have traditionally been used by NATO and its member states to prevent an adversary’s freedom of maneuver on land, sea or air. In the geographic domains, these capabilities include land mines, missiles (cruise, ballistic, surface to air, anti-ship, etc.), submarines, electronic warfare, and even Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) weapons. In the cyber domain A2/AD is achieved through offensive cyber operations. Those operations have already been used for the purpose of achieving A2/AD by NATO member states in the cyber domain. This is the case of the US-led Operation Glowing Symphony (OGS), where “the United States Cyber Command reportedly acquired administrator passwords to [Daesh] websites.

The passwords enabled deletion of digital content, including videos used for recruitment, from cyber infrastructure located in at least five countries outside actively hostile areas of Iraq and Syria. Similar digital content reportedly resided on cyber infrastructure in as many as 30 other States. Changing the passwords reportedly locked IS administrators out of the websites”.11 OGS restricted Daesh’s freedom of maneuver on networks physically residing in Iraq and Syria (which were controlled by the terrorist group), but also worldwide, where a NATO member state (the US) achieved denial of service effects against Daesh. OGS disrupted Daesh propaganda through content removal from servers residing in multiple countries and through restricting access to physical infrastructure needed to store digital data. Combined with operational successes against ISIL on the ground, OGS actions resulted in propaganda efforts being significantly reduced on several global social media platforms, including Twitter. One particular offensive cyber operation acted, ipso facto, as an A2/AD platform where a NATO member state restricted access to physical networks critical for Daesh recruitment, training, radicalization, fundraising, and command and control.

Integrating offensive cyber capabilities into NATO’s mandate for cyber deterrence and defence

Operationalizing warfighting capabilities in the cyber domain, beyond the traditional geographic domains, requires a new way of fighting in the 21st century, challenging the deterrence and defence mandate of the Alliance. Speaking at the Cyber Defence Pledge Conference in London in May 2019, NATO Secretary General highlighted that for deterrence to have full effect against state and non-state adversaries, NATO and its member states must be ready to use the full range of capabilities at their disposal, to include national offensive cyber capabilities. Deterrence is the act of diminishing an adversary’s intent by highlighting the excessive costs for the said adversary if it proceeds with an undesired action. In NATO’s case, deterrence is achieved by highlighting to an adversary the excessive costs delivered through military means in the event of an attack against Allies. For deterrence to be successful, the adversary must believe that NATO is ready and willing to impose these excessive costs across all operational domains, to include the cyber domain. This may call for Allies to develop offensive cyber capabilities and integrate them with NATO operations in order to collectively impose a high enough cost to deter adversaries from aggressive behaviour. To avoid escalation to total war and cyber fratricide during the fog of war, Allies must also agree on a list of Flexible Deterrent Options meant to allow for a gradual increase of pressure in the cyber domain, and then hopefully limiting the scope and intensity of conflict in this domain. NATO Flexible Deterrent Options in the cyber domain could include (as presented in Figure 1):

• Increasing NATO’s readiness posture through cyber education, training and exercises;

• Deploying NATO Cyber Rapid Reaction teams to conduct defensive cyber operations and protecting critical infrastructure of NATO member states and/or that NATO operations rely upon;

• Increasing public awareness of malicious cyber activities and the potential for conflict in the cyber domain;

• Taking steps to gain the support of all NATO member states in response to the cyber threat and in accordance with commitments of the 2016 Cyber Defence Pledge and the 2018 Brussels Summit;

• Triggering Article 4 of the Treaty to enhance information-sharing and mutual assistance in the cyber domain;

• Making official statements addressing violations of international law in the cyber domain;

• Alerting and deploying offensive cyber operations forces;

• Imposing cyber sanctions;12

• Conducting offensive cyber operations to achieve A2/AD effects in the cyber domain;

• Triggering Article 5 of the Treaty; and

• Conducting offensive cyber operations in combination with other maneuver forces across all operational domains.

### Offensive cyber operations – NATO cohesion and deterrence

#### Lack of integrated offensive cyber capabilities undermines deterrence and defense

**Iftimie,** Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business**, 2020**

[Ion, “NATO’s needed offensive cyber capabilities” NDC POLICY BRIEF No. 10 – May 2020 <https://www.ndc.nato.int/news/news.php?icode=1441#:~:text=This%20Policy%20Brief%20looks%20at,cyber%20capabilities%20into%20its%20operations> accessed 7/5/22 GDI-TM]

Conclusion

The lack of integrated offensive cyber A2/AD capabilities undermines both the unity of the Alliance and its mandate of defence and deterrence. On the former, the lack of coordination between Allies during unilateral cyber operations could lead to friction when resulting effects infringe on Allied cyber-physical infrastructures. It could also lead to cyber fratricide, when failure to properly attribute Allied digital personas occurs during these military operations. On the latter, while most Allies are developing offensive cyber capabilities, some remain unable to face the growing number of cyber threats unilaterally.

Successful defence and deterrence in the cyber domain calls, thus, for ready collective offensive cyber A2/AD capabilities that, when integrated with NATO operations, would complement national and/ or regional responses to malicious cyber activities. If and when this integration occurs, NATO Flexible Deterrence Options would also need to be agreed upon in order to signal cyber adversaries that Allies will respond with one voice if attacked in the cyber domain. Ultimately, political consensus within the Alliance would still need to be built on the type of needed collective offensive cyber capabilities (such as for A2/ AD purposes) and on how to integrate them into NATO’s existing operations and missions.

### Solvency - Persistent engagement – solves red and grey spaces

#### US Cyber command policies focus on red space and grey space for persistence engagement

**Smeets,** ETH Zurich, Center for Security Studies, **2020**

[Max “U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection” Intelligence and National Security vol 35, 2020 – Issue 3, Taylor and Francis Online accessed 7/5/2022 GDI-TM]

Out of Network Operations in allied systems or networks

The purpose of this section is to review the nature of U.S. Cyber Command’s out of network operations. The first part talks about the understanding of territoriality and cyber operations. The second part discusses three types of out of network operations in allied networks.

Following its change in strategy, U.S. Cyber Command seeks to operate “seamlessly, globally and continuously.”xiv In the U.S. Cyber Command vision it is stated that “[s]uperiority through persistence seizes and maintains the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver.”xv In an article for Joint Force Quarterly, NSA Director and Cyber Command head Gen. General Nakasone writes: “If we are only defending in “blue space,” we have failed. We must instead maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries”xvi

“As close as possible” means that the US seeks to achieve effects i) outside of its own networks, and ii) beyond adversaries networks. This vast area is not ungoverned space. We are talking here about routers in Nairobi, servers in the Denmark, or operating infrastructure in other countries. As Seymour Goodman put it “cyberspace always touches ground somewhere”.xvii

Yet, U.S Cyber Command’s use of terminology - as well as talk about “operating close to the adversary” - evades one issue: It is unclear whether Cyber Command only seeks to cause friction in “red space” or if it seeks to compete in “gray space” as well. These terms are often confused and not well- understood. In fact, the issue was raised for “further exploration” at Cyber Command’s 2018 symposium, specifically understanding the “relevance of concepts like area of responsibility and red- blue-gray space to the cyberspace domain.”xviii Joint Publication 3-12 (JP 3-12) on cyberspace operations, prepared under the direction of the chairman of the Joint Chiefs of Staff, explains the terminology:

The term “blue cyberspace” denotes areas in cyberspace protected by the US, its mission partners, and other areas DOD may be ordered to protect. […] The term “red cyberspace” refers to those portions of cyberspace owned or controlled by an adversary or enemy. In this case, “controlled” means more than simply “having a presence on,” since threats may have clandestine access to elements of global cyberspace where their presence is undetected and without apparent impact to the operation of the system. Here, controlled means the ability to direct the operations of a link or node of cyberspace, to the exclusion of others. All cyberspace that does not meet the description of either “blue” or “red” is referred to as “gray” cyberspace.xix

Gray space is defined based on the ‘nodes’ adversaries control. This means the vast area between U.S. government-owned networks and adversaries is not considered to be gray space. Instead, if for instance the GRU (Russia’s military intelligence agency) controls a node in the Netherlands, it is considered to be red space based on JP 3-12.xx And it is worth mentioning that the notion of control is open to interpretation by states.

This means that if U.S. Cyber Command seeks to operate only in “red space,” its activities will still have global reach. It also suggests that red space grows as adversaries expand their operational activity. Most importantly, this implies that if U.S. Cyber Command seeks to achieve “effects” in gray space, this will involve operating infrastructure that adversaries do not control—which is to say those systems or networks on which adversaries merely have a presence or are not active at all.

### AT: US unilat CP/Squo solves

#### US unilateral persistent engagement and defend forward undermines trust and causes friction when allies don’t want US to operate in allies’ space

**Smeets,** ETH Zurich, Center for Security Studies, **2020**

[Max “U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection” Intelligence and National Security vol 35, 2020 – Issue 3, Taylor and Francis Online accessed 7/5/2022 GDI-TM]

Risks for Allies and Intelligence Collection

This section addresses four connected risks associated with US strategy. The first risk is perhaps the most obvious: if U.S. Cyber Command directly operates in allied networks without consent, it creates friction by allies undermining trust. Operating instantly makes sense considering the potential operational tempo of adversaries: You cannot have protracted diplomatic discussions for two months with an ally about whether or not to take down some command and control infrastructure of an adversary hosted in the allied country. You don’t have days, let alone months. As a participant mentioned at the 2019 Cyber Command Symposium on strategy: “Opportunities within this domain are fleeting.”xxxviii

Operating seamlessly could also make sense if an ally does not mind the U.S. coming into its networks to address the malicious activity. In this vein, the U.S. can continue to build partnerships with countries that do not have the capacity to defend against cyber attacks on their own, as described above. But, what if an allied country is not keen on having the U.S. military in its networks, actively, seamlessly, and continuously disrupting an adversary’s cyber operations? As the German case shows, this scenario will likely come up a lot more in the near future.

#### US unilateral action undermines data collection and ongoing intelligence efforts of allies, altering TTP strategies mid-stream

**Smeets,** ETH Zurich, Center for Security Studies, **2020**

[Max “U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection” Intelligence and National Security vol 35, 2020 – Issue 3, Taylor and Francis Online accessed 7/5/2022 GDI-TM]

Second, it is not just about cyber effect operations taking place in systems or networks in allied territory. There could also be a negative impact on allied intelligence operations and capabilities beyond these systems and networks. The U.S Cyber Command - and other military cyber organizations - are operating in a global environment historically dominated by intelligence agencies, and the Five Eyes has always been the most dominant actor in cyberspace.xxxix But the anglophone intelligence alliance is not the only intelligence actor operating across the world. Recent cases—such as the infiltration of the Dutch General Intelligence and Security Service into the Russia-based network of the infamous hacking group Cozy Bear—have illustrated the continued global prevalence and value of allies’ intelligence operations beyond the Five Eyes alliance.xl If U.S. Cyber Command increasingly take up the role of ‘disrupter’ it may negatively impact global intelligence collection of allies—particularly those countries that favor long-term access over immediate effect. It will also more likely uncover and burn allied capabilities.

The risks of occurring are higher than one may think as intelligence agencies have a tendency and incentive to target and track the same entities. For example, in late 2014, cybersecurity company Kaspersky Lab reported on the so-called "Magnet of Threats”. The cybersecurity company discovered a server belonging to a research organization in the Middle East that simultaneously hosted implants for at least five Advanced Persistent Threat (APT) actors: Regin and the Equation Group, Turla and ItaDuke, Animal Farm, and Careto.xli All of these APTs have been associated with prominent national security and intelligence agencies. Equation group and Regin are connected to the Five-Eyes. As said, Animal Farm has been attributed to France's external intelligence agency. Turla Group has been associated with the Russian federal security service (FSB). ItaDuke is said to be linked to the Russian government too. Finally, it is theorized that Spain is behind Careto, also known as ‘The Mask’.

Consider what would have happened if one of those five APT groups had sought to cause a disruptive effect - rather than collect intelligence - against the target in the Middle East. It likely would have resulted in much earlier discovery and analysis by threat intelligence companies (or other actors) exposing the tactics, techniques and procedures (TTPs) of each actor group.

Also, even the anticipation of more cyber effect operations in non-allied networks from one allied state could lead to a change in operations by another state. Indeed, states have shown in the past that the anticipation of early discovery of an operation has led to a change in their TTPs. For example, the National Security Agency (NSA) created an "exploit orchestrator" called FoxAcid, an internet-enabled system capable of attacking target computers in a variety of different ways, depending on whether it is discovered—or likely to be discovered—in a given network.xlii FoxAcid has a modular design, with flexibility allowing the NSA to swap and replace exploits and run different exploits based on various considerations. Against technically sophisticated targets where the chance of detection is high, FoxAcid would normally choose to run low-value exploits.

#### Russia exploit frictions with allies that result from US unilateral actions that allies do not want to occur in their spaces -

**Smeets,** ETH Zurich, Center for Security Studies, **2020**

[Max “U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection” Intelligence and National Security vol 35, 2020 – Issue 3, Taylor and Francis Online accessed 7/5/2022 GDI-TM]

Third, allied friction could potentially be exploited by adversaries. Adversaries do not randomly choose which intermediate nodes to direct their operations through. If Russia has the choice to go through a network that would raise some serious diplomatic friction between the U.S. and a U.S. ally, or operate through a network that would cause no diplomatic friction for the U.S., what would it prefer?

It would make sense for adversaries to operate through the networks of exactly those countries with which the U.S. has a strong relationship but that do not want the U.S. to operate within their networks causing any effects. Russia is already good at exploiting divisions between the U.S. and its allies. Cyber Command’s new strategy might give it another avenue to do so.

### AT: allies model US policies

#### Turn – allies modeling US persistent engagement creates transforms allies’ networks into red and grey spaces

**Smeets,** ETH Zurich, Center for Security Studies, **2020**

[Max “U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection” Intelligence and National Security vol 35, 2020 – Issue 3, Taylor and Francis Online accessed 7/5/2022 GDI-TM]

Fourth, whilst allies can integrate their cyber efforts into U.S. strategy of persistent engagement, if allies would adopt their own strategy of persistent engagement - mirroring U.S. current doctrine and practice

- it would likely further undermine the alliance relationships. If US strategy of persistent engagement leads allies to adopt their own strategy of persistent engagement, it would mean allies also seek “superiority in cyberspace”; “continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver”; and operating “seamlessly, globally and continuously” - as stated in the Cyber Command vision. More specifically, it would mean that allies seek to swiftly achieve effects in systems and networks that are potentially located on U.S. territory, without necessarily notifying the U.S. government before. In other words, it means that networks and systems turn into red space and gray space for allies - like allied networks are now gray and red space for the U.S. to actively disrupt and degrade adversarial operations.

It is unlikely that the U.S. government would react positively if Germany, or any other allied country for that matter, hacks into a server hosting Russian propaganda that was located in the United States, with some form of notification but without Pentagon’s consent.xliii There are numerous reasons why the US government would be upset with this type of behavior. It would likely be seen as reckless from Germany - especially if the US was already on those same networks for intelligence collection purposes.

An important dimension of this scenario is derived from the fact that the U.S. is a vast target rich environment, potentially even prioritized as a target by adversaries such as China, Russia, North Korea, Iran - as well as non-state actors. As stated above, red space and gray space are defined, according to U.S. Joint Publication 3-12 on Cyberspace Operations, based on what “nodes” adversaries “control”. There are many nodes adversaries (of US allies) want to control in the US. In other words, if US allies would seek to swiftly disrupt and degrade cyber operations in red space and gray space on a constant-basis, much of that would be in the United States.

### AT no consensus amongst allies of offensive capabilities

#### Process of integration of offensive capabilities into exercises for deterrence can occur as part of process of consensus building on offensive cyber capabilities

**Lonergan** , assistant professor in the Army Cyber Institute at West Point and research scholar at the Saltzman Institute of War and Peace Studies at Columbia University **and Montgomery**, senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies, **2022**

Next Steps: Addressing Challenges and Mitigating Risks

Given the threat environment facing NATO, as well as the activities of several NATO members, the alliance should deliberately—but purposefully—consider incorporating offensive cyber operations below the level of armed conflict into its deterrence strategy. Any effort to explore a role for offensive cyber operations should also consider the challenges and risks that may come with doing so. A central challenge is that, at the political level, NATO allies lack consensus on the appropriate application of offensive cyber power—especially below the level of armed conflict. Addressing these disagreements among member states is essential because conducting offensive cyber operations often requires maneuvering through or operating on networks controlled by an ally or allies. Right now, NATO members do not collectively agree on the protocols and processes for partner actions in allied networks—and they also disagree on how to define sovereignty in cyberspace, or when an offensive cyber operation would rise to the level of an armed attack.

Offensive cyber operations for NATO also present real interoperability challenges. The role of intelligence in cyber operations is likely to complicate NATO planning processes. Even close allies are likely to be wary about sharing sensitive intelligence for a number of reasons. For instance, they may be averse to sharing information gleaned from signals intelligence collection or because a member state may be using the same exploits for both offensive action and their own espionage—including intelligence collection against allies. Or, allies may simply be worried that sensitive information may become exposed. On top of this, it’s challenging to adjudicate intelligence requirements among allies and to deconflict intelligence and military priorities. It is also not clear whether the alliance has established consensus thresholds that specify the conditions and timeline under which a state would have to notify others of its activities on their networks—if at all.

The alliance should account for, and address, these issues as NATO explores the prospect of incorporating offensive cyber operations below the level of armed conflict into existing NATO simulations and exercises that span the strategic, operational, and tactical levels. A number of important questions about how to coordinate offensive cyber operations and define roles and responsibilities remain unanswered. For instance, how could allies improve intelligence sharing to conduct more rapid attribution, enabling one state or the alliance to respond to adversary cyber activity? What are the conditions under which allies should consider dividing responsibilities for cyber campaign planning and developing accesses and capabilities against strategic targets in, for example, Russia? If some allies are responsible for offensive cyber operations against certain targets, what are the information-sharing and notification requirements?

### AT offensive cyber causes escalation

#### No evidence of escalation from offensives cyber – studies prove

**Lonergan** , assistant professor in the Army Cyber Institute at West Point and research scholar at the Saltzman Institute of War and Peace Studies at Columbia University **and Montgomery**, senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies, **2022**

Finally, there is an obvious risk that moving toward a more offensive posture in cyberspace will increase the likelihood of escalation. **While these concerns should not be ignored, academic research has found little support for the argument that cyber operations cause escalation**. That said, the alliance should consider how to strengthen existing confidence-building measures, particularly with Russia, to enable more effective communication and transparency about cyber operations. The expert consultations between Russia and the United States that both governments agreed to in June 2021, for example, or recent diplomatic dialogue between Russia and NATO members over the Ukraine crisis, are important to strengthen processes for crisis management and reduce the risk of instability—including that which may stem from cyber operations.

NATO has slowly begun to address the use of offensive cyber operations, and has generally limited itself to the use of these tools in traditional military campaigns. The ongoing crisis with Russia on Ukraine’s border is exposing the risk in this approach. NATO needs to figure out a way forward fast.

### Squo – US Cyber command unilateral actions – international law risk

#### US Cyber Command shifts role of the military to active disrupter – and may run afoul of international law

**Smeets,** ETH Zurich, Center for Security Studies, **2020**

[Max “U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection” Intelligence and National Security vol 35, 2020 – Issue 3, Taylor and Francis Online accessed 7/5/2022 GDI-TM]

What is really new here? The United States has long operated in networks “close to the adversary.” As Ben Buchanan’s book, “The Cybersecurity Dilemma,” demonstrates, the U.S. has long acted as an observer outside of its own networks, gathering intelligence of adversarial activity in those others’ networks.xxi In fact, information has become public concerning a case in which the Five Eyes collected intelligence about an espionage platform (dubbed “Snowglobe” by the Canadian Intelligence Agency CSEC and “Animal Farm” by Kaspersky Lab) of an allied country, France, likely operating in adversarial networks in the Middle East.xxii In other words, the practice of fourth-party collection is nothing new.xxiii Furthermore, the U.S. has long acted in foreign non-adversarial networks as a passerby, transiting through allied’ networks to access an adversarial network.

Yet, the new Cyber Command and Defense Department strategy changes the nature of the U.S. military’s behavior within those systems and networks. Under the new strategy, Cyber Command wants to be an active disrupter on those networks. It wants to achieve effects - that is to disrupt, deny, degrade, and/or destroy. The only known precedent is U.S. Cyber Command operators wiping Islamic State propaganda material off a server located in Germany.xxiv The German government was notified in some fashion but not asked for advance consent, causing much frustration.xxv This will likely lead to a systematic scaling up: U.S. Cyber Command now also seeks to be an active disrupter on those networks “globally, continuously and seamlessly”—not regionally and sporadically.xxvi

Out of network operations in allied networks also affect the turf war between the NSA and Cyber Command - mostly critically Title 10 and Title 50 concerns.xxvii As Chesney summarizes:

From a legal perspective, the issue this [case of Germany] highlights is that operations abroad implicate the UN Charter and related claims about international law protection of sovereignty. […] Intelligence agencies can more easily act in this setting when operating under Title 50 authority, as covert action status carries with it a statutory obligation to comply with the U.S. Constitution and U.S. statutes—but no more than that. Title 10, in contrast, carries with it no such implicit statutory shield against international law objections, and of course there is a general Defense Department policy of international law compliance. Thus CYBERCOM operating under Title 10 would run into the full thicket of international law concerns.xxviii

Overall, it is expected that operating in allied networks under Title 10 is likely to cause more legal friction than operating under Title 50.

## Personnel

### US key – educational framework

#### New education programs modeled after US frameworks solve personnel gaps

Ablon et al, 2019

[Lillian, information scientist at the RAND Corporation and a professor at the Pardee RAND Graduate School, "Operationalizing Cyberspace as a Military Domain", RAND, 6/19/19, https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE329/RAND\_PE329.pdf, accessed 7/3/22, GDI-cc]

NATO relies on its member nations to send qualified  personnel on rotation, but NATO also has longer-serving  staff among its civilian personnel. Whether employees have  served for three years or 30, NATO will want to ensure that  its cyber workforce has a baseline of skills and knowledge  and develop progressive educational modules to grow and  sustain its human capital. As already noted, the baseline  will vary depending on the work roles and job series a  person occupies. The U.S. Department of Defense (DoD)  has developed a DoD Cyber Workforce Framework that  encompasses four main categories of personnel: cyberspace  IT, cybersecurity, cyberspace effects, and intelligence.55 NATO could also look to bring in expertise on short-term  assignments similar to the U.S. Defense Digital Service.56 It could also develop industry fellows programs to give its  permanent staff experience in the private sector, similar to  the U.S. Secretary of Defense Executive Fellows program.57 These programs could inject new thinking and bring valu able private-sector experience to bear.

NATO’s educational institutions will play a critical role  in developing and sustaining the cyberspace workforce for  the alliance, starting with instituting courses that cover  relevant topics, from strategy and policy to more technical  areas. Some suggested topics to include in a first orienta tion course that establishes the baseline (some of which are  already being taught) would include

• NATO organizational structure and national-level  organizations that interface with the alliance. This  would include covering the roles and responsibilities  of the NCIRC, ACO Cyber Division, ACT Cyber  Capabilities Branch, and the CyOC, as well as  national-level cybercommands and EU institutions.

• strategic and operational planning, including how  cyber operations fit into the COPD and the NATO  Crisis Management Process.

• technical topics for those less familiar with the layers  of the cyber domain, from the physical infrastruc ture to the virtual or “cyber persona” domain.

• cyberspace capabilities in the alliance and at the  national level, including defensive capabilities.

• the legal and policy frameworks for cyber oper ations, including the law of armed conflict and  its application to the cyber domain, operational  authorities, and NATO declarations and policies.

### NATO needs personnel

#### Skilled cybersecurity personnel and adaptation of NATO’s educational programs key to address emerging cyberspace issues

Ablon et al, 2019

[Lillian, information scientist at the RAND Corporation and a professor at the Pardee RAND Graduate School, "Operationalizing Cyberspace as a Military Domain", RAND, 6/19/19, https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE329/RAND\_PE329.pdf, accessed 7/3/22, GDI-cc]

NATO will need staff officers, civilian personnel, and  other augmentees who not only are steeped in the technical  aspects of cyberspace but also understand how cyberspace  operations can contribute to the overall success of NATO operations and how other domains can reinforce the cyber  domain. NATO is starting to adapt its educational curriculum to address the full array of cyberspace issues. The  NATO Communications and Information Agency has built  a new school in Portugal to support its mission and teach  staff about the operation of NATO IT systems.53 Other  academic institutions, such as the NATO Defence College,  the NATO School Oberammergau, or the Cooperative  Cyber Defence Centre of Excellence, should also implement  courses focusing on cyberspace as a domain of operations.

The competition for skilled cybersecurity personnel is  well documented. The cybersecurity certification organization, (ISC)2, noted in a recent report that the workforce  shortage of these professionals is growing globally, reaching almost three million positions in 2018.54 Nearly half  of the surveyed organizations for that report expected to  increase cybersecurity staffing in the next year, underscoring that demand will grow, not diminish. NATO undoubtedly will be among those organizations competing in the  labor marketplace for skilled cybersecurity professionals,  but as we have seen, it will require more than technical  staff. It will need to educate its leadership, both military  and civilian, in the technical, operational, legal, and policy  topics of cyberspace.

Officers and civilian personnel assigned to NATO  on rotations will come with varied backgrounds and  experience for the positions they will fill. Some positions,  such as in the cyber offices at Allied Command Operations  (ACO), ACT, and the new CyOC will clearly need personnel who have a deeper experience than the broader orga nization, something that will likely rely on personnel from  a subset of the member nations for the near future, given  the wide variance in national experience in cyberspace.  But other parts of NATO will also need to draw on cyber  expertise to ensure cyberspace integration into operations,  including at the various operational headquarters.

## Resiliency

### Resiliency – NATO coordination

#### Solvency – incorporating safeguards into NATO to monitor allies’ defense preparations and reduce reliance on non-allied energy and critical infrastructure reduces vulnerabilities and increases resilience

**Becker et al.**, affiliated with the Centre for Security, Diplomacy and Strategy at the Vrije Universiteit Brussels, **2022**

(Jordan, academy professor and director of the Social Science Research Lab at West Point academy, “DON’T LET RUSSIA DOMINATE THE STRATEGIC CONCEPT,” War on the Rocks, JUNE 28, 2022, https://warontherocks.com/2022/06/dont-let-russia-dominate-the-strategic-concept/, accessed 7/3/2022, gdi-tmur)

Although defending human and physical infrastructure from asymmetric threats is inherently national business, NATO itself can serve as a platform for coordinating allied responses to these challenges. NATO allies agreed on seven baseline requirements for national resilience at their 2016 Warsaw Summit. They have also “improve[d] their cyber resilience by introducing capability targets” into the NATO Defence Planning Process.

Recently, however, national resilience has been challenged in additional areas, which should be reflected. Specifically, NATO should address democratic backsliding, election interference, and economic and information manipulation. Specifically, NATO’s requirements for national resilience should be upgraded to require national safeguards against democratic backsliding. Prior to taking up her position as the senior U.S. Department of Defense official in Europe, Rachel Ellehuus highlighted the vulnerabilities laid bare by such backsliding and argued that “the trans-Atlantic alliance will only remain strong if members genuinely abide by its founding principles.” By incorporating such safeguards into NATO’s systems for monitoring allies’ defense preparations, allies can shape one another’s political, economic, and security incentives in ways that reduce these vulnerabilities.

Allies should also agree to reduce dramatically their reliance on non-allied energy — the vulnerabilities inherent in German dependence on Russian gas have been exposed during the Russo-Ukrainian war. Progress toward independence cannot come fast enough. Finally, non-allied ownership of critical infrastructure, especially transportation and telecommunications, poses risks that have not yet materialized in the same way as energy dependency but are just as dangerous. The risks should be explicitly addressed in the strategic concept, and concrete steps toward mitigation should increase accordingly. Military mobility remains a critical infrastructural challenge that allies should also explicitly grapple with in coordination with the European Union. As in the cyber realm, the NATO Defence Planning Process may be an appropriate venue for these efforts.

## Zero –trust architecture

### Solves Russia

#### Resilient cyber capabilities and effective security approaches like zero-trust policies produce effective cyber defense against Russia

**Kramer and Pavel, 2022**

[Franklin, distinguished fellow and board director of the Atlantic Council and Former Assistant Secretary of Defense for International Security Affairs, and Barry, director of the Scowcroft Center for Strategy and Security at the Atlantic Council, "NATO priorities: Initial lessons from the Russia-Ukraine war", Atlantic Council, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/nato-priorities-initial-lessons-from-the-russia-ukraine-war/, accessed 7/3/22, GDI-cc]

In the event of a conflict with Russia, a successful defense will depend heavily on resilient cybersecurity capabilities, in order to maintain the operation of key critical infrastructures necessary to defense mission assurance. Achieving that goal will require not only government efforts, but also the establishment of an effective coordination mechanism between governments and the private sector, as the latter will be significantly engaged in the cyber fight.

Russia’s substantial cyberwarfare against Ukraine underscores the importance of such effective cybersecurity. As NATO’s assistant secretary general for intelligence has described:

All available evidence indicates that Russia has employed a coordinated cyber-campaign intended to provide its forces with an early advantage during its war in Ukraine…[T]the magnitude of Moscow’s pre-kinetic destructive cyber-operations was unprecedented. On the day the invasion began, Russian cyber-units successfully deployed more destructive malware—including against conventional military targets such as civilian communications infrastructure and military command and control centers—than the rest of the world’s cyberpowers combined typically use in a given year…The cumulative effects of these attacks were striking. In the hours prior to invasion, Russia hit a range of important targets in Ukraine, rendering the computer systems of multiple government, military, and critical infrastructure sectors inoperable.”

NATO needs to anticipate that in any conflict with Russia, it would face the same types of cyberattacks. Maintenance of governmental functions and reasonably adequate operation of critical infrastructures, especially those necessary to defense mission assurance, would be critical. Through the defense-planning process, NATO should set as a goal a cybersecurity plan that utilizes the most effective cybersecurity approaches, namely a combination of zero-trust architectures, advanced threat hunting, and continuous vulnerability analysis.

The Massachusetts Institute of Technology’s Lincoln Laboratory has described zero-trust (ZT) architectures:

The core principles behind ZT are: 1) universal authentication of all users, devices, and services; 2) access segmentation, allowing no single entity access to more than a small portion of the organization’s resources; 3) minimal trust authorization, keeping access to resources only to those entities that “need-to-know” and can be trusted; 4) encryption everywhere to protect information in flight and at rest, whether inside or outside the organization’s networks; and 5) continuous monitoring and adjustment to detect issues early and adjust access accordingly.”

# CP Answers

## EU

### Perm – EU NATO cooperation – general

#### NATO consistent assessment to test national cyber policies, including collective cyberspace defense – cooperation with the EU solves best

\*\*perm solvency – NATO take lead to work with EU

**Ahlawat, 2021**

[Urjasvi, Jindal School of International Affairs and Research Intern at the Centre for Security Studies, “NATO: CYBERSECURITY AND CYBER COALITION“CSS ISSUE BRIEF, January 2021, https://jgu.s3.ap-south-1.amazonaws.com/jsia/Urjasvi+-+NATO+Cybersecurity.pdf accessed jcp-tm 6/9]

CONCLUSION

Thus, in conclusion, several member states fail to adopt and review their national cyber- security policies, considering the promise at the Warsaw NATO Summit. As a result, NATO's attempts to develop alliance-wide cybersecurity are hampered by considerable national contradictions, and NATO's collective cyberspace defence and deterrence also reveal significant vulnerabilities against the background of a rising amount of attacks. **For NATO to operationalize cyberspace as a sphere of NATO security policy and planning, the Alliance should have permission from member states to do more than just provide guidance, experience, training, or instruction. NATO should establish benchmarks and better metrics that allow a consistent assessment** of the annual success of a country and should be charged annually with testing and assessing the skills of members**. Cooperation with the European Union is necessary to meet this goal. NATO and the EU might work together to create minimum standards and benchmarks for cybersecurity that the European Defence Agency will then implement.**

### Perm – cyber resiliency

#### Perm solves – NATO-EU cooperation for EDTs solves - European digital defense shield and cyber training

**Bonefeld-Dahl**, Director General of DIGITALEUROPE, **2022**

(Cecilia, “Preparing Europe for cyberwarfare,” The Parliament Magazine, March 28, 2022, lexis, accessed 6/28/2022, gdi-tmur)

\*ESET = a Slovak internet security company

It is no surprise therefore that malicious cyber-attacks have skyrocketed following the Russian invasion of Ukraine. ESET has identified several new strains of malware, which they have called IsaacWiper and HermeticWizard, and they have even found evidence that a cyberattack had preceded the start of the Russian invasion of Ukraine by a few hours.

So how prepared are European governments today for a potential cyber or military attack?

Unfortunately, numbers show that over the past few years, there has been little political will among European NATO members to contribute to common defence efforts. The US spends more than all of the other 29 NATO members combined. In 2020, it's estimated that the US defence contribution reached over 3.7% of GDP, while the average for NATO's European members (and Canada) was stalling at 1.77% of GDP, below the 2% of GDP commitment made by all defence ministers back in 2006.

With the current devastating war underway in Ukraine and the imminent Russian threats to the rest of Europe, European NATO leaders should urgently increase funding to 3% and dedicate at least 1% of spending to emerging and disruptive technologies (EDTs).

EDTs such as artificial intelligence, quantum technology and robotics are set to have a tremendous impact on cyber-defence and to revolutionise future military strategies and operations. It is vital that the EU and its NATO allies stay at the forefront of technological advances.

As NATO's Deputy Director General Mircea Geoana said at our Masters of Digital event back in February:' "In the 70's, 80% of innovation was produced by governments. Now the ratio has been reversed, today about 90% of security and defence innovation comes from the private sector."

As cyberwarfare is worryingly becoming more devastating, from political destabilisation to wreaking havoc on energy infrastructure to misinformation, NATO and the EU need to urgently bolster their cooperation to create a more resilient cybersecurity ecosystem based on digital innovation.

Beyond the importance of political will and financial investment, it is equally vital to close the gap in the cybersecurity workforce. According to the latest count, Europe's shortage of cybersecurity professionals has increased, reaching over 200,000 needed specialists in 2021. In the context of a devastating pandemic and a devasting war, the need for more cybersecurity professionals is expected to outpace available talent.

“EDTs such as artificial intelligence, quantum technology and robotics are set to have a tremendous impact on cyber-defence and to revolutionise future military strategies and operations"

The EU should redouble skilling efforts through existing programmes such as the Digital Europe Programme and Horizon Europe. Students and especially young girls and women should be highly encouraged to pursue a career in this field as disappointingly women make up only 20% of the cybersecurity workforce.

Finally, the EU and the US need to harness their collaboration on cybersecurity through the EU-US Trade and Technology Council (TTC). Today, more than ever, regulatory alignment on policies such as the Artificial Intelligence Act is of a paramount importance. As part of our key priorities recommendations for the upcoming TTC meeting, we have called on both allies to initiate a dialogue on mutual recognition of cybersecurity certification regimes.

The Russian invasion of Ukraine has been a wake-up call to all political leaders that collective security should be taken seriously in peace as much as in war. Today, digital technologies are not simply components of security systems; they are at the very heart of these systems. We must ensure that digital innovation is the cornerstone of any European defence shield.

### No solvency – data governance

#### Inconsistent data governance standards undermine cybersecurity cooperation effectiveness

**Selga, 2021**

[Eriks, Digital Innovation Baltic Fellow with the Transatlantic Leadership team, Visiting Researcher at the Latvian Institute of Foreign Affairs, Associate Scholar at the Foreign Policy Research Institute; “Building Common Ground in Transatlantic Cybersecurity – A Baltic Approach” The Center for European Policy Analysis August 27 2021 <https://cepa.org/building-common-ground-in-transatlantic-cybersecurity-a-baltic-approach/> accessed 6/9 jcp-tm]

Most sectors in the transatlantic alliance are quickly becoming digital, growing increasingly dependent on data flows to provide vital goods and services. As a consequence, the ambit of cyber risk is expanding proportionately, becoming increasingly costly.1 The Colonial Pipeline ransomware attack in May resulted in fuel shortages in several states and directly increased fuel prices.2 The SolarWinds supply chain attack, detected in December of 2020, targeted a third-party service provider, leaving vulnerable more than 18,000 entities worldwide, including U.S. agencies like the Department of Defense, the Department of Homeland Security, the State Department, as well as NATO systems, European government agencies, and Fortune 500 companies.3 In 2017, NotPetya erased the capital assets of hundreds of companies in minutes by encrypting and wiping their information technology systems with damages so costly they impacted national GDPs. These cyberattacks travelled across devices, sectors, jurisdictions, and oceans to ultimately inflict damage.

Cybersecurity is thus a growing priority. It is fast expanding in scope from protecting just critical infrastructure, like energy and finance, to protecting critical functions, like water distribution and payment processing, and increasingly the safety and stability of the structures and individuals underpinning them. The ambit of cyber threats is gradually creating a data complex that ties together the digital vulnerabilities of public, private, civilian, and military sectors. Yet, widening divergences in U.S. and European Union (EU) data governance approaches are limiting the interoperability of data between these sectors, directly impacting the ability of the alliance to counter the growing array of cyber risks.

The U.S. liberal market-based approach to data centers around data ownership rights, upholding a property-based regime where companies can process personal data by default.4 In turn, to extend the single market into the digital realm, the EU approach to data is focused on harmonizing data regimes between its 27 member states, generally through heavy-handed rights-based regulation.5 These differences in governance have extended into broader forks in the handling of data sharing architecture, personal data protection regimes, and digital intelligence orders.

Each bifurcation in data policy adds a layer of complexity to cybersecurity initiatives in the form of new technical standards, trust services, or supply chain certification considerations. However, the current transatlantic cybersecurity status quo is not yet equipped to handle the variance in data governance regimes. In the United States, the main cross-sectoral cybersecurity framework is created by the National Institute of Standards and Technology (NIST) in the form of a nonbinding set of best practicesthat companies can apply. On the other hand, the EU’s Network and Information Security Directive (NIS Directive) stipulates digital service providers operating across Europe enact mandatory cybersecurity frameworks. In such a scenario, the data of an international company that operates in both markets will travel through servers that may have fundamentally different cybersecurity frameworks, risk management systems, or incident reporting requirements.

Kept unaligned, these differences risk extending gaps between the cybersecurity efforts of the transatlantic partners, as well as creating new ones as new digital initiatives develop. Four working groups within the recently formed U.S.-EU Trade and Technology Council are dedicated to coordinating information and communications technology (ICT) and data governance challenges — an important indicator of the priority of digital governance and of the political will to find common ground.6 In this policy brief, the critical pain points for transatlantic cybersecurity cooperation are addressed, outlining rising divergences in data architecture, data protection regimes, law enforcement cooperation, and cyber interventionist capacity.7 After highlighting how these divergences create new cybersecurity gaps, the problem is addressed. The Baltic approach, characterized by a flexible governance structure, offers one model of how the transatlantic alliance can leverage data governance from the bottom up, toward a more integrated transatlantic data relationship.

### Coop = normal means – Strategic Concept

#### EU and NATO agree to avoid duplication and to cooperate on multiple items – normal means

**Monaghan, et al 2022**

[Sean, visiting fellow in the Europe, Russia, and Eurasia Program at the Center for Strategic and International Studies, "What Happened at NATO’s Madrid Summit?", CSIS, July 1 https://www.csis.org/analysis/what-happened-natos-madrid-summit, accessed 7/3/22, GDI-cc]

Q8: Has the Madrid Summit boosted EU-NATO cooperation?

A8: The strategic concept cites the European Union as a “unique and essential partner” and calls for greater cooperation on countering hybrid tactics, counter terrorism, addressing human security challenges, military mobility, resilience, climate change, EDTs, NATO’s Women, Peace, and Security agenda, and addressing China’s “systemic challenges.”

Existing EU-NATO cooperation already tackle most of these, but the focus on human security and countering China are new. One notable absence is a reference to maritime security, which was one of the original seven areas for EU-NATO cooperation the organizations identified in 2016. It should be noted the European Union has a growing ambition in this space.

Another absence concerns coordination on capability development, which has generated transatlantic tensions: the United States and some other allies have worried a larger role for the European Union on defense might siphon resources and focus away from NATO. The final language reflects a compromise in this regard: “Initiatives to increase defence spending and develop coherent, mutually reinforcing capabilities, while avoiding unnecessary duplications, are key to our joint efforts.”

# DA Answers

## general

### US leadership now – Ukraine

#### US asset contribution high now – Ukraine proves

**Shea, 2022**

[Jamie, Associate Fellow, International Security Programme “NATO must now transform old missions into new strategy” Chatham House, June 21 2022 <https://www.chathamhouse.org/2022/06/nato-must-now-transform-old-missions-new-strategy> accessed GDI-TM]

As a revitalized NATO alliance deals with a crisis that has major economic and humanitarian as well as military dimensions, the need for it to develop both a European and a global containment strategy grows ever more urgent.

Bolstering NATO’s defences so as to provide the capability to repel any form of Russian attack on land, at sea, in the air, or through space and cyberspace is a key aspect of this strategy as, in recent weeks, more combat forces able to defend territory have taken the form of additional troops, ships, and aircraft reinforcing the Baltic states and the Black Sea coastlines of Poland and Romania.

Ten allies have so far contributed to this effort, placing 40,000 troops under direct NATO command. Those sceptical about the future of the transatlantic security relationship have been confounded by the major role the US has played in this effort, sending parts of the 82nd Airborne Division and 3rd Armoured Division to Poland, and redeploying US Stryker brigades from Germany and Italy to the Baltic states and Romania.

Although many other allies have sent useful assets – such as French and UK aircraft to Romania or German and Netherlands Patriot batteries to Slovakia – the US contribution still surpasses all European efforts put together. The US now has 100,000 troops in Europe, the most it has deployed there since the mid-1990s.

## Midterms/Politics

### US NATO cyber coop – not key to midterms

## NATO Overstretch/Focus

### Non-unique – cyber focus now