# Cyber Info Aff

## 1AC

### 1ac – Cyber War

#### Cyberattacks are increasing now – the frequency and severity are threatening NATO operations and infrastructure.

Maigre ’22 (Merle Maigre is a Non-resident Senior Fellow with CEPA's Transatlantic Leadership Program and CEPA's Digital Innovation Initiative, as well as the Senior Cyber Security Expert at Estonia’s e-Governance Academy, a non-profit that helps governments go digital. “NATO’s Role in Global Cyber Security,” April 2022, German Marshall Fund of the United States at Harvard University, https://www.gmfus.org/sites/default/files/2022-04/Maigre%20-%20NATO%20-%20Geopolitics%20-%20Cyber%20-%20final.pdf)-mikee

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 professionals 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.11ENISA: European Union Agency for Cybersecurity, The Year in Review. ENISA Threat Landscape from January 2019 to April 2020, 2020. 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.22NATO Cooperative Cyber Defence Centre of Excellence, Recent Cyber Events: Considerations for Military and National Security Decision Makers, No. 10, May 2021.¶ According to the FireEye Mandiant Special Report: M-Trends 2021, the top five most targeted industries 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 transfers. 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.33Fire Eye Mandiant Services, Special Report, M-Trends 2021, pp. 17-19.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, prominent 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.44Ciaran Martin, “Cyber Criminals Will Cause Physical Harm,” Wired, February 2, 2022 Another set of threats comes in the form of belligerent 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 undetected for months before the victims discovered vast amounts of their data had been stolen.55Jack Stubbs, Raphael Satter, and Joseph Menn, “US Homeland Security, thousands of businesses scramble after suspected Russian hack,” December 14, 2020. 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.66Catalin Cimpanu, “Finland says hackers accessed MPs’ email accounts,” ZDNet, December 28, 2020. 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.77BBC, “Norway blames Russia for cyberattack on parliament,” October 13, 2020. 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 government has been hit by a series of cyberattacks that defaced government websites and wiped out the data on some government computers. In mid-January, 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 Transformation, whose e-governance portal gives the Ukrainian public digital access to dozens of government 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.88Kim Zetter, “What We Know and Don’t Know about the Cyberattacks Against Ukraine,” Substack, January 17, 2022. The international hacktivist collective Anonymous has declared “cyberwar” against Russia’s government, claiming credit for several cyber incidents including distributed denial of service attacks that took down Russian government websites and Russia Today, the state-backed news service.99Monica Buchanan Pitrelli, “Global hacking group Anonymous launches ‘cyber war’ against Russia,” CNBC, March 4, 2022. Around the globe, **aging critical infrastructure has long been vulnerable to attack**. The most worrying type of cyberattack is sophisticated 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 infrastructure operators and government agencies.1010Alix Pressley, “The ‘cumulative effect’ of ransomware and the lessons for UK national infrastructure,” Intelligent Cio, July 20, 2021. 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 WhisperGate, discovered in January by Microsoft, in Ukraine’s networks that “provide critical executive branch or emergency response functions”;1111Microsoft Security, Destructive malware targeting Ukrainian organizations, January 15, 2022. HermeticWizard and IsaacWiper,1212ESET Research, IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine, March 1, 2022. targeting multiple Ukrainian organizations just hours before the Russian invasion began; and CaddyWiper, spotted by researchers at the Slovak internet security company ESET in mid-March.1313ESET Research, CaddyWiper: New wiper malware discovered in Ukraine, March 15, 2022. 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.”1414Dmitri Alperovitch, “How Russia Has Turned Ukraine Into a Cyber-Battlefield,” Foreign Affairs, January 28, 2022. 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. While they can offer some advantages in military operations, cyberattacks also have limitations in feasibility and effect. In the event of military attacks, military objectives can be supported by intelligence-gathering operations, operations aimed at disrupting the opponent’s military, and psychological operations against the opponent’s public.1515Ibid. 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.1616Ciaran Martin, “Cyber Realism in a Time of War,” Lawfare, March 2, 2022. The Russian military exercise Zapad 2021 in September included one of the largest uses of electronic 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.**”1717Roger McDermott, “Russia’s Electronic Warfare Capabilities to 2025,” ICDS, September 2017. Russia sees EW as a seamless whole, ranging from kinetic combat operations on the battlefield to missions in cyberspace and the information domain.1818Jonathan Marcus, “Zapad: What can we learn from Russia's latest military exercise?” BBC, September 20, 2017. While there were no public sources confirming any navigation or communications disruption by the Baltic-Polish defense leadership during Zapad 2021, **it is nevertheless important that NATO continue to adapt to the evolving cyber-threat landscape**.

#### Status quo NATO efforts aren’t enough – deterrence, defense, and interoperability are failing because of a lack of coordination.

Blessing ’21 (Dr. Jason Blessing is a Research Fellow at the American Enterprise Institute and a returning DAAD Postdoctoral Fellow at the Foreign Policy Institute of Johns. “Fail-Deadly, Fail-Safe, and Safe-to-Fail: The Strategic Necessity of Resilience in the Cyber Domain,” Chapter 12 in NATO 2030: Towards A New Strategic Concept and Beyond, SAIS Press, 2021, <https://www.sais.jhu.edu/sites/default/files/NATO2030AndBeyondAccessibleVersion.pdf)-mikee>

There are, however, several dynamics that reveal the limits of the fail-deadly and fail-safe logics underlying NATO’s collective defense initiatives. In short, these strategic logics only apply to a narrow set of threats; they will not apply to the full spectrum of threats presented by the cyber domain. Fail-deadly deterrence is only likely to succeed in preventing state-level adversaries from undertaking resource-intensive cyber operations that reach the threshold of armed conflict with physical, destructive effects and that are quickly attributable.38 Fail-safe defensive measures also face several political and technical challenges, all of which point to a role for cyber resilience. Three main complications limit the applicability of the fail-deadly logics underpinning collective defense efforts in cyberspace. The first is deciding which actors are to be deterred. Compared to traditional warfighting domains, there are relatively low entry costs for conducting operations in the cyber domain.39 As such, both state and non-state actors can target the Alliance. There are also asymmetric operational costs—actors are faced with multiple avenues for potential gains and few risks. This means that it will be near-impossible to change the decision calculus of a malicious actor deploying low-cost, low-risk techniques such as distributed denials of service. Conversely, sophisticated cyber operations that can produce strategic effects equivalent to those of conventional military attacks will have both significant and costly intelligence requirements that can only be borne by state actors. These higher ‘start-up’ costs mean it may be possible to change the decision calculus of actors seeking to conduct highly sophisticated cyber operations. Due to this asymmetry, only state actors undertaking costly cyber operations are likely to be deterred. In all other circumstances, deterrence will be more prone to failure.40 Attribution difficulties present further challenges to the ‘who’ of deterrence. Adversaries with rapidly changing tactics, techniques, and procedures—along with the ability to easily conceal an operation’s origin and perpetrator—can pose hurdles to technical attribution.41 Technical difficulties can weaken deterrent postures by delaying the timeliness of retaliatory punishment. Moreover, the effects of an operation that a defender notices may actually be second- or third-order effects. This can add additional time between attribution and punishment.42 The larger attribution issues, however, are political. NATO lacks common standards or guidance for attributing cyber operations in either a technical or political sense. Indeed, attribution remains a member state prerogative. Not only are the targeted member states responsible for attribution, but those members looking to contribute to collective defense must perform independent attribution assessments, and the political decision for a collective defense response must come from the NAC.43 Reaching a consensus decision to trigger collective defense in response to cyberspace operations is likely to be politically contentious, and member states will have few incentives to risk revealing the intelligence sources and methods that underlie attribution decisions. These dynamics are likely to intensify when additional links in the attribution chain are required, such as when a perpetrator is encouraged or sponsored by an adversarial state but lacks direct ties. Attribution is less likely to be politically controversial across the Alliance once a conventional conflict is underway as contextual clues from kinetic attacks can reduce uncertainty. This discussion points to a greater role for deterrence-by-denial. Deterring an adversary by taking measures to deny potential gains does not hinge on attribution and thus possesses a potentially wider scope of application.44 A second and related hurdle for cyber deterrence is determining which actions the Alliance seeks to deter. Much of the activity in cyberspace falls below the physical effects thresholds associated with the disruption, degradation, or destruction of computers and networks. Such considerations complicate decisions to invoke Article 5—specifically, the types of cyberattacks to which Article 5 should apply. Indeed, cyber operations targeting military assets or critical civilian infrastructure can be incredibly costly but may not reach damage levels associated with conventional attacks.45 Moreover, espionage via network exploitation is widespread, varied, and falls well below the threshold of armed conflict.46 Problematically, such exploitation can be nearly indistinguishable from operations that eventually seek to attack computers or networks and produce effects. Network exploitation can even be precursor to conventional military operations.47 Determining how to deter presents a third obstacle to NATO’s cyber deterrence efforts. Threatening conventional military means in response to cyber operations poses dilemmas of proportionality and can risk unintended escalation.48 Retaliation with cyber tools carry their own problems. First, the Alliance faces issues of political reliability, particularly in the context of the SCEPVA framework. Legally, Allies retain different constitutional restraints on offensive cyber operations that can hamper the ability to volunteer sovereign effects. Strategically, states may be hesitant to volunteer their ‘best’ cyber effects for fear of burning an exploit that could have had a greater payoff when used in a national context. Volunteering sovereign effects can also inadvertently give unwanted insight to an adversary regarding an Ally’s techniques, tactics, and procedures. Second, the temporary and transient nature of cyber capabilities makes it incredibly difficult to establish repeatable and predictable effects required of deterrent threats.49 Finally, signaling in cyberspace is generally ambiguous and rarely straightforward.50 For instance, an adversary may not even recognize a signal, believing it instead to be a technical glitch. Even if a costly signal is received, there is no way to ensure that it has interpreted as intended. In addition to deterrence, NATO’s fail-safe cyber defense efforts face political and technical challenges. Because NATO will not undertake any active defense measures, actions to mitigate the effects of a cyberattack are limited to NATO networks or to individual member state networks when requested. This forecloses the possibility of developing an institutional strategy to mitigate the costs of a cyberattack upstream by disrupting the source of an attack, much like US Cyber Command does with its “defend forward” posture.51 More problematically, Allies have and will continue to have different legal, strategic, doctrinal, and threat frameworks for cyberspace that complicate defensive measures for the Alliance. Most immediately this means that Allies will locate resources to different aspects of cyber defense based on individual country circumstances. Different strategic focuses have the potential to intensify disparate threat perceptions, capabilities, and skillsets. This can also exacerbate interoperability problems; for example, during an operation or crisis, some systems will be controlled by NATO while others will be controlled by an ally or a group of allies with different skill and knowledge levels. In the longer term, disparate legal understandings, particularly regarding sovereignty in cyberspace, will become more impactful as a greater number of allied nations develop forward defense strategies and the requisite capabilities for out-of-network operations. An out-of-network operation can in and of itself cause operational friction. However, differing definitions of sovereignty in cyberspace—and what violates it—inevitably create political friction between Allies as some look to operate and produce effects on other Allies’ networks.52 This political friction will contribute to even greater hesitancy over cyber-intelligence sharing and complicate the coordination of defensive mitigation measures across the Alliance. Even if political barriers were removed, there are technical challenges to Allied implementation of fail-safe measures. Although there are conditions that can favor defense, such as the ability to manipulate the environment,53 offensive cyber operations can be both unpredictable and undetectable. Moreover, cyberspace presents a large and complex attack surface, where attacks can have unintended, cross-border effects. Given the sheer quantity of daily network probes experienced by NATO and individual member states, it is unlikely that every intrusion can be successfully countered or even identified. Highly sophisticated cyber operations are also likely to evade most defensive measures. Finally, fail-safe measures cannot effectively mitigate supply chain risks, as computers and systems increasingly rely on commercially available products and internationally based manufacturers. Defensive strategies will have limited utility if hardware or software components have been preloaded with malware.54 Each of these technical hurdles can contribute to slow-downs in decision-making, coordination, and response times for the Alliance while highlighting the need for greater resilience.

#### Cyber insecurity cause escalation of existing conflicts.

Erik Gartzke &Jon R. Lindsay 17. Gartzke is at the Department of Political Science, University of California, San Diego; Lindsay is at the Munk School of Global Affairs, University of Toronto. 03/01/2017. “Thermonuclear Cyberwar.” Journal of Cybersecurity, vol. 3, no. 1, pp. 37–48.

Cyber warfare is routinely overhyped as a new weapon of mass destruction, but when used in conjunction with actual weapons of mass destruction, severe, and underappreciated, dangers emerge. One side of a stylized debate about cybersecurity in international relations argues that offensive advantages in cyberspace empower weaker nations, terrorist cells, or even lone rogue operators to paralyze vital infrastructure [4–8]. The other side argues that operational difficulties and effective deterrence restrains the severity of cyber attack, while governments and cybersecurity firms have a pecuniary interest in exaggerating the threat [9–13]. Although we have contributed to the skeptical side of this debate [14–16], \*\*\*BEGIN FOOTNOTE\*\*\* 14. Gartzke E. The myth of cyberwar: bringing war in cyberspace back down to earth. Int Security 2013;38:41–73. Google ScholarCrossRef 15 Lindsay JR. Stuxnet and the limits of cyber warfare. Security Stud 2013;22:365–404. Google ScholarCrossRef 16 Lindsay JR. The impact of China on cybersecurity: fiction and friction. Int Security 2014;39:7–47. Google ScholarCrossRef \*\*\*END FOOTNOTE\*\*\* the same strategic logic that leads us to view cyberwar as a limited political instrument in most situations also leads us to view it as incredibly destabilizing in rare situations. In a recent Israeli wargame of a regional scenario involving the United States and Russia, one participant remarked on “how quickly localized cyber events can turn dangerously kinetic when leaders are ill-prepared to deal in the cyber domain” [17]. Importantly, this sort of catalytic instability arises not from the cyber domain itself but through its interaction with forces and characteristics in other domains (land, sea, air, etc.). Further, it arises only in situations where actors possess, and are willing to use, robust traditional military forces to defend their interests. Classical deterrence theory developed to explain nuclear deterrence with nuclear weapons, but different types of weapons or combinations of operations in different domains can have differential effects on deterrence and defense [18, 19]. Nuclear weapons and cyber operations are particularly complementary (i.e. nearly complete opposites) with respect to their strategic characteristics. Theorists and practitioners have stressed the unprecedented destructiveness of nuclear weapons in explaining how nuclear deterrence works, but it is equally, if not more, important for deterrence that capabilities and intentions are clearly communicated. As quickly became apparent, public displays of their nuclear arsenals improved deterrence.x At the same time, disclosing details of a nation’s nuclear capabilities did not much degrade the ability to strike or retaliate, given that defense against nuclear attack remains extremely difficult. Knowledge of nuclear capabilities is necessary to achieve a deterrent effect [20]. Cyber operations, in contrast, rely on undisclosed vulnerabilities, social engineering, and creative guile to generate indirect effects in the information systems that coordinate military, economic, and social behavior. Revelation enables crippling countermeasures, while the imperative to conceal capabilities constrains both the scope of cyber operations and their utility for coercive signaling [21, 22]. The diversity of cyber operations and confusion about their effects also contrast with the obvious destructiveness of nuclear weapons. The problem is that transparency and deception do not mix well. An attacker who hacks an adversary’s nuclear command and control apparatus, or the weapons themselves, will gain an advantage in warfighting that the attacker cannot reveal, while the adversary will continue to believe it wields a deterrent that may no longer exist. Most analyses of inadvertent escalation from cyber or conventional to nuclear war focus on “use it or lose it” pressures and fog of war created by attacks that become visible to the target [23, 24]. In a US–China conflict scenario, for example, conventional military strikes in conjunction with cyber attacks that blind sensors and confuse decision making could generate incentives for both sides to rush to preempt or escalate [25–27]. These are plausible concerns, but the revelation of information about a newly unfavorable balance of power might also cause hesitation and lead to compromise. Cyber blinding could potentially make traditional offensive operations more difficult, shifting the advantage to defenders and making conflict less likely. Clandestine attacks that remain invisible to the target potentially present a more insidious threat to crisis stability. There are empirical and theoretical reasons for taking seriously the effects of offensive cyber operations on nuclear deterrence, and we should expect the dangers to vary with the relative cyber capabilities of the actors in a crisis interaction. Nuclear command and control vulnerability General Robert Kehler, commander of US Strategic Command (STRATCOM) in 2013, stated in testimony before the Senate Armed Services Committee, “we are very concerned with the potential of a cyber-related attack on our nuclear command and control and on the weapons systems themselves” [28]. Nuclear command, control, and communications (NC3) form the nervous system of the nuclear enterprise spanning intelligence and early warning sensors located in orbit and on Earth, fixed and mobile command and control centers through which national leadership can order a launch, operational nuclear forces including strategic bombers, land-based intercontinental missiles (ICBMs), submarine-launched ballistic missiles (SLBMs), and the communication and transportation networks that tie the whole apparatus together [29, 30]. NC3 should ideally ensure that nuclear forces will always be available if authorized by the National Command Authority (to enhance deterrence) and never used without authorization (to enhance safety and reassurance). Friendly errors or enemy interference in NC3 can undermine the “always-never” criterion**,** weakening deterrence [31, 32]. NC3 has long been recognized as the weakest link in the US nuclear enterprise. According to a declassified official history, a Strategic Air Command (SAC) task group in 1979 “reported that tactical warning and communications systems … were ‘fragile’ and susceptible to electronic countermeasures, electromagnetic pulse, and sabotage, which could deny necessary warning and assessment to the National Command Authorities” [33]. Two years later, the Principal Deputy Under Secretary of Defense for Research and Engineering released a broad-based, multiservice report that doubled down on SAC’s findings: “the United States could not assure survivability, endurability, or connectivity of the national command authority function” due to: major command, control, and communications deficiencies: in tactical warning and attack assessment where existing systems were vulnerable to disruption and destruction from electromagnetic pulse, other high altitude nuclear effects, electronic warfare, sabotage, or physical attack; in decision making where there was inability to assure national command authority survival and connection with the nuclear forces, especially under surprise conditions; and in communications systems, which were susceptible to the same threats above and which could not guarantee availability of even minimum-essential capability during a protracted war. [33] The nuclear weapons safety literature likewise provides a number of troubling examples of NC3 glitches that illustrate some of the vulnerabilities attackers could, in principle, exploit [34–36]. The SAC history noted that NORAD has received numerous false launch indications from faulty computer components, loose circuits, and even a nuclear war training tape loaded by mistake into a live system that produced erroneous Soviet launch indications [33]. In a 1991 briefing to the STRATCOM commander, a Defense Intelligence Agency targeteer confessed, “Sir, I apologize, but we have found a problem with this target. There is a mistake in the computer code … . Sir, the error has been there for at least the life of this eighteen-month planning cycle. The nature of the error is such that the target would not have been struck” [37]. It would be a difficult operation to intentionally plant undetected errors like this, but the presence of bugs does reveal that such a hack is possible. Following many near-misses and self-audits during and after the Cold War, American NC3 improved with the addition of new safeguards and redundancies. As General Kehler pointed out in 2013, “the nuclear deterrent force was designed to operate through the most extreme circumstances we could possibly imagine” [28]. Yet vulnerabilities remain. In 2010, the US Air Force lost contact with 50 Minuteman III ICBMs for an hour because of a faulty hardware circuit at a launch control center [38]. If the accident had occurred during a crisis, or the component had been sabotaged, the USAF would have been unable to launch and unable to detect and cancel unauthorized launch attempts. As Bruce Blair, a former Minuteman missileer, points out, during a control center blackout the antennas at unmanned silos and the cables between them provide potential surreptitious access vectors [39]. The unclassified summary of a 2015 audit of US NC3 stated that “known capability gaps or deficiencies remain” [40]. Perhaps more worrisome are the unknown deficiencies. A 2013 Defense Science Board report on military cyber vulnerabilities found that while the: nuclear deterrent is regularly evaluated for reliability and readiness … , most of the systems have not been assessed (end-to-end) against a [sophisticated state] cyber attack to understand possible weak spots. A 2007 Air Force study addressed portions of this issue for the ICBM leg of the U.S. triad but was still not a complete assessment against a high-tier threat. [41] If NC3 vulnerabilities are unknown, it is also unknown whether an advanced cyber actor would be able to exploit them. As Kehler notes, “We don’t know what we don’t know” [28]. Even if NC3 of nuclear forces narrowly conceived is a hard target, cyber attacks on other critical infrastructure in preparation to or during a nuclear crisis could complicate or confuse government decision making. General Keith Alexander, Director of the NSA in the same Senate hearing with General Kehler, testified that: our infrastructure that we ride on, the power and the communications grid, are one of the things that is a source of concern … we can go to backup generators and we can have independent routes, but … our ability to communicate would be significantly reduced and it would complicate our governance … . I think what General Kehler has would be intact … [but] the cascading effect … in that kind of environment … concerns us. [28] Kehler further emphasized that “there’s a continuing need to make sure that we are protected against electromagnetic pulse and any kind of electromagnetic interference” [28]. Many NC3 components are antiquated and hard to upgrade, which is a mixed blessing. Kehler points out, “Much of the nuclear command and control system today is the legacy system that we’ve had. In some ways that helps us in terms of the cyber threat. In some cases it’s point to point, hard-wired, which makes it very difficult for an external cyber threat to emerge” [28]. The Government Accountability Office notes that the “Department of Defense uses 8-inch floppy disks in a legacy system that coordinates the operational functions of the nation’s nuclear forces” [42]. While this may limit some forms of remote access, it is also indicative of reliance on an earlier generation of software when security engineering standards were less mature. Upgrades to the digital Strategic Automated Command and Control System planned for 2017 have the potential to correct some problems, but these changes may also introduce new access vectors and vulnerabilities [43]. Admiral Cecil Haney, Kehler’s successor at STRATCOM, highlighted the challenges of NC3 modernization in 2015: Assured and reliable NC3 is fundamental to the credibility of our nuclear deterrent. The aging NC3 systems continue to meet their intended purpose, but risk to mission success is increasing as key elements of the system age. The unpredictable challenges posed by today’s complex security environment make it increasingly important to optimize our NC3 architecture while leveraging new technologies so that NC3 systems operate together as a core set of survivable and endurable capabilities that underpin a broader, national command and control system. [44] In no small irony, the internet itself owes its intellectual origin, in part, to the threat to NC3 from large-scale physical attack. A 1962 RAND report by Paul Baran considered “the problem of building digital communication networks using links with less than perfect reliability” to enable “stations surviving a physical attack and remaining in electrical connection … to operate together as a coherent entity after attack” [45]. Baran advocated as a solution decentralized packet switching protocols, not unlike those realized in the ARPANET program. The emergence of the internet was the result of many other factors that had nothing to do with managing nuclear operations, notably the meritocratic ideals of 1960s counterculture that contributed to the neglect of security in the internet’s founding architecture [46, 47]. Fears of NC3 vulnerability helped to create the internet, which then helped to create the present-day cybersecurity epidemic, which has come full circle to create new fears about NC3 vulnerability. NC3 vulnerability is not unique to the United States. The NC3 of other nuclear powers may even be easier to compromise, especially in the case of new entrants to the nuclear club like North Korea. Moreover, the United States has already demonstrated both the ability and willingness to infiltrate sensitive foreign nuclear infrastructure through operations such as Olympic Games (Stuxnet), albeit targeting Iran’s nuclear fuel cycle rather than NC3. It would be surprising to learn that the United States has failed to upgrade its Cold War NC3 attack plans to include offensive cyber operations against a wide variety of national targets. Hacking the deterrent The United States included NC3 attacks in its Cold War counterforce and damage limitation war plans, even as contemporary critics perceived these options to be destabilizing for deterrence [48]. The best known example of these activities and capabilities is a Special Access Program named Canopy Wing. East German intelligence obtained the highly classified plans from a US Army spy in Berlin, and the details began to emerge publicly after the Cold War. An East German intelligence officer, Markus Wolf, writes in his memoir that Canopy Wing “listed the types of electronic warfare that would be used to neutralize the Soviet Union and Warsaw Pact’s command centers in case of all-out war. It detailed the precise method of depriving the Soviet High Command of its high-frequency communications used to give orders to its armed forces” [49]. It is easy to see why NC3 is such an attractive target in the unlikely event of a nuclear war. If for whatever reason deterrence fails and the enemy decides to push the nuclear button, it would obviously be better to disable or destroy missiles before they launch than to rely on possibly futile efforts to shoot them down, or to accept the loss of millions of lives. American plans to disable Soviet NC3 with electronic warfare, furthermore, would have been intended to complement plans for decapitating strikes against Soviet nuclear forces. Temporary disabling of information networks in isolation would have failed to achieve any important strategic objective. A blinded adversary would eventually see again and would scramble to reconstitute its ability to launch its weapons, expecting that preemption was inevitable in any case. Reconstitution, moreover, would invalidate much of the intelligence and some of the tradecraft on which the blinding attack relied. Capabilities fielded through Canopy Wing were presumably intended to facilitate a preemptive military strike on Soviet NC3 to disable the ability to retaliate and limit the damage of any retaliatory force that survived, given credible indications that war was imminent. Canopy Wing included [50]: “Measures for short-circuiting … communications and weapons systems using, among other things, microscopic carbon-fiber particles and chemical weapons.” “Electronic blocking of communications immediately prior to an attack, thereby rendering a counterattack impossible.” “Deployment of various weapons systems for instantaneous destruction of command centers, including pin-point targeting with precision-guided weapons to destroy ‘hardened bunkers’.” “Use of deception measures, including the use of computer-simulated voices to override and substitute false commands from ground-control stations to aircraft and from regional command centers to the Soviet submarine fleet.” “Us[e of] the technical installations of ‘Radio Free Europe/Radio Liberty’ and ‘Voice of America,’ as well as the radio communications installations of the U.S. Armed Forces for creating interference and other electronic effects.” Wolf also ran a spy in the US Air Force who disclosed that the Americans had managed to penetrate the [Soviet air base at Eberswalde]’s ground-air communications and were working on a method of blocking orders before they reached the Russian pilots and substituting their own from West Berlin. Had this succeeded, the MiG pilots would have received commands from their American enemy. It sounded like science fiction, but, our experts concluded, it was in no way impossible that they could have pulled off such a trick, given the enormous spending and technical power of U.S. military air research. [49] One East German source claimed that Canopy Wing had a $14.5 billion budget for research and operational costs and a staff of 1570 people, while another claimed that it would take over 4 years and $65 million to develop “a prototype of a sophisticated electronic system for paralyzing Soviet radio traffic in the high-frequency range” [50]. Canopy Wing was not cheap, and even so, it was only a research and prototyping program. Operationalization of its capabilities and integration into NATO war plans would have been even more expensive. This is suggestive of the level of effort required to craft effective offensive cyber operations against NC3. Preparation comes to naught when a sensitive program is compromised. Canopy Wing was caught in what we describe below as the cyber commitment problem, the inability to disclose a warfighting capability for the sake of deterrence without losing it in the process. According to New York Times reporting on the counterintelligence investigation of the East German spy in the Army, Warrant Officer James Hall, “officials said that one program rendered useless cost hundreds of millions of dollars and was designed to exploit a Soviet communications vulnerability uncovered in the late 1970's” [51]. This program was probably Canopy Wing. Wolf writes, “Once we passed [Hall’s documents about Canopy Wing] on to the Soviets, they were able to install scrambling devices and other countermeasures” [49]. It is tempting to speculate that the Soviet deployment of a new NC3 system known as Signal-A to replace Signal-M (which was most likely the one targeted by Canopy Wing) was motivated in part by Hall’s betrayal [50]. Canopy Wing underscores the potential and limitations of NC3 subversion. Modern cyber methods can potentially perform many of the missions Canopy Wing addressed with electronic warfare and other means, but with even greater stealth and precision. Cyber operations might, in principle, compromise any part of the NC3 system (early warning, command centers, data transport, operational forces, etc.) by blinding sensors, injecting bogus commands or suppressing legitimate ones, monitoring or corrupting data transmissions, or interfering with the reliable launch and guidance of missiles. In practice, the operational feasibility of cyber attack against NC3 or any other target depends on the software and hardware configuration and organizational processes of the target, the intelligence and planning capacity of the attacker, and the ability and willingness to take advantage of the effects created by cyber attack [52, 53]. Cyber compromise of NC3 is technically plausible though operationally difficult, a point to which we return in a later section. To understand which threats are not only technically possible but also probable under some circumstance, we further need a political logic of cost and benefit [14]. In particular, how is it possible for a crisis to escalate to levels of destruction more costly than any conceivable political reward? Canopy Wing highlights some of the strategic dangers of NC3 exploitation. Warsaw Pact observers appear to have been deeply concerned that the program reflected an American willingness to undertake a surprise decapitation attack: they said that it “sent ice-cold shivers down our spines” [50]. The Soviets designed a system called Perimeter that, not unlike the Doomsday Device in Dr. Strangelove, was designed to detect a nuclear attack and retaliate automatically, even if cut off from Soviet high command, through an elaborate system of sensors, underground computers, and command missiles to transmit launch codes [54]. Both Canopy Wing and Perimeter show that the United States and the Soviet Union took nuclear warfighting seriously and were willing to develop secret advantages for such an event. By the same token, they were not able to reveal such capabilities to improve deterrence to avoid having to fight a nuclear war in the first place. Nuclear deterrence and credible communication Nuclear weapons have some salient political properties. They are singularly and obviously destructive. They kill in more, and more ghastly, ways than conventional munitions through electromagnetic radiation, blast, firestorms, radioactive fallout, and health effects that linger for years. Bombers, ICBMs, and SLBMs can project warheads globally without significantly mitigating their lethality, steeply attenuating the conventional loss-of-strength gradient [55]. Defense against nuclear attack is very difficult, even with modern ballistic missile defenses, given the speed of incoming warheads and use of decoys; multiple warheads and missile volleys further reduce the probability of perfect interception. If one cannot preemptively destroy all of an enemy’s missiles, then there is a nontrivial chance of getting hit by some of them. When one missed missile can incinerate millions of people, the notion of winning a nuclear war starts to seem meaningless for many politicians. As defense seemed increasingly impractical, early Cold War strategists championed the threat of assured retaliation as the chief mechanism for avoiding war [56–59]. Political actors have issued threats for millennia, but the advent of nuclear weapons brought deterrence as a strategy to center stage. The Cold War was an intense learning experience for both practitioners and students of international security, rewriting well-worn realities more than once [60–62]. A key conundrum was the practice of brinkmanship. Adversaries who could not compete by “winning” a nuclear war could still compete by manipulating the “risk” of nuclear annihilation, gambling that an opponent would have the good judgment to back down at some point short of the nuclear brink. Brinkmanship crises—conceptualized as games of Chicken where one cannot heighten tensions without increasing the hazard of the mutually undesired outcome—require that decision makers behave irrationally, or possibly that they act randomly, which is difficult to conceptualize in practical terms [63]. The chief concern in historical episodes of chicken, such as the Berlin Crisis and Cuban Missile Crisis, was not whether a certain level of harm was possible, but whether an adversary was resolved enough, possibly, to risk nuclear suicide. The logical inconsistency of the need for illogic to win led almost from the beginning of the nuclear era to elaborate deductive contortions [64–66]. Both mutually assured destruction (MAD) and successful brinksmanship depend on a less appreciated, but no less fundamental, feature of nuclear weapons: political transparency. Most elements of military power are weakened by disclosure [67]. Military plans are considerably less effective if shared with an enemy. Conventional weapons become less lethal as adversaries learn what different systems can and cannot do, where they are located, how they are operated, and how to devise countermeasures and array defenses to blunt or disarm an attack. In contrast, relatively little reduction in destruction follows from enemy knowledge of nuclear capabilities. For most of the nuclear era, no effective defense existed against a nuclear attack. Even today, with evolving ABM systems, one ICBM still might get through and annihilate the capital city. Nuclear forces are more robust to revelation than other weapons, enabling nuclear nations better to advertise the harm they can inflict. The need for transparency to achieve an effective deterrent is driven home by the satirical Cold War film, Dr. Strangelove: “the whole point of a Doomsday Machine is lost, if you keep it a secret! Why didn’t you tell the world, eh?” During the real Cold War, fortunately, Soviet leaders paraded their nuclear weapons through Red Square for the benefit of foreign military attaches and the international press corps. Satellites photographed missile, bomber, and submarine bases. While other aspects of military affairs on both sides of the Iron Curtain remained closely guarded secrets, the United States and the Soviet Union permitted observers to evaluate their nuclear capabilities. This is especially remarkable given the secrecy that pervaded Soviet society. The relative transparency of nuclear arsenals ensured that the superpowers could calculate risks and consequences within a first-order approximation, which led to a reduction in severe conflict and instability even as political competition in other arenas was fierce [61, 68]. Recent insights about the causes of war suggest that divergent expectations about the costs and consequences of war are necessary for contests to occur [69–73]. These insights are associated with rationalist theories, such as deterrence theory itself. Empirical studies and psychological critiques of the rationality assumption have helped to refine models and bring some circumspection into their application, but the formulation of sound strategy (if not the execution) still requires the articulation of some rational linkage between cause and effect [19, 62, 74]. Many supposedly nonrational factors, moreover, simply manifest as uncertainty in strategic interaction. Our focus here is on the effect of uncertainty and ignorance on the ability of states and other actors to bargain in lieu of fighting. Many wars are a product of what adversaries do not know or what they misperceive, whether as a result of bluffing, secrecy, or intrinsic uncertainty [75, 76]. If knowledge of capabilities or resolve is a prerequisite for deterrence, then one reason for deterrence failure is the inability or unwillingness to credibly communicate details of the genuine balance of power, threat, or interests. Fighting, conversely, can be understood as a costly process of discovery that informs adversaries of their actual relative strength and resolve. From this perspective, successful deterrence involves instilling in an adversary perceptions like those that result from fighting, but before fighting actually begins. Agreement about the balance of power can enable states to bargain (tacit or overt) effectively without needing to fight, forging compromises that each prefers to military confrontation or even to the bulk of possible risky brinkmanship crises. Despite other deficits, nuclear weapons have long been considered to be stabilizing with respect to rational incentives for war(the risk of nuclear accidents is another matter) [77]. If each side has a secure second strike—or even a minimal deterrent with some nonzero chance of launching a few missiles—then each side can expect to gain little and lose much by fighting a nuclear war. Whereas the costs of conventional war can be more mysterious because each side might decide to hold something back and meter out its punishment due to some internal constraint or a theory of graduated escalation, even a modest initial nuclear exchange is recognized to be extremely costly. As long as both sides understand this and understand (or believe) that the adversary understands this as well, then the relationship is stable. Countries engage nuclear powers with considerable deference, especially over issues of fundamental national or international importance. At the same time, nuclear weapons appear to be of limited value in prosecuting aggressive action, especially over issues of secondary or tertiary importance, or in response to aggression from others at lower levels of dispute intensity. Nuclear weapons are best used for signaling a willingness to run serious risks to protect or extort some issue that is considered of vital national interest. As mentioned previously, both superpowers in the Cold War considered the warfighting advantages of nuclear weapons quite apart from any deterrent effect, and the United States and Russia still do. High-altitude bursts for air defense, electromagnetic pulse for frying electronics, underwater detonations for anti-submarine warfare, hardened target penetration, area denial, and so on, have some battlefield utility. Transparency per se is less important than weapon effects for warfighting uses, and can even be deleterious for tactics that depend on stealth and mobility. Even a single tactical nuke, however, would inevitably be a political event. Survivability of the second strike deterrent can also militate against transparency, as in the case of the Soviet Perimeter system, as mobility, concealment, and deception can make it harder for an observer to track and count respective forces from space. Counterforce strategies, platform diversity and mobility, ballistic missile defense systems, and force employment doctrine can all make it more difficult for one or both sides in a crisis to know whether an attack is likely to succeed or fail. The resulting uncertainty affects not only estimates of relative capabilities but also the degree of confidence in retaliation. At the same time, there is reason to believe that platform diversity lowers the risk of nuclear or conventional contests, because increasing the number of types of delivery platforms heightens second strike survivability without increasing the lethality of an initial strike [78]. While transparency is not itself a requirement for nuclear use, stable deterrence benefits to the degree to which retaliation can be anticipated, as well as the likelihood that the consequences of a first strike are more costly than any benefit. Cyber operations, in contrast, are neither robust to revelation nor as obviously destructive. The cyber commitment problem Deterrence (and compellence) uses force or threats of force to “warn” an adversary about consequences if it takes or fails to take an action. In contrast, defense (and conquest) uses force to “win” a contest of strength and change the material distribution of power. Sometimes militaries can change the distribution of information and power at the same time. Military mobilization in a crisis signifies resolve and displays a credible warning, but it also makes it easier to attack or defend if the warning fails. Persistence in a battle of attrition not only bleeds an adversary but also reveals a willingness to pay a higher price for victory. More often, however, the informational requirements of winning and warning are in tension. Combat performance often hinges on well-kept secrets, feints, and diversions. Many military plans and capabilities degrade when revealed. National security involves trade-offs between the goals of preventing war, by advertising capabilities or interests, and improving fighting power should war break out, by concealing capabilities and surprising the enemy. The need to conceal details of the true balance of power to preserve battlefield effectiveness gives rise to the military commitment problem [79, 80]. Japan could not coerce the United States by revealing its plan to attack Pearl Harbor because the United States could not credibly promise to refrain from reorienting defenses and dispersing the Pacific Fleet. War resulted not just because of what opponents did not know but because of what they could not tell each other without paying a severe price in military advantage. The military benefits of surprise (winning) trumped the diplomatic benefits of coercion (warning). Cyber operations, whether for disruption and intelligence, are extremely constrained by the military commitment problem. Revelation of a cyber threat in advance that is specific enough to convince a target of the validity of the threat also provides enough information potentially to neutralize it. Stuxnet took years and hundreds of millions of dollars to develop but was patched within weeks of its discovery. The Snowden leaks negated a whole swath of tradecraft that the NSA took years to develop. States may use other forms of covert action, such as publicly disavowed lethal aid or aerial bombing (e.g. Nixon’s Cambodia campaign), to discretely signal their interests, but such cases can only work to the extent that revelation of operational details fails to disarm rebels or prevent airstrikes [81]. Cyber operations, especially against NC3, must be conducted in extreme secrecy as a condition of the efficacy of the attack. Cyber tradecraft relies on stealth, stratagem, and deception [21]. Operations tailored to compromise complex remote targets require extensive intelligence, planning and preparation, and testing to be effective. Actions that alert a target of an exploit allow the target to patch, reconfigure, or adopt countermeasures that invalidate the plan. As the Defense Science Board points out, competent network defenders: can also be expected to employ highly-trained system and network administrators, and this operational staff will be equipped with continuously improving network defensive tools and techniques (the same tools we advocate to improve our defenses). Should an adversary discover an implant, it is usually relatively simple to remove or disable. For this reason, offensive cyber will always be a fragile capability. [41] The world’s most advanced cyber powers, the United States, Russia, Israel, China, France, and the United Kingdom, are also nuclear states, while India, Pakistan, and North Korea also have cyber warfare programs. NC3 is likely to be an especially well defended part of their cyber infrastructures. NC3 is a hard target for offensive operations, which thus requires careful planning, detailed intelligence, and long lead-times to avoid compromise. Cyberspace is further ill-suited for signaling because cyber operations are complex, esoteric, and hard for commanders and policymakers to understand. Most targeted cyber operations have to be tailored for each unique target (a complex organization not simply a machine), quite unlike a general purpose munition tested on a range. Malware can fail in many ways and produce unintended side effects, as when the Stuxnet code was accidentally released to the public. The category of “cyber” includes tremendous diversity: irritant scams, hacktivist and propaganda operations, intelligence collection, critical infrastructure disruption, etc. Few intrusions create consequences that rise to the level of attacks such as Stuxnet or BlackEnergy, and even they pale beside the harm imposed by a small war. Vague threats are less credible because they are indistinguishable from casual bluffing. Ambiguity can be useful for concealing a lack of capability or resolve, allowing an actor to pool with more capable or resolved states and acquiring some deterrence success by association. But this works by discounting the costliness of the threat. Nuclear threats, for example, are usually somewhat veiled because one cannot credibly threaten nuclear suicide. The consistently ambiguous phrasing of US cyber declaratory policy (e.g. “we will respond to cyber-attacks in a manner and at a time and place of our choosing using appropriate instruments of U.S. power” [82]) seeks to operate across domains to mobilize credibility in one area to compensate for a lack of credibility elsewhere, specifically by leveraging the greater robustness to revelation of military capabilities other than cyber. This does not mean that cyberspace is categorically useless for signaling, just as nuclear weapons are not categorically useless for warfighting. Ransomware attacks work when the money extorted to unlock the compromised host is priced below the cost of an investigation or replacing the system. The United States probably gained some benefits in general deterrence (i.e. discouraging the emergence of challenges as opposed to immediate deterrence in response to a challenge) through the disclosure of Stuxnet and the Snowden leaks. Both revelations compromised tradecraft, but they also advertised that the NSA probably had more exploits and tradecraft where they came from. Some cyber operations may actually be hard to mitigate within tactically meaningful timelines (e.g. hardware implants installed in hard-to-reach locations). Such operations might be revealed to coerce concessions within the tactical window created by a given operation, if the attacker can coordinate the window with the application of coercion in other domains. As a general rule, however, the cyber domain on its own is better suited for winning than warning [83]. Cyber and nuclear weapons fall on extreme opposite sides of this spectrum. Dangerous complements Nuclear weapons have been used in anger twice—against the Japanese cities Hiroshima and Nagasaki—but cyberspace is abused daily. Considered separately, the nuclear domain is stable and the cyber domain is unstable. In combination, the results are ambiguous. The nuclear domain can bound the intensity of destruction that a cyber attacker is willing to inflict on an adversary. US declaratory policy states that unacceptable cyber attacks may prompt a military response; while nuclear weapons are not explicitly threatened, neither are they withheld. Nuclear threats have no credibility at the low end, where the bulk of cyber attacks occur. This produces a cross-domain version of the stability–instability paradox, where deterrence works at the high end but is not credible, and thus encourages provocation, at low intensities. Nuclear weapons, and military power generally, create an upper bound on cyber aggression to the degree that retaliation is anticipated and feared [22, 83, 84]. In the other direction, the unstable cyber domain can undermine the stability of nuclear deterrence. Most analysts who argue that the cyber–nuclear combination is a recipe for danger focus on the fog of crisis decision making [85–87]. Stephen Cimbala points out that today’s relatively smaller nuclear arsenals may perversely magnify the attractiveness of NC3 exploitation in a crisis: “Ironically, the downsizing of U.S. and post-Soviet Russian strategic nuclear arsenals since the end of the Cold War, while a positive development from the perspectives of nuclear arms control and nonproliferation, makes the concurrence of cyber and nuclear attack capabilities more alarming” [88]. Cimbala focuses mainly on the risks of misperception and miscalculation that emerge when a cyber attack muddies the transparent communication required for opponents to understand one another’s interests, redlines, and willingness to use force, and to ensure reliable control over subordinate commanders. Thus a nuclear actor “faced with a sudden burst of holes in its vital warning and response systems might, for example, press the preemption button instead of waiting to ride out the attack and then retaliate” [85]. The outcome of fog of decision scenarios such as these depend on how humans react to risk and uncertainty, which in turn depends on bounded rationality and organizational frameworks that might confuse rational decision making [89, 90]. These factors exacerbate a hard problem. Yet within a rationalist framework, cyber attacks that have already created their effects need not trigger an escalatory spiral. While being handed a fait accompli may trigger an aggressive reaction, it is also plausible that the target’s awareness that its NC3 has been compromised in some way would help to convey new information that the balance of power is not as favorable as previously thought. This in turn could encourage the target to accommodate, rather than escalate. While defects in rational decision making are a serious concern in any cyber–nuclear scenario, the situation becomes even more hazardous when there are rational incentives to escalate. Although “known unknowns” can create confusion, to paraphrase Donald Rumsfeld, the “unknown unknowns” are perhaps more dangerous. A successful clandestine penetration of NC3 can defeat the informational symmetry that stabilizes nuclear relationships. Nuclear weapons are useful for deterrence because they impose a degree of consensus about the distribution of power; each side knows the other can inflict prohibitive levels of damage, even if they may disagree about the precise extent of this damage. Cyber operations are attractive precisely because they can secretly revise the distribution of power. NC3 neutralization may be an expensive and rarified capability in the reach of only a few states with mature signals intelligence agencies, but it is much cheaper than nuclear attack. Yet the very usefulness of cyber operations for nuclear warfighting ensure that deterrence failure during brinksmanship crises is more likely. Nuclear states may initiate crises of risk and resolve to see who will back down first, which is not always clear in advance. Chicken appears viable, ironically, because each player understands that a nuclear war would be a disaster for all, and thus all can agree that someone can be expected swerve. Nuclear deterrence should ultimately make dealing with an adversary diplomatically more attractive than fighting, provided that fighting is costly—as would seem evident for the prospect of nuclear war—and assuming that bargains are available to states willing to accept compromise rather than annihilation. If, however, one side knows, but the other does not, that the attacker has disabled the target’s ability to perceive an impending military attack, or to react to one when it is underway, then they will not have a shared understanding of the probable outcome of war, even in broad terms. Consider a brinksmanship crisis between two nuclear states where only one has realized a successful penetration of the rival’s NC3. The cyber attacker knows that it has a military advantage, but it cannot reveal the advantage to the target, lest the advantage be lost. The target does not know that it is at a disadvantage, and it cannot be told by the attacker for the same reason. The attacker perceives an imbalance of power while the target perceives a balance. A dangerous competition in risk taking ensues. The first side knows that it does not need to back down. The second side feels confident that it can stand fast and raise the stakes far beyond what it would be willing to if it understood the true balance of power. Each side is willing to escalate to create more risk for the other side, making it more likely that one or the other will conclude that deterrence has failed and move into warfighting mode to attempt to limit the damage the other can inflict. The targeted nature and uncertain effects of offensive cyber operations put additional pressure on decision makers. An intrusion will probably disable only part of the enemy’s NC3 architecture, not all of it (which is not only operationally formidable to achieve but also more likely to be noticed by the target). Thus the target may retain control over some nuclear forces, or conventional forces. The target may be tempted to use some of them piecemeal to signal a willingness to escalate further, even though it cannot actually escalate because of the cyber operation. The cyber attacker knows that it has escalation dominance, but when even a minor demonstration by the target can cause great damage, it is tempting to preempt this move or others like it. This situation would be especially unstable if only second strike but not primary strike NC3 was incapacitated. Uncertainty in the efficacy of the clandestine penetration would discount the attacker’s confidence in its escalation dominance, with a range of possible outcomes. Enough uncertainty would discount the cyber attack to nothing, which would have a stabilizing effect by returning the crisis to the pure nuclear domain. A little bit of uncertainty about cyber effectiveness would heighten risk acceptance while also raising the incentives to preempt as an insurance measure. Adding allies into the mix introduces additional instability. An ally emboldened by its nuclear umbrella might run provocative risks that it would be much more reluctant to embrace if it was aware that the umbrella was actually full of holes. Conversely, if the clandestine advantage is held by the state extending the umbrella, allies could become unnerved by the willingness of their defender to run what appear to be outsize risks, oblivious of the reasons for the defender’s confidence, creating discord in the alliance and incentives for self-protective action, leading to greater uncertainty about alliance solidarity. The direction of influence between the cyber and nuclear realms depends to large degree on which domain is the main arena of action. Planning and conducting cyber operations will be bounded by the ability of aggressors to convince themselves that attacks will remain secret, and by the confidence of nuclear nations in their invulnerability. Fears of cross-domain escalation will tend to keep instability in cyberspace bounded. However, if a crisis has risen to the point where nuclear threats are being seriously considered or made, then NC3 exploitation will be destabilizing. Brinksmanship crises seem to have receded in frequency since the Cuban Missile Crisis but may be more likely than is generally believed. President Vladimir Putin of Russia has insinuated more than once in recent years that his government is willing to use tactical nuclear weapons if necessary to support his policies. Cyber power and nuclear stability Not all crises are the same. Indeed, their very idiosyncrasies create the uncertainties that make bargaining failure more likely [75]. So far our analysis would be at home in the Cold War, with the technological novelty of cyber operations. Yet not every state has the same cyber capabilities or vulnerabilities. Variation in cyber power relations across dyads should be expected to affect the strategic stability of nuclear states. The so-called second nuclear age differs from superpower rivalry in important ways [91]. There are fewer absolute numbers of warheads in the world, down from a peak of over 70 000 in the 1980s to about 15 000 today (less than 5000 deployed), but they are distributed very unevenly [92]. The United States and Russia have comparably sized arsenals, each with a fully diversified triad of delivery platforms, while North Korea only has a dozen or so bombs and no meaningful delivery system (for now). China, India, Pakistan, Britain, France, and Israel have modest arsenals in the range of several dozen to a couple hundred weapons, but they have very different doctrines, conventional force complements, domestic political institutions, and alliance relationships. The recent nuclear powers lack the hard-won experience and shared norms of the Cold War to guide them through crises, and even the United States and Russia have much to relearn. Cyber warfare capacity also varies considerably across contemporary nuclear nations. The United States, Russia, Israel, and Britain are in the top tier, able to run sophisticated, persistent, clandestine penetrations. China is a uniquely active cyber power with ambitious cyber warfare doctrine, but its operational focus is on economic espionage and political censorship, resulting in less refined tradecraft and more porous defenses for military purposes [16]. France, India, and Pakistan also have active cyber warfare programs, while North Korea is the least developed cyber nation, depending on China for its expertise [93]. It is beyond the scope of this article to assess crisis dyads in detail, and data on nuclear and cyber power for these countries are shrouded in secrecy. Here, as a way of summing up the arguments above, we offer a few conjectures about how stylized aspects of cyber power affect crisis stability through incentives and key aspects of decision making. We do not stress relative nuclear weapon capabilities on the admittedly strong (and contestable) assumption that nuclear transparency in the absence of cyber operations would render nuclear asymmetry irrelevant for crisis bargaining because both sides would agree about the terrible consequences of conflict [94]. We also omit domestic or psychological variables that affect relative power assessments, although these are obviously important. Even if neither India nor Pakistan have viable cyber–nuclear capabilities, brinksmanship between them is dangerous for many other reasons, notably compressed decision timelines, Pakistan’s willingness to shoot first, and domestic regime instability. Our focus is on the impact of offensive and defensive cyber power on nuclear deterrence above and beyond the other factors that certainly play a role in real-world outcomes. First, does the cyber attacker have the organizational capacity, technical expertise, and intelligence support to “compromise” the target’s NC3? Can hackers access critical networks, exploit technical vulnerabilities, and confidently execute a payload to disrupt or exploit strategic sensing, command, forces, or transport capacity? The result would be some tangible advantage for warfighting, such as tactical warning or control paralysis, but one that cannot be exercised in bargaining. Second, is the target able to “detect” the compromise of its NC3? The more complicated and sensitive the target, the more likely cyber attackers are to make a mistake that undermines the intrusion. Attribution is not likely to be difficult given the constricted pool of potential attackers, but at the same time the consequences of misattributing “false flag” operations could be severe [95]. At a minimum, detection is assumed to provide information to the target that the balance of power is perhaps not as favorable as imagined previously. We assume that detection without an actual compromise is possible because of false positives or deceptive information operations designed to create pessimism or paranoia. Third, is the target able to “mitigate” the compromise it detects? Revelation can prompt patching or network reconfiguration to block an attack, but this assumption is not always realistic. The attacker may have multiple pathways open or may have implanted malware that is difficult to remove in tactically meaningful timelines. In such cases the cyber commitment problem is not absolute, since the discovery of the power to hurt does not automatically disarm it. Successful mitigation here is assumed to restore mutual assessments of the balance of power to what they would be absent the cyber attack. Table 1 shows how these factors combine to produce different deterrence outcomes in a brinksmanship (chicken) crisis. If there is no cyber compromise and the target detects nothing (no false positives) then we have the optimistic ideal case where nuclear transparency affords stable “deterrence.” Transparency about the nuclear balance, including the viability of secure second strike forces, provides strategic stability. We also expect this box to describe situations where the target has excellent network defense capabilities and thus the prospect of defense, denial or deception successfully deters any attempts to penetrate NC3. This may resemble the Cold War situation (with electronic warfare in lieu of cyber), or even the present day US–Russia dyad, where the odds of either side pulling off a successful compromise against a highly capable defender are not favorable. Alternately the attack may be deemed risky enough to encourage serious circumspection. However, the existence of Canopy Wing does not encourage optimism in this regard. [[TABLE 1 OMITTED]] Conversely, if there is a compromise that goes undetected, then there is a heightened risk of “war” because of the cyber commitment problem. This box may be particularly relevant for asymmetric dyads such as the United States and North Korea, where one side has real cyber power but the other side is willing to go to the brink where it believes, falsely, that it has the capability to compel its counterpart to back down. Cyber disruption of NC3 is attractive for damage limitation should deterrence fail, given that the weaker state’s diminutive arsenal makes damage limitation by the stronger state more likely to succeed. The dilemma for the stronger state is that the clandestine counterforce hedge, which makes warfighting success more likely, is precisely what makes deterrence more likely to fail. The United States would face similar counterforce dilemmas with other dyads like China or even Russia, although even a strong cyber power should be more circumspect when confronted with an adversary with a larger/more capable nuclear and conventional arsenal. More complex and cyber savvy targets, moreover, are more likely to detect a breach in NC3, leading to more ambiguous outcomes depending on how actors cope with risk and uncertainty. Paradoxically, confidence in cyber security may be a major contributor to failure; believing one is safe from attack increases the chance that an attack is successful. If the successful compromise is detected but not mitigated, then the target learns that the balance of power is not as favorable as thought. This possibility suggests fleeting opportunities for “coercion” by revealing the cyber coup to the target in the midst of a crisis while the cyber attacker maintains or develops a favorable military advantage before the target has the opportunity to reverse or compensate the NC3 disruption. Recognizing the newly transparent costs of war, a risk neutral or risk averse target should prefer compromise. The coercive advantages (deterrence or compellence) of a detected but unmitigated NC3 compromise will likely be fleeting. This suggests a logical possibility for creating a window of opportunity for using particular cyber operations that are more robust to revelation as a credible signal of superior capability in the midst of a crisis. It would be important to exploit this fleeting advantage via other credible military threats (e.g. forces mobilized on visible alert or deployed into the crisis area) before the window closes. One side may be able gain an unearned advantage, an opportunity for coercion via a “bluff,” by the same window-of-opportunity logic. A target concerned about NC3 compromise will probably have some network monitoring system and other protections in place. Defensive systems can produce false positives as a result of internal errors or a deception operation by the attacker to encourage paranoia. It is logically possible that some false positives would appear to the target to be difficult to mitigate. In this situation, the target could believe it is at a disadvantage, even though this is not in fact the case. This gambit would be operationally very difficult to pull off with any reliability in a real nuclear crisis. Cyber–nuclear coercion and bluffing strategies are fraught with danger. Detection without mitigation might put a risk-acceptant or loss-averse target into a “use-lose” situation, creating pressures to preempt or escalate. The muddling of decision-making heightens the risk of accidents or irrational choices in a crisis scenario. Worry about preemption or accident then heightens the likelihood that the initiator will exercise counterforce options while they remain available. These pressures can be expected to be particularly intense if the target’s detection is only partial or has not revealed the true extent of damage to its NC3 (i.e. the target does not realize it has already lost some or all of what it hopes to use). These types of scenarios are most usually invoked in analyses of inadvertent escalation [23–27]. The essential distinction between “use-lose” risks and “war” in this typology is the target’s knowledge of some degree of NC3 compromise. Use-lose and other cognitive pressures can certainly result in nuclear war, since the breakdown of deterrence leads to the release of nuclear weapons, but we distinguish these outcomes to highlight the different decision making processes or rational incentives at work. A “spiral” of mistrust may emerge if one side attempts a compromise but the defender detects and mitigates it. Both sides again have common mutual estimates of the relative balance of power, which superficially resembles the “deterrence” case because the NC3 compromise is negated. Unfortunately, the detection of the compromise will provide the target with information about the hostile intentions of the cyber attacker. This in turn is likely to exacerbate other political or psychological factors in the crisis itself or in the crisis-proneness of the broader relationship. The strange logical case where there is no compromise but one is detected and mitigated could result from a false positive misperception (including a third-party false flag operation) that could conflict spiraling [96, 97]. The bluff and coercion outcomes are also likely to encourage spiraling behavior once the fleeting bargaining advantage dissipates or is dispelled (provided anyone survives the interaction). The risk of crisis instability is not the same for all dyads. It is harder to compromise the NC3 of strong states because of the redundancy and active defenses in their arsenal. Likewise, strong states are better able to compromise the NC3 of any states but especially of weaker states, because of strong states’ greater organizational capacity and expertise in cyber operations. Stable deterrence or MAD is most likely to hold in mutually strong dyads (e.g. the United States and the Soviet Union in the Cold War or Russia today to a lesser extent). Deterrence is slightly less likely in other equally matched dyads (India–Pakistan) where defensive vulnerabilities create temptations but offensive capabilities may not be sufficient to exploit them. Most states can be expected to refrain from targeting American NC3 given a US reputation for cyber power (a general deterrence benefit enhanced by Stuxnet and Snowden). The situation is less stable if the United States is the attacker. The most dangerous dyad is a stronger and a weaker state (United States and North Korea or Israel and Iran). Dyads involving strong and middle powers are also dangerous (United States and China**).** The stronger side is tempted to disrupt NC3 as a warfighting hedge in case deterrence breaks down, while the weaker but still formidable side has a reasonable chance at detection. The marginally weaker may also be tempted to subvert NC3, particularly for reconnaissance; the stronger side is more likely to detect and correct the intrusion but will be alarmed by the ambiguity in distinguishing intelligence collection from attack planning [98]. In a brinksmanship crisis between them, windows for coercion may be available yet fleeting, with real risks of spiral and war**.**

#### An entangled NATO response to inevitable Russian cyber aggression triggers a nuclear escalation ladder

O’Hanlon 19—Senior fellow in Foreign Policy at the Brookings Institution, where he specializes in U.S. defense strategy, the use of military force, and American national security policy. He is also director of research for the Foreign Policy program at Brookings. He is an adjunct professor at Columbia, Princeton, and Syracuse universities and University of Denver [Michael E., April 2019, *The Senkaku Paradox: Risking Great Power War Over Small Stakes*, Chapter 2: Plausible Scenarios, pgs 36, Brookings Institution Press, ProQuest Ebook, Accessed through the Wake Forest Library] AMarb

A NATO military response to the postulated Russian aggression seems very likely. Perhaps evidence of its preparations to move forces into position to defend its ally and liberate its territory from Russian occupation would be enough to catalyze a diplomatic resolution of the crisis. If not, however, the stage would be set for the possible eruption of World War III. Russia might try to impede a deployment through cyber-, space, and other such attacks, which would likely only slow the deployment, not stop it. Thus escalation could easily result. 62 Once shots were fired, NATO would be unlikely to back down. Not every nation would necessarily send significant military forces, to be sure, but some key countries would probably remain resolute. Much more likely than acceptance of defeat would be a redoubled commitment to complete the mission—and, if Russian nuclear weapons had been used by that point, even in a limited attack, to respond in kind. Put differently, if Russia did choose to try to physically prevent the deployment of large forces into eastern NATO territory in likely preparation for a counterattack, there would be two possibilities. If that attempt failed, a showdown in the east on land would still loom. If it succeeded, NATO would then face a momentous decision: accept defeat, or reinforce dramatically with conventional forces (perhaps after a period of repairing damage and building more equipment and weaponry, depending on how many losses it had already suffered), or escalate to the nuclear level. In situations of this sort, the parties to the conflict might find themselves living scenarios like those that nuclear theorists pondered throughout the Cold War. They could be engaged in behavior that Thomas Schelling might have described as “the threat that leaves something to chance” or that Herman Kahn might have placed on the lower rungs of a nuclear escalation ladder that reached potentially to all-out war. 63 American planners saw these kinds of escalatory ladders and options as ideas that might serve U.S. interests; thus it would not be too surprising to see Russian planners invoke them now. 64 And whatever the dangers during the deployment phase, they would snowball during any actual maneuver warfare in eastern Europe. For example, it is entirely imaginable that an operation designed to liberate a Baltic state from a Russian occupation would trespass onto Russian territory to cut off supply lines and possible reinforcements. 65 Moscow may or may not simply take NATO’s word that it has no designs on the country’s government. In other words, it might even fear that NATO’s counteroffensive could aspire to regime change in Russia. It may or may not have a clear picture of the kind of attack it is experiencing, as command and control systems would be compromised in the course of conventional battle, quite possibly including those systems commonly used for nuclear weapons. 66

#### Russia war causes extinction

Dr. Owen Cotton-Barratt 17, PhD in Pure Mathematics, Oxford, Lecturer in Mathematics at Oxford and Research Associate at the Future of Humanity Institute, et al, “Existential Risk: Diplomacy and Governance”, 2/3/2017, https://www.fhi.ox.ac.uk/wp-content/uploads/Existential-Risks-2017-01-23.pdf

The bombings of Hiroshima and Nagasaki demonstrated the unprecedented destructive power of nuclear weapons. However, even in an all-out nuclear war between the United States and Russia, despite horrific casualties, neither country’s population is likely to be completely destroyed by the direct effects of the blast, fire, and radiation.8 The aftermath could be much worse: the burning of flammable materials could send massive amounts of smoke into the atmosphere, which would absorb sunlight and cause sustained global cooling, severe ozone loss, and agricultural disruption – a nuclear winter. According to one model 9 , an all-out exchange of 4,000 weapons10 could lead to a drop in global temperatures of around 8°C, making it impossible to grow food for 4 to 5 years. This could leave some survivors in parts of Australia and New Zealand, but they would be in a very precarious situation and the threat of extinction from other sources would be great. An exchange on this scale is only possible between the US and Russia who have more than 90% of the world’s nuclear weapons, with stockpiles of around 4,500 warheads each, although many are not operationally deployed.11 Some models suggest that even a small regional nuclear war involving 100 nuclear weapons would produce a nuclear winter serious enough to put two billion people at risk of starvation,12 though this estimate might be pessimistic.13 Wars on this scale are unlikely to lead to outright human extinction, but this does suggest that conflicts which are around an order of magnitude larger may be likely to threaten civilisation. It should be emphasised that there is very large uncertainty about the effects of a large nuclear war on global climate. This remains an area where increased academic research work, including more detailed climate modelling and a better understanding of how survivors might be able to cope and adapt, would have high returns. It is very difficult to precisely estimate the probability of existential risk from nuclear war over the next century, and existing attempts leave very large confidence intervals. According to many experts, the most likely nuclear war at present is between India and Pakistan.14 However, given the relatively modest size of their arsenals, the risk of human extinction is plausibly greater from a conflict between the United States and Russia. Tensions between these countries have increased in recent years and it seems unreasonable to rule out the possibility of them rising further in the future.

#### Cyber-attacks threaten critical infrastructure and grids.

O’Hanlon 19—Senior fellow in Foreign Policy at the Brookings Institution, where he specializes in U.S. defense strategy, the use of military force, and American national security policy. He is also director of research for the Foreign Policy program at Brookings. He is an adjunct professor at Columbia, Princeton, and Syracuse universities and University of Denver [Michael E., April 2019, *The Senkaku Paradox: Risking Great Power War Over Small Stakes*, Chapter 2: Plausible Scenarios, pgs 34-6, Brookings Institution Press, ProQuest Ebook, Accessed through the Wake Forest Library, language edited change denoted by brackets] AMarb

If any initial conventional engagements went against its interests, Russia might also consider limited nuclear employment options. Indeed, some of its strategists currently entertain an “escalate to de-escalate” concept that would attempt to intimidate NATO allies into reversing their plans. Russia might detonate a nuclear weapon high in the atmosphere to create a powerful nuclear-induced electromagnetic pulse (EMP) that could prove lethal to air defense radars, military communications systems, and much civilian infrastructure over a region many hundreds of kilometers in radius. A Russian EMP burst using a high-altitude nuclear weapon would be an extremely provocative and risky move, to be sure. 57 But some Russian leaders could argue that it was not strictly speaking a nuclear attack, since no humans would be killed by the direct explosive effects of such a weapon—and thus might delude themselves into thinking it was a relatively low-risk option. In fact, the risks could be very high. Some types of EMP attacks (or even cyberattacks) by Russia could ~~disable~~ [shut down] large chunks of the U.S. or European electricity grids for many months.58 A severe attack of this type might even lead to a U.S. nuclear response, in light of the new nuclear doctrine of the Trump administration. 59 Beyond the EMP option, Russia could use nuclear weapons directly against ships that carried military equipment, missile defense radars, or other capabilities. Indeed, it threatened to target nuclear missiles at any Danish ships joining the U.S.-led missile defense effort in 2015. Again, the provocation would be enormous— but the direct human stakes might be fairly limited, since only dozens of sailors, or at most a couple hundred, might be on a given naval vessel. 60 Moscow might, perhaps delusionally, think the risks were acceptable. Of course, there would be enormous significance and risk to crossing the nuclear threshold in any way. But if weapons were used against isolated military targets (as both sides contemplated in various ways during the Cold War), Moscow again might convince itself, rightly or wrongly, that escalation risks could be tolerated and managed. That might be particularly true for attacks limited to the kinds of target sets that posed disproportionate vulnerability and dependence for NATO. These could include cargo ships at sea, rail marshaling yards where train tracks change gauge (necessitating unloading and reloading) at the Poland- Lithuania border, or particularly weak bridges without nearby alternative routes. 61 If Russia could limit NATO fatalities to hundreds of sailors and not itself present any target sets that were characterized by a similar combination of relatively high military importance and relatively great separation from vulnerable civilian populations, NATO might not have a good recourse. Moscow might hope as much, at least—and so elect to roll the dice. Such a decision would be reckless and foolish, but perhaps not beyond the pale of how human beings have behaved historically in wars they felt they were otherwise likely to lose.

#### Grid collapse causes extinction

Weiss 19—National Sales Director at United Medical Instruments, UMI and Research assistant at the American Jewish University [Matthew Weiss and Martin Weiss (Neurosurgeon at UCLA-Olive View Medical Center), 5/29/2019, “An assessment of threats to the American power grid”, Energy, Sustainability and Society, Volume 9, Article number: 18, <https://energsustainsoc.biomedcentral.com/articles/10.1186/s13705-019-0199-y#Sec2>] AMarb

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. A prescription for failure Even if all the recommendations of the Congressional EMP Commission were implemented, there is no guarantee that the grid will not sustain a prolonged collapse. There should therefore be contingency plans for such a failure. There is also another consideration. The foundational pillars of prior American nuclear defense policy, in today’s climate, are of uncertain validity. Mutual assured destruction is the Maginot line of the 21st century. Nonproliferation will prove difficult to resurrect. The consequences of a widespread nuclear attack have been positioned to the public as massive deaths from blast effects, and then further lingering deaths from the effects of radiation. We suspect there will be no electricity, and there will be no electricity for a very long time. There should be an actionable plan in anticipation of a possible prolonged collapse of the grid—a retro-structure and a skill set to provide a framework for survival. Our sense is there is no plan.

#### Cyberwar causes nuclear war and draw-in even if NATO-Russia war does not---independently crushes nuclear deterrence

Michael T. Klare 19, professor emeritus of peace and world security studies at Hampshire College and senior visiting fellow at the Arms Control Association., 11-1-2019, "Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation," No Publication, <https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#bio>, language edited change denoted by brackets

For the past several years, the U.S. Department of Defense has been exploring how it could employ its own very robust cyberattack capabilities to compromise or destroy enemy missiles from such states as North Korea before they can be fired, a strategy sometimes called “left of launch.”3 Russia and China can assume, on this basis, that their own launch facilities are being probed for such vulnerabilities, presumably leading them to adopt escalatory policies such as those espoused in the 2018 NPR report. Wherever one looks, therefore, the links between cyberwar and nuclear war are growing. The Nuclear-Cyber Connection These links exist because the NC3 systems of the United States and other nuclear-armed states are heavily dependent on computers and other digital processors for virtually every aspect of their operation and because those systems are highly vulnerable to cyberattack. Every nuclear force is composed, most basically, of weapons, early-warning radars, launch facilities, and the top officials, usually presidents or prime ministers, empowered to initiate a nuclear exchange. Connecting them all, however, is an extended network of communications and data-processing systems, all reliant on cyberspace. Warning systems, ground- and space-based, must constantly watch for and analyze possible enemy missile launches. Data on actual threats must rapidly be communicated to decision-makers, who must then weigh possible responses and communicate chosen outcomes to launch facilities, which in turn must provide attack vectors to delivery systems. All of this involves operations in cyberspace, and it is in this domain that great power rivals seek vulnerabilities to exploit in a constant struggle for advantage. The use of cyberspace to gain an advantage over adversaries takes many forms and is not always aimed at nuclear systems. China has been accused of engaging in widespread cyberespionage to steal technical secrets from U.S. firms for economic and military advantages. Russia has been accused, most extensively in the Robert Mueller report, of exploiting cyberspace to interfere in the 2016 U.S. presidential election. Nonstate actors, including terrorist groups such as al Qaeda and the Islamic State group, have used the internet for recruiting combatants and spreading fear. Criminal groups, including some thought to be allied with state actors, such as North Korea, have used cyberspace to extort money from banks, municipalities, and individuals.4 Attacks such as these occupy most of the time and attention of civilian and military cybersecurity organizations that attempt to thwart such attacks. Yet for those who worry about strategic stability and the risks of nuclear escalation, it is the threat of cyberattacks on NC3 systems that provokes the greatest concern. Gen. Paul M. Nakasone, commander of U.S. Cyber Command, testifies during a Senate Armed Services Committee hearing on February 14. He warned that China and Russia are conducting sustained cybercampaigns against the United States. (Photo: Mark Wilson/Getty Images)Gen. Paul M. Nakasone, commander of U.S. Cyber Command, testifies during a Senate Armed Services Committee hearing on February 14. He warned that China and Russia are conducting sustained cybercampaigns against the United States. (Photo: Mark Wilson/Getty Images)This concern stems from the fact that, despite the immense effort devoted to protecting NC3 systems from cyberattack, no enterprise that relies so extensively on computers and cyberspace can be made 100 percent invulnerable to attack. This is so because such systems employ many devices and operating systems of various origins and vintages, most incorporating numerous software updates and “patches” over time, offering multiple vectors for attack. Electronic components can also be modified by hostile actors during production, transit, or insertion; and the whole system itself is dependent to a considerable degree on the electrical grid, which itself is vulnerable to cyberattack and is far less protected. Experienced “cyberwarriors” of every major power have been working for years to probe for weaknesses in these systems and in many cases have devised cyberweapons, typically, malicious software (malware) and computer viruses, to exploit those weaknesses for military advantage.5 Although activity in cyberspace is much more difficult to detect and track than conventional military operations, enough information has become public to indicate that the major nuclear powers, notably China, Russia, and the United States, along with such secondary powers as Iran and North Korea, have established extensive cyberwarfare capabilities and engage in offensive cyberoperations on a regular basis, often aimed at critical military infrastructure. “Cyberspace is a contested environment where we are in constant contact with adversaries,” General Paul M. Nakasone, commander of the U.S. Cyber Command (Cybercom), told the Senate Armed Services Committee in February 2019. “We see near-peer competitors [China and Russia] conducting sustained campaigns below the level of armed conflict to erode American strength and gain strategic advantage.” Although eager to speak of adversary threats to U.S. interests, Nakasone was noticeably but not surprisingly reluctant to say much about U.S. offensive operations in cyberspace. He acknowledged, however, that Cybercom took such action to disrupt possible Russian interference in the 2018 midterm elections. “We created a persistent presence in cyberspace to monitor adversary actions and crafted tools and tactics to frustrate their efforts,” he testified in February. According to press accounts, this included a cyberattack aimed at paralyzing the Internet Research Agency, a “troll farm” in St. Petersburg said to have been deeply involved in generating disruptive propaganda during the 2016 presidential elections.6 Other press investigations have disclosed two other offensive operations undertaken by the United States. One called “Olympic Games” was intended to disrupt Iran’s drive to increase its uranium-enrichment capacity by sabotaging the centrifuges used in the process by infecting them with the so-called Stuxnet virus. Another left of launch effort was intended to cause malfunctions in North Korean missile tests.7 Although not aimed at either of the U.S. principal nuclear adversaries, those two attacks demonstrated a willingness and capacity to conduct cyberattacks on the nuclear infrastructure of other states. Efforts by strategic rivals of the United States to infiltrate and eventually degrade U.S. nuclear infrastructure are far less documented but thought to be no less prevalent. Russia, for example, is believed to have planted malware in the U.S. electrical utility grid, possibly with the intent of cutting off the flow of electricity to critical NC3 facilities in the event of a major crisis.8 Indeed, every major power, including the United States, is believed to have crafted cyberweapons aimed at critical NC3 components and to have implanted malware in enemy systems for potential use in some future confrontation. Pathways to Escalation Knowing that the NC3 systems of the major powers are constantly being probed for weaknesses and probably infested with malware designed to be activated in a crisis, what does this say about the risks of escalation from a nonkinetic battle, that is, one fought without traditional weaponry, to a kinetic one, at first using conventional weapons and then, potentially, nuclear ones? None of this can be predicted in advance, but those analysts who have studied the subject worry about the emergence of dangerous new pathways for escalation. Indeed, several such scenarios have been identified.9 The first and possibly most dangerous path to escalation would arise from the early use of cyberweapons in a great power crisis to ~~paralyze~~ the vital command, control, and communications capabilities of an adversary, many of which serve nuclear and conventional forces. In the “fog of war” that would naturally ensue from such an encounter, the recipient of such an attack might fear more punishing follow-up kinetic attacks, possibly including the use of nuclear weapons, and, fearing the loss of its own arsenal, launch its weapons immediately. This might occur, for example, in a confrontation between NATO and Russian forces in east and central Europe or between U.S. and Chinese forces in the Asia-Pacific region. Speaking of a possible confrontation in Europe, for example, James N. Miller Jr. and Richard Fontaine wrote that “both sides would have overwhelming incentives to go early with offensive cyber and counter-space capabilities to negate the other side’s military capabilities or advantages.” If these early attacks succeeded, “it could result in huge military and coercive advantage for the attacker.” This might induce the recipient of such attacks to back down, affording its rival a major victory at very low cost. Alternatively, however, the recipient might view the attacks on its critical command, control, and communications infrastructure as the prelude to a full-scale attack aimed at neutralizing its nuclear capabilities and choose to strike first. “It is worth considering,” Miller and Fontaine concluded, “how even a very limited attack or incident could set both sides on a slippery slope to rapid escalation.”10 U.S. servicemen conduct a defensive cyberoperations exercise at Ramstein Air Base, Germany, on March 8. (U.S. Air Force photo by Master Sgt. Renae Pittman)U.S. servicemen conduct a defensive cyberoperations exercise at Ramstein Air Base, Germany, on March 8. (U.S. Air Force photo by Master Sgt. Renae Pittman)What makes the insertion of latent malware in an adversary’s NC3 systems so dangerous is that it may not even need to be activated to increase the risk of nuclear escalation. If a nuclear-armed state comes to believe that its critical systems are infested with enemy malware, its leaders might not trust the information provided by its early-warning systems in a crisis and might misconstrue the nature of an enemy attack, leading them to overreact and possibly launch their nuclear weapons out of fear they are at risk of a preemptive strike. “The uncertainty caused by the unique character of a cyber threat could jeopardize the credibility of the nuclear deterrent and undermine strategic stability in ways that advances in nuclear and conventional weapons do not,” Page O. Stoutland and Samantha Pitts-Kiefer wrote in 2018 paper for the Nuclear Threat Initiative. “[T]he introduction of a flaw or malicious code into nuclear weapons through the supply chain that compromises the effectiveness of those weapons could lead to a lack of confidence in the nuclear deterrent,” undermining strategic stability.11 Without confidence in the reliability of its nuclear weapons infrastructure, a nuclear-armed state may misinterpret confusing signals from its early-warning systems and, fearing the worst, launch its own nuclear weapons rather than lose them to an enemy’s first strike. This makes the scenario proffered in the 2018 NPR report, of a nuclear response to an enemy cyberattack, that much more alarming.

#### Nuclear deterrence solves existential threats

Chilton 18—USAF, Retired Former commander, US Strategic Command [General Kevin P. Chilton, Spring 2018, “Defending the Record on US Nuclear Deterrence”, Strategic Studies Quarterly, <https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-1/Chilton.pdf?ver=2018-02-14-170000-437>] AMarb

Some argue the US nuclear deterrent should be eliminated because its existence represents Cold War think. If nuclear deterrence is Cold War think, then one might posit machine guns are World War I think and main battle tanks are World War II think and conclude the US does not need those anymore for the defense of the nation. In fact, nuclear deterrence is not Cold War think. The reality is nuclear deterrence underpins the national security of the United States and will continue to do so for the foreseeable future. It remains relevant and necessary today to deter the existential threats to our nation posed by both Russia and China and by lesser but certainly horrific threats posed by the Democratic People’s Republic of North Korea. It also helps to deter nonnuclear attacks that could have catastrophic consequences, such as attacks involving biological weapons. The term Cold War think is a pejorative typically proffered by those who have never thought seriously about, let alone studied, deterrence theory or by those who have run out of ways to defend their position. It is generally the last throwaway line of argument from an uninformed antinuclear ideologue. “No One Would Ever Use a Nuclear Weapon against the United States” Those who would use this argument seem willing to risk the very existence of the nation on the basis of their speculation and without forethought. However, this is not a wager military planners should ever risk. The US military must ensure national survival through deterrence provided by a safe, secure, capable, reliable, flexible, and vigilant nuclear posture. It is our duty to assume the worst and then take steps to ensure it never happens. Additionally, we must deter attacks on our friends, allies, and fielded US military forces deployed abroad. This will become more challenging as Russia, China, and North Korea appear to include the possible employment of nuclear weapons in their planning; indeed, Russia and North Korea openly discuss nuclear weapons as instruments to be used in future conventional conflicts with the US and NATO.

### 1ac – NATO Unity

#### Diverging cyber security policies lock in current rifts in the alliance.

Dr. Max Smeets 21 [Center for Security Studies, ETH Zürich (Switzerland). “NATO allies’ offensive cyber policy: A growing divide?”. August 6, 2021. https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/]

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.

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] 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.

#### Russia will exploit divisions between NATO members to instigate nuclear crises---extinction.

Kulesa ’18 [Lukasz; February 2018; Research Director at the European Leadership Network; European Leadership Network, “Envisioning a Russia-NATO Conflict: Implications for Deterrence Stability,” <http://www.jstor.com/stable/resrep17437>]

Escalation: Can a NATO - Russia conflict be managed?

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

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

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

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

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

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

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

Conflict termination

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

#### NATO cohesion checks numerous existential crises.

Gallagher ’19 [Mike and Colin Dueck; January 2019; Representative for Wisconsin’s Eighth District in the U.S. House of Representatives; Professor in the Schar School of Policy and Government at George Mason University; National Review, “The Conservative Case for NATO,” <https://www.nationalreview.com/2019/01/nato-western-military-alliance-bolsters-american-interests/>]

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

#### Russian cyber ops are the key to their strategy of disrupting NATO unity- fragmentation gives Russia leverage to increase populism.

Oscar Jonsson in 2021

scholar of strategy, emerging technology and Russia who is founder of Phronesis Analysis and Researcher at Swedish Defence University; FROM EASTERN FLANK TO WESTERN ELECTIONS: RUSSIAN OPERATIONS AGAINST THE EU AND NATO; The Center for European Policy Analysis; https://cepa.org/the-evolution-of-russian-hybrid-warfare-eu-nato/

While Russian influence operations have a history that goes far beyond the concept of hybrid warfare, they have seldom gotten such attention. This chapter investigates the evolution of Russian hybrid means and the ends to which they are applied. The Russian leadership’s best bet against the collective West is currently in these operations. The core of countering them lies in changing the Russian cost-benefit analysis that suggests, so far, that conducting these operations holds great rewards and carries fairly small risks.¶ 1. RUSSIAN GOALS AND THE LIMITS OF RUSSIAN POWER¶ At their foundations, the European Union (EU) and NATO are based on a political agreement that acknowledges mutual interests, security, and support. This is the focus of the conflict between Russia and the West (here shorthand for the EU and NATO). Russia stands little chance of prevailing in this conflict in the face of a committed and united West. Conversely, it has a great opportunity to succeed against a divided West. Unfortunately, many divisions exist that can be exploited. Fragmenting the West’s political unity lies at the core of Russia’s strategy as it seeks to promote economic ties with some European states — Germany and France — while isolating and provoking others. This paper focuses on Russian influence operations against both the EU and NATO as well as individual member states.¶ The Russian leadership’s ability to achieve its goals — regime security and great power status through weakening the EU and NATO — comes from its power of destruction rather than its power of attraction. Russia has few true allies in the world. Even China, which shares an increasingly close relationship with Russia, cannot be considered an ally.1¶ The United States and Europe have seen increasing political polarization and decreasing trust in democracy over the past few decades.2 Russia has sought to exploit this fact through its support for far-right and populist actors and movements that are united in their opposition to the EU, NATO, or simply “the establishment.”3 This enables Russia to have a destructive influence over processes that are already contentious.¶ Elections and referenda, which, in essence, are processes to settle political contention, are particularly vulnerable. The core idea of popular votes is that even if one’s own side does not win, one will accept the outcome as the process was free and fair. There is, therefore, an incentive for Russia to influence the outcome of these processes to sow doubt and create instability.4 The European Parliament accurately summarized the goal of Russian cyber operations targeting the EU as: “distorting truths, provoking doubt, dividing Member States, engineering a strategic split between the European Union and its North American partners and paralyzing the decision-making process, discrediting the EU institutions and transatlantic partnerships … undermining and eroding the European narrative based on democratic values, human rights and the rule of law.”5

#### Populism increases the risk the nuclear world order and non-proliferation norms – causes global nuclear war.

Meier & Vieluf ’21 — Oliver Meier; Senior Researcher at the Institute for Peace Research and Security Policy. Prior to this, he was Deputy Head in the International Security Division of the German Institute for International and Security Affairs. Maren Vieluf; Researcher at Institute for Peace Research and Security Policy. December 16, 2021; "Upsetting the nuclear order: how the rise of nationalist populism increases nuclear dangers"; *The Nonproliferation Review*; <https://doi.org/10.1080/10736700.2020.1864932>; //CYang

Nationalist populists as leaders of states that possess nuclear weapons undermine the nuclear order and increase nuclear dangers in novel, significant, and persistent ways. Such leaders talk differently about nuclear weapons; they can put nuclear policy making and crisis management in disarray; and they can weaken international alliances and multilateral nuclear institutions. The rise of nationalist populists in nuclear-armed states, including some of the five nuclear-weapon states recognized under the 1968 Treaty on the Nonproliferation of Nuclear Weapons, shatters the presumed distinction between responsible and irresponsible nuclear powers and complicates attempts to heal rifts in the international order. Policies to wait out populists or to balance their influence in multilateral institutions seem to have had limited success. A sustainable strategy to deal with the challenge posed by populists would need to start by recognizing that we can no longer assume that nuclear weapons are safe in the hands of some states but not in others’. Introduction The rise of nationalist populists1 to power in nuclear-armed states and their allies is undermining the nuclear order and raising the risks of nuclear war. That populists such as Boris Johnson, Narendra Modi, Vladimir Putin, and Donald Trump were able to take charge of nuclear arsenals, including in some of the nuclear powers recognized under the 1968 Treaty on the Non-Proliferation of Nuclear Weapons (NPT), challenges the assumption that established nuclear-weapon states behave responsibly. Nationalist populism,2 understood as a nationalist, anti-elitist, illiberal, and anti-pluralist set of ideas and politics conducted in the supposed interests of “the people” — that is, the domestic constituencies of the nationalist-populist leaders—has been on the rise globally since the mid-2000s. It has come to include the leadership of a growing number of countries3 and has begun to influence the effectiveness of time-honored institutions of the nuclear order. We argue that this rise of nationalist populists and their foreign and defense policies weakens the nuclear order in novel, significant, and persistent ways. Three characteristics are typical of nationalist populists’ nuclear policies: they talk differently about nuclear weapons; they have a specific way of getting involved in national decision making on nuclear-weapon issues; and their approach to international alliances and institutions is unique. The fact that nationalist-populist leaders have assumed control over nuclear weapons in countries at the core of the nuclear order shatters the presumed distinction between “responsible” and “irresponsible” nuclear powers. These leaders threaten the nuclear order built on the principled acceptance of a logic of restraint by the nuclear-weapon states.

#### Russian cyber ops undermine NATO unity through the spread of disinformation, which causes democratic backsliding.

Ivana Stradner 5/17/22

Advisor; Russian Disinformation and Propaganda in Relation to the War Against Ukraine¶ Subcommittee on Security and Defence; Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation; Testimony to European Parliament; https://www.fdd.org/analysis/2022/05/17/russian-disinformation-propaganda/

Given Russia’s military shortcomings in Ukraine, many in the West are already celebrating his failure. However, it is too early to do so, in part because Putin still has a powerful non-military tool at his disposal: information weapons. The Kremlin does not limit itself to hacking our computers — it also wants to hack our minds, aiming to disrupt our democracies, polarize our societies, and sow fear and doubt among our populations.¶ The importance of information operations is clear to anyone who follows Russia closely. The Soviets were known for “active measures.” They used disinformation campaigns to shape the information space abroad and influence events in other countries; they often referred to these campaigns as “political warfare.”¶ Russian active measures today do not differ in their goals. The only difference is in the technology used to pursue them. Social media platforms allow Russia both to increase its reach and to target specific audiences when conducting information operations, which Moscow uses both for political warfare and to augment conventional military operations. Last year, Russia published a new National Security Strategy, in which it devoted an entire section to “information security.” Similarly, Russian Minister of Defense Sergey Shoigu declared that “information has become a weapon.” In 2017, Russian officials acknowledged the establishment of information warfare troops.¶ Moscow’s information operations and other hybrid warfare undertakings in Europe aim to undermine European security and NATO unity.¶ Russia’s information campaigns are integral part of its hybrid warfare strategy. Russian information operations against Ukraine kicked into high gear in 2014. When the war started, Russia used disinformation to shape the information space. For instance, Moscow claimed that NATO’s enlargement was a threat to Russia. Russia and Putin have spread a long line of such falsehoods about Ukraine. Moscow claimed that Russian-language speakers in Ukraine faced “genocide” at Kyiv’s hands and would welcome a Russian invasion. Moscow denied Ukrainian statehood, claiming Ukraine has always been part of Russia and framing its “special military operation” as necessary to “liberate” Ukrainians from their “Nazi leader.” This messaging was intended to be consumed inside Russia, in Ukraine, and globally. Ukraine, which has been strengthening its information operations tools for over a decade, has achieved notable victories in this space since the war began.

#### Democracy solves every impact---it’s comparatively more stable than autocracies

MattKroenig 20**,** Professor of government and foreign service at Georgetown. 4/3 “Why the U.S. Will Outcompete China” <https://www.theatlantic.com/ideas/archive/2020/04/why-china-ill-equipped-great-power-rivalry/609364/>

National-security analysts see China as one of the greatest threats facing the United States and its allies. According to an emerging conventional wisdom, China has the leg up on the U.S. in part because its authoritarian government can strategically plan for the long term, unencumbered by competing branches of government, regular elections, and public opinion. **Yet this faith in autocratic ascendance and democratic decline is contrary to historical fact. China may be able to put forth big, bold plans**—the kinds of projects that analysts think of as long term—**but the visionary projects of autocrats don’t usually pan out**. Watch White Noise, the inside story of the alt-right The Atlantic’s first feature documentary ventures into the underbelly of the far-right movement to explore the seductive power of extremism. Stream Now Yes, democratic governments are obligated to answer to their citizens on regular intervals and are sensitive to public opinion—t**hat’s actually democracies’ greatest source of strength. Democratic leaders have a harder time advancing big, bold agendas**, but the upside of that difficulty is that the plans that do make it through the system have been carefully considered and enjoy domestic support. Historically speaking, once a democracy comes up with a successful strategy, it sticks with the plan, even through a succession of leadership. Washington has arguably followed the same basic, three-step geopolitical plan since 1945. First, the United States built the current, rules-based international system by providing security in important geopolitical regions, constructing international institutions, and promoting free markets and democratic politics within its sphere of influence. Second, it welcomed into the club any country that played by the rules, even former adversaries, like Germany and Japan. And, third, the U.S. worked with its allies to defend the system from those countries or groups that would challenge it, including competitors such as Russia and China, rogue states such as Iran and North Korea, and terrorist networks. America can pursue long-term strategy in part because it enjoys domestic political stability. While new politicians seek to improve on their predecessor’s policies, the United States is unlikely to see the drastic shifts in strategy that come from the fall of one political system and the rise of another. Democratic elections may be messy, but they’re not as messy as coups or civil wars. Daniel Blumenthal: The Unpredictable Rise of China **Open societies** have many other advantages as well. They **facilitate innovation**, **trust in financial markets**, and economic growth. Because **democracies** tend to be more reliable partners, they **are typically skillful alliance builders**, and they can accumulate resources without frightening their neighbors. **They tend to make thoughtful, informed decisions on matters of war and peace**, and to focus their security forces on external enemies, not their own populations. Autocratic systems simply cannot match this impressive array of economic, diplomatic, and military attributes. David Leonhardt recently wrote in The New York Times, “Chinese leaders stretching back to Deng Xiaoping have often thought in terms of decades.” Commonly cited examples of that long-term thinking include the Belt and Road Initiative, a program that invests in infrastructure overseas; Made in China 2025, an effort to subsidize China’s giant tech companies to become world leaders in 21st-century technologies, such as artificial intelligence; and Beijing’s promise to be a global superpower by 2049. Since putting in place sound economic reforms in the 1970s, China has seen its economy expand at eye-popping rates, to become the world’s second largest. Many economists predict that China could even surpass the United States within the decade, and some have suggested that China’s model of state-led capitalism will prove more successful, in terms of economic growth, than the U.S. template of free markets and open politics. I doubt these predictions. Because autocratic leaders are unconstrained and do not have to contend with a legislature or courts, they have an easier time taking their countries in new and radically different directions. Then, when the dictator changes his mind, he can do it again. Mao’s autocratic China ricocheted from one failed policy to another: the Great Leap Forward, then the Hundred Flowers Campaign, then the Cultural Revolution. Mao aligned with the Soviet Union in 1950 only to nearly fight a nuclear war with Moscow in the next decade. Beginning in the time of Deng Xiaoping, China pursued a fairly constant strategy of liberalizing its economy at home and “hiding its capabilities and biding its time” abroad. But President Xi Jinping abandoned these dictums when he took over. As the most powerful leader since Mao—he has changed China’s constitution to set himself up as dictator for life—he could once again jerk China in several new directions, according to his whims, and back again. According to the Asia Society, he has stalled or reversed course on eight of 10 categories of economic reform promised by the Chinese Communist Party (CCP) itself. Moreover, Xi is baring China’s teeth militarily, taking contested territory from neighbors in the South China Sea and conducting military exercises with Russia in Europe. The problem for Beijing is that stalled reforms will stymie its economic potential and its confrontational policies are provoking an international coalition to contain them. The 2017 U.S. National Security Strategy declared great-power competition with China the foremost security threat to the U.S.; the European Union labeled China a “systemic rival”; and Japan, Australia, India, and the United States have formed a new “quad” of powers to balance China in the Pacific. Furthermore, the plans often cited as evidence of China’s farsighted vision, the Belt and Road Initiative and Made in China 2025, were announced by Xi only in 2013 and 2015, respectively. Both are way too recent to be celebrated as brilliant examples of successful, long-term strategic planning. A certain level of domestic political stability is a prerequisite for charting a steady strategic course in foreign and domestic affairs. **But autocratic regimes are notoriously brittle. While institutionalized political successions in democracies typically lead to changes of policy, political successions in autocracies are likely to result in regime collapse and war**. China’s “5,000 years of history” were pockmarked by rebellion, revolution, and new dynasties. Fearing internal threats to domestic political stability—consider the protests this year in Hong Kong and Xinjiang—the CCP spends more on domestic security than on its national defense. If you follow the money, the CCP is demonstrating that the government is more afraid of its own people than of the Pentagon. This domestic fragility will frustrate China’s efforts to design and execute farsighted plans. If threats to Chinese domestic stability were to materialize and the CCP were to collapse tomorrow, for example, Chinese grand strategy could undergo another seismic shift, including possibly opting out of competition with the United States altogether. Shadi Hamid: China Is Avoiding Blame by Trolling the World Autocracies have other vulnerabilities as **well. State-led planning has never produced high rates of economic growth over the long term. Autocrats are poor alliance builders** who fight with their supposed allies more than with their enemies. And the highest priority of autocratic security forces is repressing their own people, not defending the country. The world has undergone drastic changes in just the past few years, but these enduring patterns of international affairs have not. Some fear that Trump’s nationalist tendencies will erode the U.S. position, but the momentum of America’s successful grand strategy has kept the country on a fairly steady course. Despite Trump’s criticism of NATO, for example, two new countries have joined the alliance on his watch, including North Macedonia this week. The coronavirus has upended a sense of security in the U.S., leading many people into the familiar trap of lauding autocratic China’s firm response in contrast to the halting and patchwork measures in the United States. But there is good reason to believe that this assessment will be updated in America’s favor with the benefit of hindsight. Already we are seeing evidence that conditions are much worse in China than CCP officials are letting on and that China’s attempts at international “disaster diplomacy” are backfiring. It has been revealed that the CCP has continually misrepresented the numbers of COVID-19 infections and deaths in China, and European nations have rejected and returned faulty Chinese coronavirus testing kits.

### 1ac – Plans

#### Text v1

#### The United States should substantially increase its cybersecurity cooperation with the North Atlantic Treaty Organization.

#### Text v2

**The United States should substantially increase its cybersecurity intelligence sharing and training and capacity-building for cyber operations within the North Atlantic Treaty Organization.**

### 1ac – Solvency

#### The plan solves Increased intelligence sharing, coordination, and training leads to better attribution and response frameworks – that’s key to effective cyber deterrence and mitigation.

Maigre ’22 (Merle Maigre is a Non-resident Senior Fellow with CEPA's Transatlantic Leadership Program and CEPA's Digital Innovation Initiative, as well as the Senior Cyber Security Expert at Estonia’s e-Governance Academy, a non-profit that helps governments go digital. “NATO’s Role in Global Cyber Security,” April 2022, German Marshall Fund of the United States at Harvard University, https://www.gmfus.org/sites/default/files/2022-04/Maigre%20-%20NATO%20-%20Geopolitics%20-%20Cyber%20-%20final.pdf)-mikee

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 transparency. 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 consequences. With attribution, policymakers show that they know what is happening in these networks and can investigate incidents. It also clearly spells out unacceptable behavior and can help create state practice. The best way to implement the international norms is by calling out behavior and having consequences when these norms are breached. Attribution will make clear to the malicious actor that their actions will be seen and addressed. It is the basis, under international law, for countermeasures and self-defense. When should states publicly attribute cyberattacks? Effective public attribution requires a clear understanding of the attributed cyber operation and the cyber-threat actor, but also the broader geopolitical environment, allied positions and activities, and the legal context. The public attribution framework put forward by Max Smeets and Florian Egloff in March 2021 27 distinguishes four factors that act as enablers or constraints in public attribution. These factors are intelligence, incident severity, geopolitical context, and post-attribution actions. The combination of these four components enables consistent decision-making about whether to publicly disseminate information about an adversary’s actions, privately tell the adversary, or restrict knowledge of the intrusion to the government and potentially other partners. Collecting and processing intelligence—information about foreign countries and their agents— provides a technical basis for attribution. How could allies improve intelligence sharing to conduct more rapid attribution and enable a response to adversary cyber activity? During the Nordic-Baltic foreign ministers meeting in Tallinn in September 2020, a 90-minute tabletop exercise was organized28 to test the ministers’ ability to respond to and attribute an escalating cyberattack. They answered multiple-choice questions on communication of and possible diplomatic countermeasures to the attack. The ministers learned through first-hand experience that a timely exchange of technical intelligence can be key in attributing any cyberattack. “The shared view [of the countries involved]—especially when it comes to complicated issues—is crucial,” said Urmas Reinsalu, Foreign Minister of Estonia.29 Attribution is only as good as the information that allies are willing to share. NATO’s value can be in becoming the preferred platform for sharing cyber information. General Paul Nakasone, who heads US Cyber Command, told the House Armed Services subcommittee on intelligence that “in 35 years” he has never seen a better sharing of accurate, timely, and actionable intelligence than what has transpired with Ukraine. 30 Sharing information and intelligence with allies “builds coalitions” and can “shine a light on disinformation” campaigns, like the one Russia used to lay the groundwork for their invasion of Ukraine. As the second course of action, NATO should use the current crisis to accelerate the progress with setting up NATO’s own cyber command and sharpen allied responses to malicious cyber actions. Overall, this would give more credibility to its cyber defense. In February 2019, allies endorsed a set of tools to respond to cumulative cyber activities, but not much has happened to take it forward. It is now time to build upon this set and develop concrete steps at the political, military, and technical levels to model alliance behavior according to the threat landscape. This means a sharper focus on future responses to highand low-end cyberattacks along with concrete deterrence actions and tools for individual sectors and target types. Much of this is based on the high-end cyber capabilities of select individual allies called “volunteer sovereign cyber effects,” where cybercapable nations deliver voluntarily offensive cyber effects on a target designated by an operational-level commander. The NATO Cyber Command would be responsible for matching military needs with the willingness and capabilities of the nations potentially able to deliver such effects.31 The alliance should clarify which allies are responsible for offensive cyber operations against certain targets and the information-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 Cooperative Cyber Defense Centre of Excellence (CCDCOE) Locked Shields exercise is a good way to do so. Organized 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 activities should be practiced among allies and with likeminded 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 Maryland, 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. The third action focuses on building resilience of domestic critical infrastructures. Doors are locked to keep homes safe. Likewise, all NATO member states should address their digital insecurity by locking digital doors as individuals, companies, and countries. The strategic vulnerability to disruption and sabotage lies not so much in the military space but in the hospital booking system, logistics schedule, power grid, and thousands of other mainstream, civilian, mostly privately owned networks. Based on the 2016 Cyber Defence Pledge, in which member states committed to improving their ability to protect their cyber networks, the alliance could formulate a NATO cyber-security baseline with concrete resilience goals to achieve or maintain the baseline. These resilience goals could then be apportioned among member states in the same way as the defense-planning capability targets. This should come with obvious financial and investment implications. Public debates on burden sharing within NATO for too long have focused on how much member states spend on defense in isolation, without adequate prioritizing where those funds are going. Member states should be rethink defense spending relative to emerging threats and collective security challenges. To ensure funding for cyber security is appropriately prioritized, NATO should strengthen a commitment to digital defense spending, building on the strong base it has developed in terms of doctrine, standards, and requirements. This also includes strengthening the political resilience of member states by broadening NATO consultations to include more areas of government. Regular North Atlantic Council-format meetings among member state directors of cyber authorities at the political and military levels would help build consensus on cyber policy issues. Another course of action for NATO in cyber security is to increase its cyber capacity-building efforts for partner countries of strategic importance, reinforcing NATO’s commitment to partners and projecting stability in NATO’s neighborhood. This kind of cyber capacity-building could include various types of support, ranging from strategic advice and cyber institution-building in defense sectors to education and training or advice and assistance in cyber defense. The objective should to be to enable capacity-building activities for military actors, along with the provision of training, equipment, and infrastructure for security purposes. This would allow NATO to improve the capacities of partners to address crises, prevent conflicts, and cater for their own security and stability by themselves, to the benefit of their population. As one example, NATO could fill a gap in capacity building for partner countries by bringing together military Computer Emergency Response Teams (CERTs) to share information on incident management dynamics, a key factor in modern cyber defense. While partner countries can receive support from donors in establishing mechanisms and processes to exchange information between civilian CERTs, such cooperation and communication channels are much less developed in the military domain due in large part to the high sensitivity of the information. There is a need to extend the information-sharing practices used in civilian circles to partner countries’ military CERTs. Building cyber-security capacity should focus on partners’ ability to respond to and recover from cyber incidents. In sum, most future conflicts will have cyber components that require a technical, political, and diplomatic response. Whether the adversary is a state’s elite unit or a criminal group rendering ransomware as a service, cyber security is about risk management and solid, pragmatic defense and response measures to improve the security of the digital environment. There is a technical aspect to hardening defenses and building redundancy in data and services, but the core of resilience lies in leadership that does not ignore the problem. How our national cyber-security strategies are translated into policies and procedures needs to be understood by all stakeholders. It is now up to the alliance’s member states to provide clarity and coherence to successfully draft a new Strategic Concept that includes defense and deterrence. But this is not a job for NATO alone—it requires close coordination across national governments and the private sector, and NATO and the European Union must therefore continue to work very closely on this vital issue.

#### Increased US cyber security cooperation, in the form of intelligence sharing and training, solves NATO cohesion and cyber deterrence.

Porter & Jordan ’19 (Christopher Porter is the chief intelligence strategist of cybersecurity company FireEye and a nonresident senior fellow at the Atlantic Council; Klara Jordan is director of the Cyber Statecraft Initiative at the Atlantic Council’s Scowcroft Center for Strategy and Security; Don’t Let Cyber Attribution Debates Tear Apart the NATO Alliance; <https://www.lawfareblog.com/dont-let-cyber-attribution-debates-tear-apart-nato-alliance>)-mikee

Long-Term Thinking In the long run, though, the U.S. and its more technologically advanced allies—such as its fellow Five Eyes (Australia, Canada, New Zealand and the U.K.), France and Japan—will have to make important policy changes in the interests of furthering alliance cooperation in cyberspace: a willingness to sometimes risk sensitive sources and methods in order to get cyber threat intelligence into the hands of other countries better positioned to take policy action, an end to classifying public information like IP addresses solely because of their acquisition via classified means, and greater transparency on their own decision-making. Government cyber leaders within the alliance should consider taking another page out of the private-sector playbook as well: running cyber-crisis exercises that involve more than the IT department. In the commercial world, the more successful practice runs involve leaders at both the CISO level and some presence from nontechnical teams that would weigh in during a crisis, such as communications and legal. The best exercises involve executives, too, who despite their busy schedules must see for themselves how their companies would survive and respond during a potentially ruinous cyberattack, and work through the minutiae of leading a response themselves. The experience and confidence is invaluable if ever called on during a real-life crisis, and the organizational introspection by involving decision-makers at all levels is irreplaceable. Military-to-military cyber training as part of cross-country force standardization and joint operational planning could pull in more senior national leadership, beyond battlefield commanders, and be coupled with increased funding for foreign affairs-led training for nontechnical leaders. The private sector could also meaningfully contribute during NATO consultations when developing Allied Joint Publications to make sure that definitions and requirements for threat intelligence incorporate the best practices of NATO member countries’ private sectors. If a U.S. diplomat reaches out to his or her counterpart in an allied country to ask for assistance responding to malware that’s damaging critical infrastructure, and that counterpart has to ask what malware is, the response isn’t going to happen. \*\*\* NATO’s essential and enduring purpose is to safeguard the freedom and security of all its members by political and military means. Tolerating cyberattacks, especially those deliberately targeting civilians and the political legitimacy of governments—without the alliance having the capability to jointly discuss attribution and have the confidence to act and assist one another—undermines this core purpose of the alliance. Likewise, pursuing only deterrence and response without an active role for the alliance in reaching peaceful diplomatic agreements with potential adversaries abrogates member responsibilities to their citizens but is impossible without a common language and operational picture to discuss enforcement of such agreements. The U.S. is stronger with allies, and with attention to these issues its cybersecurity can be too.

#### NATO cooperation is key – cyber system resilience depends on coordinated information sharing. The plan spills up, and out, to include all allied networks.

Blessing ’21 (Dr. Jason Blessing is a Research Fellow at the American Enterprise Institute and a returning DAAD Postdoctoral Fellow at the Foreign Policy Institute of Johns. “Fail-Deadly, Fail-Safe, and Safe-to-Fail: The Strategic Necessity of Resilience in the Cyber Domain,” Chapter 12 in NATO 2030: Towards A New Strategic Concept and Beyond, SAIS Press, 2021, <https://www.sais.jhu.edu/sites/default/files/NATO2030AndBeyondAccessibleVersion.pdf)-mikee>

‘Safe-to-Fail’: Building Cyber Resilience into NATO The political and technical dynamics discussed in the previous section highlight the necessity of a safe-to-fail strategy for NATO in the cyber domain. Cyber resilience offers a way for the Alliance to address a range of threats below the threshold of armed conflict to which fail-deadly and fail-safe strategies fail to apply—such as ransomware attacks, distributed denials of service, exploitation of digital supply chains, or operations conducted by non-state proxy actors. Moreover, even low-sophistication cyberattacks can produce disruptive and cascading effects across societies with consequences that are difficult to anticipate. Resilience thus offers a broader strategic umbrella for the Alliance to plan for, recover from, and adapt in the wake of unanticipated disruptions from cyberspace. From a technical perspective, cyber resilience hinges on the ability of key information and communications systems to anticipate and withstand disruptions to service provision by allowing core services and functions to fail without compromising their ability to recover at or above original capacity.55 These same principles can be applied to the strategic level. As a safe-to-fail strategy, cyber resilience is premised on both the failure to deter and defend against all cyber threats and the failure to foresee all potential strategic disruptions. The goal of cyber resilience is thus to favorably shape the conditions of such failures by forecasting, preparing for, and learning from strategic shocks in or through the cyber domain that can have unanticipated, multiple-order, and spillover effects NATO already possesses the strategic foundation for pursuing greater cyber resilience and has recently reiterated its commitment to resilience writ large.56 At the 2016 Warsaw Summit, Allies agreed to seven baseline requirements for national resilience, one of which seeks to strengthen civil communications systems. This requirement was updated in November 2019 to reflect considerations for 5G.57 The Cyber Defense Pledge offers a more specific platform for linking national capability development to allied resilience. It emphasizes the need for greater resources, more domestic stakeholder interaction and information sharing, and better cyber hygiene and education.58 However, these initiatives have both been couched in the self-help principle of Article 3 of the North Atlantic Charter, whereby Allies work towards greater resilience “separately and jointly, by means of continuous and effective self-help and mutual aid.”59 As such, Allies pursue cyber resilience relatively independently. For example, the Cyber Section of NATO’s Emerging Security Challenges Division (ESCD) conducts a regular survey of all member states for the Cyber Defense Pledge, but national responses are voluntary and Allies must individually request information from previous surveys. Yet, fully incorporating safe-to-fail principles into the Alliance necessitates viewing resilience outside of the Article 3 context as a necessarily shared effort among member states. The limitations of collective defense discussed in this chapter highlight the potential for cyber operations to produce unanticipated, cross-boundary effects. Allied resiliency is inextricably interdependent—the digital interconnectedness of allied economic and defense efforts means that the vulnerabilities of one ally become vulnerabilities for all. Entanglement with the private sector is also an important confounding factor for members’ self-help efforts. NATO and its members will continue to rely on the private sector and civilian infrastructure for mission-critical systems and new technologies. The speed and spillover of disruptive cyber incidents like the WannaCry ransomware and the NotPetya wiperware-disguised-as-ransomware speak to the insufficiency of relying only on self-help measures to build cyber resilience.60 Resilience through selfhelp is therefore only part of the puzzle; safe-to-fail policies require more formalized coordination across NATO. Such efforts can leverage consultation mechanisms and processes derived from Article 4 of the North Atlantic Treaty,61 and Article 2 provides a powerful basis for members to coordinate with the private sector and deconflict economic policies underlying cyber resilience.62 This shared resilience must also be projected forward outside the bounds of the Alliance to NATO’s partners. The same cyber threat dynamics that make resilience a shared endeavor among members also highlight the importance of developments in partner and other third-party states (on partnerships, see Elgin and Wieslander in this volume). Unlike in traditional domains, NATO’s resilience and collective defense in the cyber domain are directly affected by the resiliency of non-members. Ukraine serves as a key example, as the country has been a testbed for Russian cyber operations with international implications. For instance, the BlackEnergy Trojan malware deployed against the Ukrainian power grid in 2015 was later found on US power grid networks.63 In the case of the 2017 cyberattacks on Ukraine, the NotPetya malware self-replicated and spread rapidly and destructively to over 150 countries using the Windows-based exploits.64 These incidents show the tenuous nature of cyber resilience and the need for the Alliance to aid partners in modernizing and building resilient digital infrastructures. Article 10 of the Treaty already lays the foundation for projecting resilience forward to aspiring members65 and can be used to set cyber resilience requirements alongside more traditional standards. Forward cyber resilience is in NATO’s best interests: the Alliance will be more resilient if its neighbors and partners are more resilient. Operationalizing shared and forward cyber resilience as a safe-to-fail strategy will require four main lines of effort.66 First, critical cyber assets, functions, personnel, and intersections and dependencies, must be identified and prioritized. Prioritization hinges on determining the relative exposure and significance of assets, how they may be targeted and attacked, and the areas where greater risks can be assumed. Second and related is risk minimization, particularly in terms of supply chains. One issue that has risen in prominence is the use of 5G infrastructures and networks. For instance, relying on non-allied suppliers of military or other vital communications infrastructures, such as Chinese companies Huawei and ZTE, can entail increased vulnerabilities for the Alliance.67 Other important aspects of risk minimization include continuous threat monitoring and the development of continuity-of-operations plans for cyber crises. Continuity plans are particularly crucial for ensuring that adversaries gain fewer and shorter-term payoffs from disruptions like ransomware attacks or sophisticated wiper worms that delete information. Third, foresight and long-term trend analysis are critical for cyber resilience, as strategic and technological change will further complicate an already complex operational environment. Threat actors will continue to develop new doctrines, institutions, and capabilities for the cyber domain. Emerging technologies, such as quantum computing, and the increased use of artificial intelligence will undoubtedly impact the scope, nature, and disruptive potential of cyber threats to the Alliance and its members.68 In this vein, NATO’s proposed establishment of a defense innovation accelerator is an important forward-looking development.69 Fourth, effective cyber resilience requires not only bouncing back to normal from disruptions, but also bounding forward via adaptation and the institutionalization of ‘lessons learned.’ Each of these lines of efforts will require institutionalized cooperation among member states and between NATO and its partner countries. Shared and forward cyber resilience complements collective defense by addressing a range of grey zone threats to which fail-deadly and fail-safe logics do not apply. At the same time, the safe-to-fail logic of resilience can strengthen the Alliance’s ability to carry out its other core tasks. Resilience makes collective defense more credible, as the continuity of critical functions and services are crucial for reducing the benefits of disruption for adversaries. For instance, implementing a safe-to-fail strategy helps to reduce the impact of defensive capability gaps between allies in the cyber domain. Resilience efforts also support collective defense by overlapping with deterrence-by-denial measures.70 Moreover, and particularly in terms of crisis management, cyber resilience can support efforts in traditional domains by ensuring that NATO and Allied land, sea, and air components dependent upon cyberspace can continue to operate with minimal disruption. Projecting cyber resilience forward to NATO’s partner countries also provides an avenue from which to strengthen the Alliance’s cooperative security engagements. Finally, the future-oriented and adaptive nature of resilience provides an important foundation for collective defense, crisis management, and cooperative security in the cyber domain to evolve with the emergence of new technologies and threats as the Alliance heads into the next decade and beyond.

#### Coordination and cooperation over intelligence solves unity and deterrence – US leadership is key.

Alina Polyakova and Mathieu Boulègue in 2021

President and CEO of the Center for European Policy Analysis (CEPA) as well as an adjunct professor of European studies at the Johns Hopkins University’s School of Advanced International Studies (SAIS) AND Senior Research Fellow, Russia and Eurasia Programme @ Chatham House; The Evolution of Russian Hybrid Warfare: Conclusion; https://cepa.org/the-evolution-of-hybrid-warfare-conclusion/

The United States should invest more capabilities and training in cybersecurity threat mitigation. Russia’s cyber capabilities have evolved to become increasingly sophisticated and far-reaching. The United States, and other Western allies, are not immune to cyberattacks — rather, Western countries are quickly becoming prime targets for Russian cyber operations. The 2020 SolarWinds hack, attributed to Russia, infiltrated more than 250 U.S. federal agencies as well as hundreds of U.S. companies.1¶ The 2018 U.S. cyber strategy opened the door for the United States to pursue offensive cyber capabilities.2 U.S. Cyber Command (USCYBERCOM) should fully explore and carefully deploy these capabilities to deter future cyberattacks by Russia.¶ In the longer term, the United States and Europe will need to work together to develop a cyber deterrence strategy vis-à-vis Russia and other state actors that seek to use cyber tools to attack critical infrastructure systems, steal sensitive national security data, and breach intellectual property rights. Such a strategy should set out clear parameters for engaging with adversarial states in the cyber domain, which should include an elaborate response framework that works to de-escalate confrontation between cyber superpowers.¶ COGNITIVE RESILIENCE¶ The fight against information manipulation — Russian or otherwise — starts at school and must continue through all demographics. It is of the utmost importance to offer future generations of information consumers the proper tools to decipher the informational environment. Comprehensive media literacy education is indispensable for a long-term defense against norm destabilization and disinformation. It provides a safety net as media practices evolve and should be woven into national curricula from an early stage.¶ In this regard, there are lessons that Western countries can learn from frontline states, such as Ukraine and Estonia, that have been targets of Russian information warfare for decades. Developing a critical lens for misleading or manipulative information as part of a broader civics education should be a priority in secondary education curricula.¶ 2. UNITY OF ENDEAVOR¶ REASSESS THE NATURE OF THE ‘RUSSIA CHALLENGE’¶ After the end of the Cold War and the West’s declaration of “victory” over the Soviet Union, Russia studies were quickly relegated to an unwanted dark art. Meanwhile, Russian military planners never stopped red teaming the West.¶ It is time to pay more attention to Russia studies. There is an urgent need for a better policy understanding of the evolution of Russian strategic thinking and its tactical applications. The U.S. government should increase support to public institutions, agencies, research centers, and think tanks working on Russia studies. This must be done by taking into consideration the diversity of national approaches to Russia, and the need to better coordinate expertise and policy in the United States and beyond.¶ Through more coordinated and calibrated policy, the goal should be to achieve a sense of unity in the West as regards the nature of the “Russia challenge.” This could be achieved in the United States through increased engagement with European partners, fostered by the Biden administration. While it may be hard to achieve a common understanding, greater policy coherence with Western partners should be pursued.¶ In parallel, it is vital that the new U.S. administration does not relegate Russia affairs to the back burner or deprioritize them. The “Russia challenge” is here to stay and should not be overlooked as a consequence of the overarching necessity to address all things China.¶ COOPERATION AND SUPPORT FOR ALLIES¶ The United States cannot push back against Russia alone. It should spearhead more comprehensive links with partners and allies in order to calibrate not only policies but also effects.¶ Sharing best practices is critical in that regard, alongside increased coordination and support in countries targeted by Russian hybrid warfare. This could take the form of increased intelligence sharing, return of experience, and lessons learned from successfully pushing back against Russian hybrid attacks, as well as specific cooperation programs between NATO allies — an effort the United States could lead.

#### Successful NATO cyber coordination restores faith in NATO’s credibility---that enables effective

Odgaard ’22 [Liselotte; April 25; Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich, co-founder and Director of the European Cyber Conflict Research Initiative (ECCRI.eu), an organization promoting the interdisciplinary study of cyber conflict and statecraft in Europe and beyond, also an Affiliate at Stanford University Center for International Security and Cooperation; Washington Quarterly, “NATO’s China Role: Defending Cyber and Outer Space,” 45:1]

Looking to the future, NATO’s success in establishing transatlantic mechanisms for cyber and outer space safeguards and consultation will be crucial to allow NATO a key role in taking on the China challenge in ways that help restore faith in NATO’s credibility as a provider of collective defense in all domains. It will also assist NATO in straddling the chasm between member states prioritizing threats from either China, Russia, the Middle East, or North Africa, since cyber and space threats potentially stem from all of them, and the effectiveness of cyber and space defense mechanisms do not necessarily depend on geographical origin. Cyber and space would allow NATO a key role in the China challenge without prioritizing China Improved communication between NATO and the EU will be essential for NATO to successfully address the military aspects of cyber and space threats. The framework for permanent EU-NATO relations, Berlin Plus, was concluded in March 2003. It allows for the exchange of classified information, the EU’s use of NATO assets and capabilities for EU-led crisis management operations, and the establishment of consultation arrangements.31 Due to disagreements over responsibilities and jurisdiction, however, meaningful coordination did not take place until July 2016. On this occasion, NATO and the EU issued a joint declaration stating their intention to work together on security and defense responses to unprecedented challenges emanating from the South and East of the Euro-Atlantic area.32 During Biden’s visit to Brussels in June 2021, NATO promised to strengthen cooperation with the EU on promoting peace and stability including protecting critical infrastructure, strengthening resilience, maintaining a technological edge, and addressing challenges to a rules-based order.33 The EU-US summit statement from the same visit merely reaffirms support for robust NATO-EU cooperation and promises to strengthen the partnership.34 At the level of policy implementation, it is clear when talking to NATO and EU officials that usually they do not coordinate their strategies and tactics for countering China challenges.35 The EU-US summit statement’s negligible mention of cooperation with NATO indicates that the ball is in NATO’s court if strengthening NATO-EU coordination is to take place. French and German concerns about entrapment are a major barrier to meaningful NATO-EU cooperation. The area of cyber and space security may allow NATO to work around this roadblock. In line with the EU’s practice of supporting the efforts of groups of member states to take the lead on issues where EU institutions cannot trump sovereignty, in the area of cybersecurity the EU has decentralized implementation to work around national resistance. This has allowed the EU to respond collectively and effectively to cyberattacks in Europe, primarily through bolstering capacities and law enforcement cooperation.36 However, the EU is not yet a globally influential and effective cyber-power because differences among member states over issues such as whether to prioritize tech sovereignty or Europe’s global tech competitiveness prevent the EU from acting in unison on the global stage. The first US-EU TTC meeting held in September 2021 was an important step in strengthening the EU’s global position in cooperation with the United States, and hence called into question whether NATO has a role to play in cyber security.37 The next couple of years will demonstrate whether the EU and the US are able to focus on becoming mutually supportive global cyber security guardians by cooperating on strengthening investment screening, export controls, and rebalance global supply chains in semiconductors. The successful implementation on both sides of the Atlantic of the recommendations of the TTC working groups will determine if transatlantic cooperation positions the US and the EU as global partners in guarding cyber space. In part, this will depend on the EU’s ability to forge common positions that meet the US halfway on issues such as tech sovereignty and data privacy, points of contention through which transatlantic relations have been marred by conflict. The potential convergence of transatlantic views on cybersecurity leaves room for NATO to play a significant role because the EU is a civilian and economic, rather than military, set of institutions. The NATO summit in Brussels in 2018 carved out a role for NATO which the EU cannot fulfill, allowing NATO members to integrate their sovereign cyber capabilities into NATO operations and missions.38 However, compared to the EU’s major role in cyber, NATO’s role is negligible. As EU civil-military cooperation ramps up in enhancing Europe’s autonomous defense profile while allowing US companies a role in this effort, the union looks set to become an even more dominant actor in transatlantic cyber defense. Because NATO is a military organization, it has the procedures and instruments to position itself in a key role in coordinating and implementing the military aspects of cyber defense between the US and Europe. The multinational cybersecurity effort which is confronting the global threat posed by Chinese state-sponsored cyberattacks involves NATO, the EU, Australia, New Zealand, and Japan, and sets NATO off to a good start in enhancing its profile in countering Chinese challenges to transatlantic cybersecurity.39 However, it remains to be seen if it manages to deliver mechanisms that succeed in integrating allied responses in the military sector in a way that complements US and EU cyber defense initiatives. In outer space, the EU is also increasingly active, recognizing the need to deepen investments in areas such as satellite navigation, earth observation, space situational awareness, and secure communications, which are all central to enhanced space security. The EU has established the EU Agency for the Space Programme, which has oversight over everything the EU does in orbit as a bloc. Moreover, the EU uses the European Space Agency (ESA) as technical advisor and industrial procurement agent. This setup allows the EU to become more agile, dynamic, and innovative in space as rapid industrialization is taking place with US entrepreneurs and well-funded Chinese space programs in leading roles.40 In the pipeline are a next generation of Europe’s satellite-navigation system, Galileo, and an extension of the scope and capabilities of its Copernicus-Sentinel spacecraft, which monitors the state of the planet. The EU focuses on ensuring that Europe has independent space capabilities, but it does not develop instruments such as space weapons systems.41 In the outer space realm, NATO has tremendous potential for playing a key role in developing instruments in the military sector that involve European and US space capabilities. NATO’s decision to declare outer space an operational domain at the London summit in 2019 is a first step in allowing NATO an active role in addressing growing anti-satellite threats from China and Russia.42 With the US as the leading power in outer space and with the EU developing its space platforms to enhance situational awareness and security, NATO has the tools to work out a common transatlantic definition of the anti-satellite challenges that need to be addressed. The establishment of mechanisms that ensure coordination across military NATO commands regarding intelligence gathering and the interface between cyber and space defense, as well as civilian and military occurrences and initiatives, would potentially strengthen the ability of allies to counter anti-satellite threats considerably. As with cyber, NATO must first integrate the space issue into all its organizational and operational structures, and secondly, develop mechanisms that focus on coordination between US and European capacities on the basis of a common understanding of the challenges to be addressed. NATO has the tools to work out a common transatlantic definition of anti-satellite challenges NATO’s Role in the Global Commons NATO can only be as effective as its member states allow it to be. NATO reflects the state of transatlantic relations: are US and European security outlooks sufficiently compatible such that the alliance is able to address threats from China collectively? This question is reflected in how well they manage to define common challenges and establish mechanisms that allow them to address these challenges together. NATO was a natural center of security focus for Washington when Europe was the main arena for US-Soviet deterrence. Today, the Indo-Pacific competes for US attention and resources as competition with China has moved to the center stage of US security and defense priorities. The strategic shift in US priorities does not mean that Europe cannot continue to remain a significant influence on global security dynamics. The EU has demonstrated its continued relevance in the security realm, not merely by relying on its role as a major trade bloc, but also by reforming the interplay between member states and EU institutions to avoid being paralyzed by consensus requirements, which apply in most areas outside the trade sector. This is done by providing platforms for member states to start initiatives. If successful in attracting support within the union, the initiatives are consolidated by supportive mechanisms and programs.43 NATO is not the EU and hence should not duplicate its methods. The EU is driven by the urge to secure the continued influence of its member states on major global issues. NATO’s raison d’être is to facilitate transatlantic cooperation in the military sector to counter common threats and challenges. Coordination is complex at a time when US and European security outlooks are drifting apart in terms of threat perceptions and priorities. At the same time, fears of entrapment stifle NATO’s efforts to update its relevance, principally because key members such as France and Germany are not interested in NATO taking on China as a threat. Nevertheless, NATO’s agreement to define China as a challenge promises opportunities for positioning the alliance in a key role in transatlantic relations. Because cyber and space encompass threats from other adversaries such as Russia and Iran, these domains are a good place to start taking on China as they do not require that China be singled out as a threat. By taking on the responsibility for coordinating US and European definitions of cyber and outer space threats in the military sector, integrating these domains in all organizational and operational NATO structures, devising mechanisms for the member states to address cyber and outer space threats, and by facilitating intelligence exchange and management of the vulnerabilities produced by civil-military interaction and overlapping interfaces between the cyber and space sectors, NATO can demonstrate its continued relevance for transatlantic security in an era where threats are increasingly global and transcend geographical boundaries. There’s no time like the present.

#### Expanding authority for security cooperation with NATO, specifically sharing intel and OCO capabilities, enables effective US cyberposture and restores NATO cohesion

Hansen ’21 [Dave and Morgan Musser; March 11; career US Army intelligence officer currently serving at the NATO Allied Rapid Reaction Corps, works in US Air Force Special Operations Command as an MC-130J pilot serving on Joint Special Operations Air Component; Foreign Area Senior Noncommissioned Officer serving as a regional planner in Stuttgart, Germany; The Civil Affairs Association, “The Rhetoric vs the Reality: Understanding NATO’s Capacity to Address Russian Gray-zone Conflict,” Eunomia Journal]

Despite these challenges, the NATO toolbox does include a variety of instruments, such as the imposition of sanctions. And while the Alliance has made clear it neither limits punishment to similar cyber-attacks nor excludes them, it keeps the option open to use the full range of Allied capabilities to deter and counter gray-zone actions. At the 2018 Brussels Summit, Allies expressed their determination “to employ the full range of capabilities, including cyber, to deter, defend against, and to counter the full spectrum of cyber threats, including those conducted as part of a hybrid campaign.”[33] Thus, NATO could retaliate in a proportional manner, but it does not necessarily have to do so by granting the authority to mirror Russian activity, especially considering Russia employs tactics that violate the norms of the liberal international order. Corruption, illicit finance, elections in­terference, debt traps, the restriction of free speech, spreading false narratives, territorial aggression, and ex­tra-legal operations are all areas NATO may rightfully choose to not engage. From a technical standpoint, should an adversary proliferate computer viruses to shut down power grids, countering with a cyber-attack may not stop/prevent the attacker’s imminent capacity to reengage. Despite an open-ended potential for graduated response options, NATO policy on gray-zone activities, particularly in cyber and information remain wholly constructed around a defensive posture. Unfortunately, defensive actions do not adequately address either the safeguarding of personal data that Russian or other malign actors might use in cyber-enabled information warfare or the economic incentives that drive users toward such behavior. Considering US cyber capacity, DoD’s stepped-up current posture of “persistent engagement” bodes well for active cyber defense.[34] However, questions remain as to whether it effectively enables operations to be deployed fast enough to address the ever-changing threat profiles and to manage escalation potential. Moreover, the approach requires the tight coupling of strategic ends—typically identified in an interagency policy process—and operational effects. It remains unclear if the current NATO collective defense strategy is able to deliver that coupling for US capabilities, which can create risks of unintended escalation or self-defeating effects not understood by well-meaning policymakers. Finally, significant gaps remain in intelligence and warning for cyber incidents across NATO, as well as normative frameworks to guide responsible use.[35] Some efforts to resolve gray-zone conflict remain in their infancy. For example, in 2016, Finland instituted the European Centre of Excellence for Countering Hybrid Threats in Helsinki with participation open to EU member states and NATO.[36] However, the Hybrid CoE provides only an analytical framework for the assessment of current and future hybrid warfare situations and their practical implication. The development of the Hybrid CoE is a model that could be applied in other regions for building capacity, and interoperability, and its existence is an important step forward for EU and NATO members to informally address vulnerabilities. However, this effort holds no authority or capacity to engage a response. Holistically, despite a number of declarations, increased force presence in Eastern Europe, and newly formed information-sharing centers, NATO’s actions remain pursuant to conventional forms of military deterrence or research. None specifically counter gray-zone activity or prevent Russia from targeting weaker nations. From a military deterrence standpoint, there clearly appears to be a functional mismatch between NATO’s traditional hard deterrence and the hybrid actions it wishes to remedy. Integrating multiple elements of national security remains unaddressed. Authorities One of the key challenges often plaguing US and NATO response to gray-zone conflict is “authorities.” This problem is two-fold. The first are the challenges internal to the US regarding perceived inadequate or dispersed authorities to effectuate coherent activity. The second are insufficient authorities inside the NATO Alliance – partly a function of the political bureaucracy within NATO itself, arguably slow to elicit timely and relevant responses. Much of the literature on countering gray-zone activity recognizes the need for an interdependent system.[37] Critics have additionally pointed to several issues which include the lack of a holistic methodology for dealing with Russia’s gray-zone behavior.[38] But without a formalized methodology for defining and assigning policy priorities and actions, effective long-term strategies for deterring, competing against, and responding to competitors’ use of state-controlled forces will likely be limited. Limitations precluding a real-time, multi-agency approach to address adversarial actions are especially salient in the information and cyber domains. Within the US government, responsibilities and authorities are spread across numerous entities, to include DoD, DoS, and Treasury. There is no unity of effort and no specific organization has lead for synchronizing the employment of all instruments of national power.[39] Within DoD, most of the capabilities reside inside the force structure of geographic and functional combatant commands (CCMD) and are tasked through unified combatant command (COCOM) au­thority. Authorities quickly cut across both functional and geographic lines. This may slow defining roles and responsibilities. Also, several offensive capabilities are either compartmentalized due to the technology behind them or, considering their effect, may yield undesirable strategic impact. Therefore, authorities for their use – specifically in the information and cyber domains are often retained at the SECDEFs level (or above). This can dramatically impact the speed of response. To fix this, some authorities (and associated risk acceptance) might be delegated down to Ambassador level, such that in a steady-state environment, permission might be granted to create effects in the information environment, while retaining country-team level and multi-agency awareness. Additional challenges with authority are a result of ambiguity in US law. Both Title 10 and Title 22 authorities grant DoD and DoS authorities to support, train, and partner with forces, with legal checks and controls on human rights and ac­countability measures. However, there is no clear de­lineation over whether building/countering US local partners should be under Title 10 or Title 50 (Central Intelligence Agency) authorities. As a result, the question of who owns long-term proxy strategy and operational development remains unanswered in the US interagency.[40] This “authorities dilemma” is even more convoluted within the NATO alliance. The United States’ aspirational model for countering Russia’s gray-zone activity via whole-of-government approach, is not well-suited for a multinational security-based alliance. Opportunities and Recommendations There are several observably difficult challenges in how the US and NATO approach gray-zone competition, as a military, as individual nations, and as Allies. Such challenges do come with opportunities. The Department of Defense cannot abruptly restructure itself to engage in all gray-zone activities, nor should it necessarily want to. What the Alliance does have however, includes asymmetric advantages of transparency through its rule of law. The system of alliances and partners can work to extend democratic principles, acknowledge humanitarian concerns, prevent violent conflict, identify and stymie political and economic ex­ploitation, and support free and fair media outlets.[41] Thus, developing methods that directly compete in the gray-zone can exist outside the development of like-capabilities. Likewise, NATO cannot immediately establish a multi-agency organization, built to compete across a spectrum of gray-zone activities, empowered to lead, synchronize, and coordinate diverse capabilities across the conflict continuum.[42] Authorities still must be reconfigured down and across to appropriate levels to enable proportionality, when directed. The good news for US DoD is that it may not have to embark on a complicated restructuring in order to counter Russia’s malign actions. DoD’s current approach places war-fighting authorities under CCMDs. There are certainly numerous challenges in synchronizing prior­ities, resources, and actions to leverage a broad toolset and eliminate the stovepipes. Indeed, specific capabilities such as information warfare, or offensive cyber, are neither geographically nor functionally lim­ited.[43] Yet while true, just because some gray-zone actions cross geographical and functional lines, this does not inherently mean the response is hindered. While broad oversight may be an enabler, lack of it is not an inhibitor and it does not mean that a Combatant Command is disabled. In fact, Russia’s activities are often geographically focused — making them ripe for inclusion into CCMD Campaign Plans. Under the current structure, the geographic Combatant Commands are arguably best postured to compete against Russia’s gray-zone activities, taking full advantage of supporting the coordinated activities of USCYBERCOM as well as the expertise of US SOCOM. Specific authorities could be granted now for implementation by US forces in support of NATO objectives to reduce Russia’s information position, as well as granting authorities for the leveraging of the information environment to the benefit of both US and NATO strategic interests. While a US whole-of-government approach with a singular lead organization is a lofty ideal, this is simply not practical in the short term. There are actions that can be taken to establish a unified purpose, and to ensure that reform priorities for competing in the gray-zone are formed around making the most of available US strengths by mitigating current gaps in the ability to execute national interest-based strategy via campaign plans. If NATO is to deal effectively with such competition, then it too must refocus its own military strategy and forces to give gray-zone and hybrid conflicts at least equal standing with traditional deterrence. At present, NATO has only recognized cyberspace as a domain of operations since 2016. While an important first step in combating gray-zone activities in the information domain, the information centers standing up are limited to situational awareness, along with some planning and coordination tools.[44]The Alliance has yet to refocus its security strategy to address the impact of gray-zone activity across global, regional, and national levels. Delegated authorities and packaged measures will need to be tailored and based on a better understanding of the strategic intent behind the use of gray-zone tools. This can help the military better engage in the debate and develop capabilities to support Allies in countering non-military threats, such as using special operations, information, and psychological operations. A focused approach with delegated authority would vastly improve NATO’s efficiency in influencing the cost-benefit analysis of potential aggressors in what has now become the modern theatre of operations. In short, if opponents increasingly act in the gray area, NATO must be efficiently enabled to defend, attribute, and respond. The initial structure is in place, but the operationalization of strategy and authority for appropriate comprehensive tools lags. Defeating Russia’s sophisticated strategy requires strategic competence and a concerted effort to restore confidence in democratic principles, institutions, and processes, along with remediating the vulnerabilities Russia exploits. To compete properly, NATO must articulate clear guidance for its threshold warfare deterrence posture, with options that realistically allow forces to respond to Russian gray-zone behavior. Management of these threats must be an ongoing endeavor, requiring a change in mindset from the deliberate sequential planning processes associated with classic forms of conflict to a more dynamic approach of continuously updated situational awareness, driving political discussion, option development, decision-making, and measured response under political control. To do this effectively, NATO will have to progress from crisis-response operations to reinvigorate both its military strategy and forces and ensure gray-zone and hybrid conflicts are prioritized along with higher levels of warfare. This may include refocusing its current security strategy to address the overall impact of Russian civil competition at all levels by fully integrating its military, political, and economic strategies and operations. How much of (and when) technological capacity should be delegated down must ultimately be considered and reviewed, along with how NATO integrates response capabilities into the multi-national environment. These gaps must be bridged to enable multinational teaming. Without them, NATO’s plans for deterrence, defense, and dialogue run the risk of becoming reactive, or even outmaneuvered. Many gray-zone operations will not require the actual use of military force. Some will be entirely civil or economic – using non-military means to achieve strategic or tactical objectives. This will inevitably require ‘whole-of-government’ capacity within NATO structures in a way that NATO is presently not organized or enabled to perform. If NATO members agree that the trend of cyberspace is the most active battlefield, then it is crucial the Alliance has a threat preparation and mitigation plan that is continuously monitored, assessed, and adjusted, with deterrence mechanisms built-in. Presently they are not. The significance to NATO is clear. NATO must overhaul its deterrence strategy, to include options far more nuanced than tactical overmatch, by re-evaluating the role of its military as a deterrent, through increased sub-Article 5 capacities. This might even include support from the private sector and international organizations, with emphasis on a comprehensive approach. Conclusion Since its inception, NATO has been more than just a military alliance. It has embraced a political role, unifying Allies behind a common strategic vision. Future uncertainties demand NATO must continue to adapt. Given the significant changes in the security environment since Russia’s incursion into Georgia and Crimea, this presents an opportunity to determine the character of the Alliance’s military capabilities vis-à-vis gray-zone warfare. Future decades will certainly be different than the world the Alliance inhabited during the Cold War. NATO’s cohesion resides in the ability and will to act collectively against shared threats. This is the lifeblood that ensures the vitality, credibility, and durability of NATO. It becomes increasingly important in a sharpened competitive environment requiring collaboration and effective networks. Therefore, the distinctive capabilities required to counter gray-zone warfare must be seriously contemplated.

## Cyber War Advantage Extensions

### NATO Vulnerable Now

#### NATO is at risk for cyber-attacks- autonomous devices vulnerable and easy to manipulate

Jacopo Bellasio 2020, Senior Analyst Defence Security and Infrastructure RAND Europe; The Impact of New and Emerging Technologies on the Cyber Threat Landscape and Their Implications for NATO; Nato Coropative Cyber Defense Centre of Excellence; https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030\_Horizon-Scanning-and-Analysis.pdf

Autonomous devices and systems are platforms and devices that can achieve their goals independently and require little or external control and supervision. They combine intelligent software which, thanks to AI-enabled autonomy, conducts or assists with decision-making via hardware devices which interact with the system’s surroundings and the physical world to collect data and undertake tasks (Scharre, 2018; Vallor and Bekey, 2017). 92 Autonomous systems can vary in size, hardware and level of autonomy. The level of autonomy is typically classified according to the expected ‘meaningful human control’, which is a metric reflecting the extent to which humans are required to intervene in a system’s interactions with the real world (Scharre, 2018; Fong, 2019; Leikas et al., 2019). A wide array of autonomous systems with direct relevance to security and defence have been developed in recent years, including autonomous unmanned vehicles, unmanned weapons systems and smart medical devices. Further advances in this field are expected to stem from developments in swarming technologies2 and of more sophisticated autonomous systems, including for autonomous weapons. These advances are expected to reduce reliance on humans for decision-making or operational control, thus opening vulnerabilities for the possible disruption and manipulation of autonomous systems. From a cyber threat perspective, the proliferation of autonomous systems and devices is expected to increase the attack surface available to adversaries and malicious actors (Bogan & Feeney, 2020). For example, autonomous weapons systems that include a tether, enabling the remote control of a system from a supplying country wishing to ensure compliance of the use of its systems with international humanitarian law, could result in the embedding of back doors and kill switches limiting the value of autonomous system assets and potentially making them vulnerable to disruption or manipulation by other third parties (Kajander et al., 2020). Similarly, the use of autonomous vehicles for logistics could be targeted by adversaries leveraging cyber vulnerabilities or adversarial AI to disrupt the logistics and supply chains of a military operation (Danks, 2020; Bogan & Feeney, 2020).

#### NATO is high for cyber stacks- changing to computing power that are easily manipulated

Jacopo Bellasio 2020, Senior Analyst Defence Security and Infrastructure RAND Europe; The Impact of New and Emerging Technologies on the Cyber Threat Landscape and Their Implications for NATO; Nato Coropative Cyber Defense Centre of Excellence; https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030\_Horizon-Scanning-and-Analysis.pdf

Computing power and data storage technologies are fundamental enablers of ICT systems. Along with sensors, these technologies allow the capture, manipulation and storage of data. Advances in these fields have led to the development of sophisticated capabilities able to record, store and manipulate expanding datasets at increasing speed. Over the next few years, advances for computing technologies are expected to lead to increasing miniaturisation and greater power, enabling a variety of new solutions such as miniaturised supercomputers, semiconductors and microprocessors like ‘smart dust’ (Shaikh et al., 2016; Beijing Innovation Centre for Future Chips, 2018). With regard to data storage, in addition to the development of high-density low-energy consumption data storage solutions, it is expected that the future will see a continuation of the growing use and reliance of cloud storage technologies, enabling ubiquitous, on-demand access to data through remote servers (Hess et al., 2019). These trends and their effects are expected to be further reinforced by advances 2 The development of advanced collective behaviour mechanisms that enable two or more autonomous systems to operate collectively. 93 in the fields of sensors. Sensors are used on IT-enabled systems to acquire data to contribute to the performing of different tasks, including decisionmaking and the tracking and monitoring of a variety of different phenomena. Advances in sensors are expected to result in improved performance and accuracy, further miniaturisation3 and improved ability to record or generate new types of data. From a defence standpoint, modern platforms and systems have already witnessed the embedding of an increasing number and type of networked sensors which monitor and support their performance. In the coming decade, sensors could also see a growing integration at the level of individual soldiers or systems to improve communications, situational awareness and enable more robust decision-making at different levels through data fusion and analysis (Kepe et al., 2018). These trends are expected to be further reinforced thanks to advances in telecommunications infrastructure. Telecommunications technologies comprise all the physical and digital infrastructure that enables information to flow across the internet and between devices and systems. The global telecommunication infrastructure is expected to continue evolving rapidly and already encompasses a wide range of technologies including Wi-Fi, optical fibre, light-fidelity and fifth-generation mobile networks (5G) (Deloitte, 2017; ENISA, 2019). Advances in telecommunications technologies in the next years are expected to increase bandwidth, decrease latency and increase spectral efficiency, leading to greater connectivity and a more digitalised world. The coming decade is likely to see a continuation of the shift from offline to online, with more devices, systems and services becoming digital and connected, including in critical infrastructure sectors (Bogan & Feeney, 2020). **This will extend to military platforms and activities, providing for a greater impact of cyber threats beyond the cyber domain to traditional military domains of operations and the day-to-day functioning of military institutions** (Kepe et al., 2018). Sensors, computing, data storage and telecommunications technology are therefore expected to play a key enabling role for trends and challenges discussed in Section Three of this chapter.

#### NATO’s cyber security is at risk-reliance on networks can be damaged by a range of people

A. Ertan et al 2020, a cybersecurity researcher and PhD candidate at Royal Holloway, University of London, K. Floyd is the Director of William & Mary’s Whole of Government Center of Excellence, P. Pernik a Researcher of the Strategy Branch of the NATO CCDCOE, T. Stevens Senior Lecturer in the Department of War Studies, CCDCOE; <https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf>

All members of NATO benefit greatly from digital connectivity and the many¶ opportunities it provides for social, economic and political development. At¶ the same time, **it is widely recognised that heightened dependency on digital**¶ **networks** and systems **is a systemic vulnerability that can be exploited by a**¶ **wide range of** criminal and strategic **actors**. The community of like-minded democracies gathered under the NATO umbrella is therefore being challenged as never before by diverse and dynamic cyber threats. This volume¶ looks ahead to how NATO can best address these issues over the next decade,¶ contributing to the conversation begun by Secretary General Jens Stoltenberg¶ in June 2020. In launching the NATO 2030 initiative, the Secretary General¶ canvassed input from a wide range of stakeholders about how to strengthen¶ NATO militarily and politically in a turbulent and competitive world (Stoltenberg, 2020; NATO Science and Technology Organization, 2020). This¶ volume engages directly with that discussion and aims to stimulate broader¶ debate on the future operational environment from the perspective of cyber¶ threat horizon-scanning and analysis, with particular attention to the impact of new and emerging technologies.¶ In the period under consideration, NATO’s technological edge will be increasingly challenged. Recent work by **NATO has highlighted the wide range**¶ **of emerging and disruptive technologies which may negatively impact international security** **and stability** and the ability to promote democratic norms¶ (NATO Science and Technology Organization, 2020). In May 2019, the Secretary General warned that new technologies such as artificial intelligence and¶ machine learning will render cyber threats even more pernicious, as well as¶ potentially altering the nature of warfare (Stoltenberg, 2019). NATO is fortunate to be already deeply invested in addressing these issues. The Cyber Defence Pledge (2016), for instance, exists in part ‘to ensure the Alliance keeps¶ pace with the fast-evolving cyber threat landscape’ and reasserts a collective¶ will to tackle cyber threats extending as far back as the 1990s (NATO, 2016;¶ Burton, 2015). This includes successive Strategic Concepts recognising the¶ critical importance of cybersecurity to NATO’s missions and military operations. Since 2016, NATO has bolstered its existing outreach and engagement¶ programmes and embarked upon new ones, all geared to improving its cybersecurity and that of its member states.¶ As recognised by NATO, however, more work is required to understand the¶ evolution of the cyber threat environment. This was emphasised in the Strategic Foresight Analysis of NATO Allied Command Transformation, which¶ encouraged NATO to ‘develop capacities to detect both subtle and seismic¶ changes in the information environment and understand them on local, operational and global levels’ (NATO Allied Command Transformation, 2017:¶ p. 51). The Cyber Defence Pledge itself aims to ‘improve our understanding of cyber threats, including the sharing of information and assessment’¶ (NATO, 2016). In this context, Alliance political and strategic leaders need¶ to improve their understanding of cyber threat vectors; actors’ objectives, ¶ intent and capabilities; and the future cyberspace operational environment¶ across all phases and contexts. This includes peacetime conditions, targeted cyberspace operations with disruptive or even lethal impacts, and kinetic¶ warfighting in conjunction with destructive cyber attacks. In addition, cyber threat intelligence (CTI) must be comprehensible and operationalised to¶ support strategic-political decision-making.

#### Current NATO efforts insufficient – Lack of modernization efforts hinders NATO ability to respond to emerging fronts

Cordesman and Hwang 2/16/22

Anthony H. Cordesman is the Emeritus Chair in Strategy at the Center for Strategic and International Studies (CSIS). He has previously served in the Office of the Secretary of Defense, the National Security Council, the State Department, and the Department of Energy. Grace M. Hwang holds Ph.D. & M.S. degrees in Biophysics and Structural Biology from Brandeis University. Her doctoral dissertation was on computational neuroscience where she specialized in analyzing cohorts of human brainwaves to understand the neural basis of visual and verbal memory formation. She developed novel nonparametric statistical techniques for high-dimensional data that enabled robust across- and within-subject multi-factorial analysis. NATO and Ukraine: Reshaping NATO to Meet the Russian and Chinese Challenge, CSIS, <https://csis-websiteprod.s3.amazonaws.com/s3fspublic/publication/220216_Cordesman_NATO_Ukraine.pdf?cS8vKRNOdoYvg3t_y6QMZMSCpadAo90a>

At the same time, the U.S. has also maintained good reason to be concerned about the defense efforts of most European powers, and there is a need for the U.S. to pressure given NATO European states to increase the key aspects of their defense efforts that really matter. As the country-by-country analysis later in this report also shows, many European states have fallen short Put simply, the U.S. needs to recognize that **NATO needs to be fixed** – rather than broken – and Europe needs to recognize that there are no real European alternatives to Atlantic deterrence and defense. It shows that the U.S. and each of its NATO European allies need to focus on making the alliance more effective. They need to cooperate far more in shaping NATO’s real-world strategy and on actual levels of **meaningful modernization** and cooperation. Moreover, they need to focus on nation-by-nation improvements in the common capability to deter, defend, and cooperate, rather than on burden-sharing, setting arbitrary spending goals, and substituting good intentions for action. NATO needs new realities, not more rhetoric. Every nation in the alliance needs to do more to actually implement the strategic and force modernization goals set out in NATO’s 2030 plan and to deal with what NATO calls “emerging and disruptive technologies.”5 The plan shows that the creation of a well-balanced, integrated, and interoperable mix of national forces for NATO should be a common U.S., European, and Canadian objective. At the same time, the summary analysis of individual member country’s forces in this analysis shows that such efforts need to address the military strengths and weaknesses of each member state in very different ways. The NATO alliance needs a far more nuanced country-by-country approach to force planning based on a real net assessment, plans, and budgets. Moreover, the conclusion to this analysis shows that NATO needs to actively review the changing capabilities of the world’s three superpowers and to consult on the rising threat from China, rather than just focusing on Russia, terrorism, and the out of area threats near Europe.

#### NATO needs to recognize its vulnerabilities – Modernization in cyberspace needed to ward off Russia

Cordesman and Hwang 2/16/22

Anthony H. Cordesman is the Emeritus Chair in Strategy at the Center for Strategic and International Studies (CSIS). He has previously served in the Office of the Secretary of Defense, the National Security Council, the State Department, and the Department of Energy. Grace M. Hwang holds Ph.D. & M.S. degrees in Biophysics and Structural Biology from Brandeis University. Her doctoral dissertation was on computational neuroscience where she specialized in analyzing cohorts of human brainwaves to understand the neural basis of visual and verbal memory formation. She developed novel nonparametric statistical techniques for high-dimensional data that enabled robust across- and within-subject multi-factorial analysis. NATO and Ukraine: Reshaping NATO to Meet the Russian and Chinese Challenge, CSIS, <https://csis-websiteprod.s3.amazonaws.com/s3fspublic/publication/220216_Cordesman_NATO_Ukraine.pdf?cS8vKRNOdoYvg3t_y6QMZMSCpadAo90a>

NATO must develop clear NATO Priorities and National Force Plans that Address the Major Changes Taking Place in Military Dynamics and in Emerging and Disruptive Technologies (EDTs) The key to dealing with these issues is to go back to the NATO force planning efforts from the past that attempted to address member countries’ force plans on a country-by-country basis and attempted to develop both interoperability and goals for sustainability, training and readiness, and modernization. Some lessons here are obvious. Such efforts require annual updates, but they must look some five years into the future as to plans, program, and budgets to develop credible continuity and planning efforts. The U.S Future Years Defense Program (FYDP) and the European five-year plans need to be properly implemented, and these plans must focus on the full range of military capabilities instead of simply fixating on major force numbers and weapons platforms. What is less obvious is the need is to focus on a future with very different military dynamics in an era of massive technological change. NATO has begun to address some of these issues, but they need to take into consideration both national force planning as well as the reality that smaller nations and forces will often need to depend heavily on the large powers and those with the most advanced technological base. NATO cannot succeed here by asking every nation to make the same effort in its spending burden. The alliance must deal with national, political, and economic realities. It also faces extremely complex challenges in the form of what is almost certainly going to be an ongoing revolution in military affairs. There are issues too complex to deal with in this analysis in any depth, but the following figures illustrate the sheer level of change and its complexity. Figure Nine provides a brief summary of the new military dynamics NATO must adjust to over the coming decade. Figure Ten shows a NATO-created list of the emerging and disruptive technologies (EDTs) that the alliance as well as each member country must adjust to in shaping its future force plans. Figure Eleven shows a matching list issued by the U.S. Department of Defense of EDTs, and one that lists clearer force planning and modernization priorities. They make it all too clear that member states must develop a common approach to modernization and joint all-domain warfare. Interoperability and standardization have always been a clear alliance priority, but the challenge is now far greater than in the past. To provide advantage for the joint force in highly contested environments, the Department must develop wideband sensors to operate at the intersection of cyber space, electronic warfare, radar, and communications. Sensors must be able to counter advanced threats and can no longer be stove-piped and single function. There is no easy way to illustrate the scale of the changes in the military balance between the three current superpowers since many are qualitative rather than quantitative. Figure Twelve illustrates the quantitative changes in some detail. It shows just how much smaller U.S., Russian, and Chinese force numbers are today in many such metrics and that their current forces bear only a limited resemblance to the forces they deployed in 1991. At the same time, the previous analysis has shown that the qualitative improvements in Russian forces mean that cuts in force numbers in Figure Twelve do not mean cuts in Russian capability to threaten, pressure, or fight in a Europe where NATO countries have made – at the very least – equal reductions in their force numbers. Moreover, Figure Twelve shows that the U.S. made major force cuts after 1991, matching those of its European partners Russia relied heavily on military mass until the break-up of the FSU, but it has steadily improved its force quality in many areas like air and missile defense since 1991. It has remained competitive in conventional weapons modernization, and it has aggressively modernized it nuclear forces. It has shown its ability to compete in gray area warfare in Libya and Ukraine, created new forward capabilities in Syria, and returned to the Mediterranean – as well as steadily improved its cooperation with China in Asia and the Pacific. Russia may have lost military and economic strength because of the break-up of the FSU and the liberation of East European states – many of which have joined NATO. Yet, many of these former Warsaw Pact states have failed to modernize their forces and make them more interoperable with NATO. The fact that the expansion of NATO has fundamentally changed the strategic map of Europe **does not mean** that most of the states that have joined NATO since the break-up of the FSU do not depend on the U.S. and other European states for deterrence and defense. As this analysis has shown, rhetoric about European defense cooperation cannot ignore the critical new vulnerabilities in NATO’s new forward areas. Russia remains a major and growing threat.

#### NATO interoperability is lacking --- Russia’s invasion of Ukraine highlights this.

Mikayla Easley 3/9/2022; Staff Writer; WEB EXCLUSIVE: Ukraine Invasion Prompts Plea from French Official to Speed Up NATO Tech Integration; NDIA’s Business & Technology Magazine; https://www.nationaldefensemagazine.org/articles/2022/3/9/nato-must-prioritize-system-interoperability-french-defense-official-says

NATO officials for years have been preaching the need for interoperability among member nations’ weapon systems. France’s top defense official said in light of Russia’s war against Ukraine, it isn’t happening fast enough. French Chief of Defense Gen. Thierry Burkhard March 8 said: “The systems that are deployed within NATO countries have to be compatible with the other systems in use within NATO, so we need to make sure they are compatible [and] interoperable in massive ways,” he said. “I think we’re not making progress in the right direction in that field.” Russia’s invasion of Ukraine highlights the need to speed up NATO interoperability, he said. The ability for weapons and other military systems to communicate and share information among NATO allies is one of the most important aspects for the alliance’s success in future fights, Burkhard said during a fireside chat hosted by the Center for New American Security. Collective interoperability is not currently the standard, he noted. For example, Burkhard has witnessed communication issues with the increased deployment of the F-35 joint strike fighter into various NATO ally’s air forces. “The F-35 is designed as a very effective and efficient system,” he said. “It has great qualities, but its design is a very closed system and I think this is a mistake.” NATO militaries must play a decisive role in ensuring network interoperability standards across the alliance, he added. France is also working to improve interoperability within its own armed forces in an effort similar to the U.S. Defense Department’s joint all-domain command and control, or JADC2, which aims to link sensors and shooters at the tactical edge. France’s internal campaign to achieve interoperability is part of its Scorpion program, which “aims at digitalizing all land forces in order to be able to extend information very quickly and also improve [our] operational pace in order to be able to impose our will on opponents,” he said. A document — Burkhard’s Strategic Vision for 2030 — is not unlike modernization plans made by the United States and the United Kingdom to move away from operations against nonstate actors and prepare for potential conflict with adversaries such as China and Russia. An exception the U.S. and U.K. militaries’ desires to shrink the size of its land forces. France will be focusing its attention on upgrading its Army by the year 2030, he noted. This includes the development of two new ground vehicles for the French army to replace the service’s aging vehicles and systems: the Griffon, a multi-role armored vehicle, and the Jaguar, an armored reconnaissance and combat vehicle. Burkhard said the ability of these vehicles and other new capabilities to connect and share information across domains is “the true driver” for success. Russia’s operations — which have not gone to Moscow’s plans — signal the true amounts of effort required for high-intensity operations. “It doesn’t mean that we are not able right now ready to engage in a high-intensity conflict, but not with all the assets that were identified or the level of training we [expected] to reach by 2030,” he said. “The situation today shows us that we need to speed up the process — but let us not lie to ourselves … that’s what the invasion of Ukraine by the Russian army is showing negatively. This is something that requires a lot of effort and a lot of time,” he said.

#### European energy infrastructure is vulnerable now and Russia will target it- increasing cybersecurity is key

Alejandro Romero, Jonathan Nelson, 3-7-2022, "Why Europe’s energy industry is vulnerable to cyber-attacks," ECFR, https://ecfr.eu/article/why-europes-energy-industry-is-vulnerable-to-cyber-attacks/

**Russia’s war on Ukraine has created widespread concern that European energy supplies and infrastructure will come under intensifying cyber-attacks. The Putin regime,** which has long used such disruptive tactics, **may retaliate against Western economic sanctions with cyber-warfare**. European states and energy companies should reflect on the laundry list of such attacks that have occurred in recent years to recognise and respond to the risks they face in this area.¶ On 7 May 2021, the US Colonial Pipeline suffered a critical ransomware cyber-attack [resulting from a single leaked password](https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/) – the largest cyber-attack on infrastructure in US history. This prompted the authorities to declare a state of emergency in 17 US states along the east coast and in Washington, and resulted in major fuel shortages and long queues at gas stations throughout affected sectors. By early February 2022, a slew of subsequent [cyber-attacks](https://www.bbc.com/news/technology-60250956) had struck oil and gas facilities across Europe, disrupting the operations of multiple oil transport and storage companies in Germany, Belgium, and the Netherlands, and threatening production and distribution in the sector.¶ Such attacks are possible due to three unique vulnerabilities of the global energy ecosystem.¶ Firstly, this ecosystem relies on inherently complex infrastructure. Utility companies are exposed to relatively high risks because their networks of both physical infrastructure and cyber-infrastructure – including distributors, suppliers, storage facilities, and other assets – often overlap and are spread across many countries.¶ Secondly, the digital infrastructure that supports the global energy sector operates around the clock, with virtually no downtime.¶ Thirdly, the vulnerability of the global energy sector is rooted in the many motivations for attacks against it. As noted in a recent assessment by the [Canadian Centre for Cyber Security](https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-canadas-electricity-sector), these include attacks carried out by states trying to achieve geopolitical goals, by criminals attempting to extort money from desperate companies, and by activists seeking to publicise their agendas or oppose particular projects.¶ **Therefore, given the frequency with which these structures come under attack and how vital they are to the economy, the energy sector is a key geopolitical battleground.** The vulnerabilities of Europe’s digital security and global energy interconnections could have a significant impact on citizens’ lives. The World Economic Forum [highlighted](https://www.weforum.org/whitepapers/cyber-resilience-in-the-oil-and-gas-industry-playbook-for-boards-and-corporate-officers) this in 2021, arguing that: “as one of the world’s most sophisticated and complex industries makes a multifaceted transition – from analogue to digital, from centralized to distributed and from fossil-based to low-carbon – managing cyber risk and preventing cyberthreats are quickly becoming critical to company value chains.”¶ The pandemic accelerated the digitisation of the European economy and prompted a rapid shift to distributed, hybrid working practices. The process has dramatically expanded opportunities to attack critical energy infrastructure. The Putin regime’s war on Ukraine is one of many conflicts to [involve](https://apnews.com/article/russia-ukraine-technology-business-europe-russia-e791990f60841b599f664c34f58403de) hybrid operations that include targeted cyber-attacks on critical infrastructure in areas such as banking and internet services – as was particulary clear during the surge in attacks on the country that occurred in early 2022.¶ The attack on the Colonial Pipeline showed how various actors could exploit a single compromised password to severely disrupt the energy infrastructure of the United States for several days. How was this possible?¶ A [recent report](https://info.constellaintelligence.com/energy-sector-exposure-report-2021) by Constella Intelligence revealed just how much sensitive personal information tied to corporate credentials is in circulation. In the last few years, millions of records of sensitive personal and employee data linked to the 20 largest global energy companies (by revenue) have circulated online. Moreover, these risks reach the senior level: nearly half of the executives of these companies were found to have suffered exposure of their data in recent years. Each of these data breaches could create additional vulnerabilities that various actors can exploit.¶ Corporate and geopolitical risks are highly contingent on the integrity and security of inidividuals’ data. Public and private security protocols are among the most effective tools to improve such integrity and security. However, in a rapidly evolving digital sphere, it is difficult to create legislation suited to protect private companies, public organisations, and individual citizens. The **European Union’s push for cyber-resilience has been deliberate and diligent. Yet the evolution of threats in the digital ecosystem could outpace the EU’s attempts to implement cyber-security measures across all its member states.**

### Cyber Risk High Now

#### NATO must boost cybersecurity - Risks of cyberattacks on NATO high now

Lete & Dege 17 [Bruno & Daiga; 2017; senior fellow or security and defense policy in GMF’s security office; trainee in office, “NATO cybersecurity: a roadmap to resilience, <https://www.gmfus.org/sites/default/files/NATO%2520Cybersecurity_edited.pdf>]

Cybersecurity has become as crucial as conventional security, thereby shifting the realm of the security environment. Rogue actors have boosted their capabilities, and the costs of such resources owned by attackers are threatening security on both sides of the Atlantic. NATO must put forward recommendations and implement the securitization agenda in order to create an interconnected approach within different sectors. NATO will need to continue building the forcemultiplying functions of its cyber capabilities, improve effective command and decision-making structures in cyber crisis and conflicts, and enhance the interoperability between allies and partners in cyberspace. The security challenges of today require quick responses, necessitating flexible policy frameworks that allow for coercive reactions from networked actors. Cybersecurity has long been part of Alliance calculus but only recently came at earnest to the forefront of its agenda. The 2007 cyber-attacks in Estonia forced NATO to think more seriously about this type of threat, and in 2008 NATO developed its very first policy on cyber defense. The cyber-attacks fuelling the crisis in Ukraine’s Crimea and Donbass regions served as a definitive wake-up call. At its 2014 Wales Summit, NATO effectively created a mind-set of urgency, featuring cybersecurity prominently on top of the meeting’s political agenda. Allies endorsed a new cyber defense policy in Wales and approved a new action plan in line with the evolving cyber threat. Thinking more creatively about the implementation of collective security in the digital context on top of the agenda for NATO. NATO made more significant steps in cybersecurity at the 2016 Summit in Poland. In Warsaw, Allies decided to operationalize cyberspace as a domain of NATO defense policy and planning efforts, in addition to land, sea, and air. An important product of the Warsaw Summit was the so-called NATO Cyber Defense Pledge through which member states committed to prioritize the strengthening the cyber defense of national networks and infrastructures. Most member states have created national cyber defense strategies, or are reviewing their existing ones. The concrete result of these policy shifts is a growing number of workshops, trainings, and exercises to boost the experience, resilience, and capabilities of Allies in cyberspace. A remarkable effort in this light is exercise Locked Shields, the world’s largest and most advanced international technical live-fire cyber defense exercise, which is hosted annually by the NATO Cooperative Cyber Defense Center of Excellence (CCDCoE) in Tallinn, Estonia. Locked Shields challenges cybersecurity experts from NATO member states, partner countries, and industry with scenario-based, real-time cyber-attacks enabling the participants to practice defending information technology networks and systems. Cyber and hybrid warfare crisis scenarios are now also being integrated in NATO’s annual Crisis Management Exercise (CMX), where Alliance civilian and military personnel test the procedures of decision-making and consultation through realistic mock Article 4 and Article 5 scenarios. These and other exercises like the annual Cyber Coalition Exercise are now an integral part of building NATO’s defensive cyber capabilities. As part of the NATO–EU Joint Declaration at the Warsaw Summit, NATO is also pressing ahead to boost its cooperation on cyber defense with the European Union as both share an interest in becoming more resilient. NATO and the EU signed a Technical Arrangement on Cyber Defense in February 2016 to strengthen cooperation, communication, and information sharing between NATO’s Computer Incident Response Capability and the EU’s Computer Emergency Response Team. The EU has also become a regular observer of NATO cyber defense exercises. NATO also increasingly recognizes the importance of working with industry partners to enable the Alliance to achieve its cyber defense policy objectives. A significant effort — the NATO Industry Cyber Partnership — was launched in September 2014 as a signal that NATO and industry must work more closely together in sharing information, experience, and expertise to counter cyber threats. Keeping Pace with an Evolving Threat Today NATO faces ongoing efforts from antagonists, including non-state actors, to intimidate and destabilize member states through cyber-attacks. The notion of cyber warfare is not new, but the scale, speed, and intensity of the challenge demands a new approach toward the preparation, deterence, and defense against these threats. One important innovation that cyber activities provide an adversary is ambiguity, both of intent and attribution. The source of cyber aggression is not easy to identify and requires advanced technological capabilities that only a few member states in NATO possess. Cyber aggression is even more difficult to prove publicly because laws and regulations in cyberspace are still incomplete. For NATO, the ambiguity of cyber campaigns present challenges vis-à-vis action that needs to be collectively addressed across the political, military, civilian, and technological spectrum. The following recommendations are designed to strengthen NATO resilience in cyberspace. Today NATO faces ongoing efforts from antagonists, including non-state actors, to intimidate and destabilize member states through cyber-attacks. The notion of cyber warfare is not new, but the scale, speed, and intensity of the challenge demands a new approach toward the preparation, deterence, and defense against these threats. One important innovation that cyber activities provide an adversary is ambiguity, both of intent and attribution. The source of cyber aggression is not easy to identify and requires advanced technological capabilities that only a few member states in NATO possess. Cyber aggression is even more difficult to prove publicly because laws and regulations in cyberspace are still incomplete. For NATO, the ambiguity of cyber campaigns present challenges vis-à-vis action that needs to be collectively addressed across the political, military, civilian, and technological spectrum. The following recommendations are designed to strengthen NATO resilience in cyberspace.

#### Cyberwar is increasingly likely---SolarWind emboldens hackers to undermine critical infrastructure and nuclear supply chains.

Bajema 21, \*Dr. Natasha Bajema is the Director of the [Converging Risks Lab at the Council on Strategic Risks](https://councilonstrategicrisks.org/programs/csw/dr-natasha-bajema/) and an IEEE Spectrum contributor. She has held long-term assignments at the National Defense University, in the U.S. Office of the Secretary of Defense, and at the U.S. Department of Energy’s National Nuclear Security Administration; (March 24th, 2021, “Today's Cyberattacks Foreshadow Wars to Come”, https://spectrum.ieee.org/riskfactor/aerospace/military/todays-cyberattacks-foreshadow-wars-to-come)

Cyberattacks are no longer just a matter of cybersecurity, they directly threaten a country’s national security. Cyberattacks alter the character of warfare—much like nuclear weapons once did, allowing adversaries to potentially cross enemy lines to harm large numbers of innocent civilians.

Today’s malicious actors can now seek to cause physical damage from remote locations through digital channels, wreaking devastation on a country at levels that previously would have required a kinetic attack.

On February 8, 2021, hackers breached the Bruce T. Haddock Water Treatment Plant in Oldsmar, Fla. using known software vulnerabilities in an attempt to poison the local water supply with sodium hydroxide—also known as lye. They accessed the plant through its industrial control system (ICS)—a system designed to allow for remote control and supervision of the plant. Taking over the plant’s controls, hackers increased parts of the chemical, used to [adjust the acidity and remove metals from drinking water](https://www.foxnews.com/politics/senate-intel-chairman-florida-water-plant-cyberattack), to one hundred times over the normal level. The system used an [old version of Windows, was accessible with a shared password, and had no firewall protection against intrusions](https://techgenix.com/florida-water-treatment-facility-cyberattack/). Thankfully, [a supervisor noticed the dangerous change in time whilst working remotely](https://www.govtech.com/em/safety/Cyberattack-on-Water-Treatment-Facility-Suggests-More-to-Come.html), averting a crisis that may have caused chemical burns and blindness among those exposed to the toxic chemical.

U.S. government officials have recently expressed concerns about similar vulnerabilities across water and energy sectors and other critical infrastructure including [health, emergency services, food and agriculture, and transportation systems](https://www.foxnews.com/politics/senate-intel-chairman-florida-water-plant-cyberattack). The cyberattack on the water plant occurred just a week before a major winter storm led to a widespread blackout and water crisis across Texas. [More than five million](https://time.com/5939633/texas-power-outage-blackouts/) went without power and running water for several days, illustrating the fragility of such interconnected infrastructure and the physical devastation that could be caused in the event of a cyberattack targeting the grid.

Critical infrastructure is not alone in its vulnerabilities to cyberattacks with physical implications—supply chains are also at risk. For at least a span of months (if not years), hackers have [exploited vulnerabilities](https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach) in software from Microsoft, VMWare and the Texas-based company [SolarWinds](https://www.solarwinds.com/) to compromise data security in at least 200 organizations in the U.S. government and other agencies around the world.

Although the SolarWinds attack appears to be a [case of classic espionage by Russia](https://www.securityinfowatch.com/cybersecurity/article/21206223/more-questions-than-answers-as-solarwinds-breach-probe-expands) via the U.S. supply chain, there are aspects of the attack that also illustrate the potential for achieving physical effects via digital channels. As early as [March 2020](https://www.securityinfowatch.com/cybersecurity/article/21206223/more-questions-than-answers-as-solarwinds-breach-probe-expands), Russian hackers breached the Orion network management software designed by SolarWinds, a federal contractor, and planted malicious code likely intended to gain access to sensitive information. Evidence of malware was first detected [in December by a cybersecurity company](https://www.newsweek.com/colorado-representative-says-solarwinds-hack-could-cyber-equivalent-pearl-harbor-1555994) that also uses the Orion software. The impact of the SolarWinds cyberattack spanned [thousands of networks](https://www.securityinfowatch.com/cybersecurity/article/21206223/more-questions-than-answers-as-solarwinds-breach-probe-expands) at [nine federal agencies and 100 private sector companies](https://www.cyberscoop.com/solarwinds-cyber-espionage-russia-neuberger/), including the Department of Energy’s National Nuclear Security Administration (NNSA), which is responsible for overseeing the U.S. nuclear weapons stockpile.

Although NNSA claims there was no impact to classified systems, officials found [evidence of attempted intrusion](http://www.politico.com/news/2020/12/22/nuclear-weapons-agency-congress-hacking-450184) in unclassified systems—although, according to the NNSA Public Affairs office, the system in question was used for business purposes, not for transport of nuclear weapons and materials. The agency also detected attempts to gain access to servers at the Los Alamos National Laboratory—one of three nuclear weapons labs. [NNSA immediately disconnected the software from relevant networks](https://www.energy.gov/articles/doe-update-cyber-incident-related-solar-winds-compromise), removing the possibility for deleterious effects. While hackers were not likely targeting the transport of nuclear weapons, the [vulnerabilities of nuclear weapons](https://www.nap.edu/read/11538/chapter/6#112) [while en-route](https://www.osti.gov/servlets/purl/1409912) [between secure locations](https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1348_web.pdf) are well known.

The exact objectives for the SolarWinds cyberattack remain unclear, but the vast extent of its reach may demonstrate to U.S. adversaries the significant potential of cyberattacks for achieving physical ends, including the possibility of stealing nuclear weapons. However, the incident is not the first major one from which malicious actors have deduced such capabilities—[consider the lessons from the NotPetya attack in 2017](https://spectrum.ieee.org/tech-talk/computing/it/notpetya-latest-ransomware-is-a-warning-note-from-the-future). Russian hackers spread malicious code through a popular accounting software developed by a Ukrainian business across many countries in Europe, eventually infecting tens of thousands of computers around the world. In addition to rendering infected computers useless, the attack shut down the global operations of the Maersk shipping company and caused major traffic congestion on the roads near ports in the United States. It also slowed operations of Merck & Co, Inc., a major producer of drugs and vaccines in the U.S., [reducing production capacity for a short period of time](https://www.fiercepharma.com/manufacturing/merck-has-hardened-its-defenses-against-cyber-attacks-like-one-last-year-cost-it). Even a classic espionage or sabotage incident may carry significant potential for physical damage.

The [Biden administration has already issued guidance](https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/) for shoring up vulnerabilities in U.S. supply chains, but much more needs to be done to protect critical infrastructure and dissuade malicious actors from exploiting digital channels to achieve physical ends. In an era of hybrid and gray zone warfare, cyberattacks are attractive to nations seeking to undermine their adversaries due to challenges of attribution and the associated benefit of deniability. In the future, these nations may also come to see cyberattacks with physical effects as a new form of warfare—a Trojan horse in the form of their adversary’s own infrastructure or supply chains. In so doing, they can cross enemy lines and cause damage and destruction without defeating any military forces.

#### Cooperation with NATO is key to cybersecurity- Chinese cyberattacks threaten critical infrastructure

Kramer et al 20

[**Franklin**](https://www.businessinsider.com/author/ben-winck) D. Kramer; Distinguished fellow and board director at Atlantic Council. Expert in cybersecurity, defense policy, and non-traditional threats; Lauren M. Speranza; Director of the Transatlantic Defense and Security program at the Center for European Policy Analysis (CEPA); Conor Rodihan; Associate director at Scowcroft Center for Strategy and Security; NATO needs continuous responses in cyberspace; Atlantic Council; https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/

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. Russia and China challenge NATO and its members in cyberspace on a daily basis, as part of ongoing hybrid campaigns to undermine the transatlantic community. The Kremlin’s actions have involved intrusions into Allies’ critical infrastructures, manipulating Allies’ elections through hacks and disinformation, and even blocking GPS information critical to NATO activities. The Chinese government has engaged in cyber espionage against Allies’ military capabilities; intellectual property theft related to sensitive technologies, industries, and infrastructure; and disinformation against transatlantic countries, including around the coronavirus. These efforts to weaken NATO countries and Alliance cohesion represent a persistent threat to Allied security. NATO has recognized the collective dangers of these hybrid attacks in cyberspace. Up to this point, however, the Alliance has taken a reactive approach, responding as if Russian and Chinese cyber attacks are each isolated incidents. But because Russian and Chinese cyber efforts are part of continuous campaigns directed at the overall capability of the Alliance, NATO’s response has been insufficient, failing to reduce or dissuade further attacks. To assure the security of its members going forward, NATO needs its own continuous response campaign to these threats. President-elect Biden and his team have pledged to renew US leadership in cooperation with Allies and partners. That agenda should start at NATO, and a key focus should be on cybersecurity. In early NATO meetings, the Biden administration should champion a cybersecurity continuous-response campaign, built around three key actions.

### Russia Attacks Increasing

#### Russia’s failure in the Ukraine means it will resort to more cyber-attacks.

Atlamazoglou ’22 (Stavros, Stavros Atlamazoglou is a seasoned defense journalist specializing in special operations, a Hellenic Army veteran, and a Johns Hopkins University graduate. “Putin’s Next Move: A Cyber War On NATO?” May 17, 2022, <https://www.19fortyfive.com/2022/05/putins-next-move-a-cyber-war-on-nato/> )

Is Putin Planning a Cyber Attack? The director of one of the United Kingdom’s top spy agencies warned that Russia is looking to target the U.S., NATO, and European Union countries with cyberattacks for their ongoing support of Ukraine. Putin’s Cyberwarfare Plan The war in Ukraine isn’t going well for Russian President Vladimir Putin and the Kremlin. The Russian military has suffered failure after failure in Ukraine, losing thousands of troops, tanks, aircraft, and vehicles in the process. Russia and Putin are becoming an international pariah as NATO wants to add new members. Sweden and Finland have decided to shed hundreds of years of non-alignment and join the transatlantic military alliance. It seems that **cyberwarfare remains the one warfighting domain in which Russia can truly be effective and a tool Putin can leverage. And the West knows that**. In a cyber security conference, Sir Jeremy Fleming, the director of the Government Communications Headquarters (GCHQ), warned that the **Russian military and intelligence services are searching for targets in the West to potentially attack with cyberweapons**. “We’re seeing it in cyber too. Perhaps, the concept of a ‘cyber war’ was over-hyped. But, there’s plenty of cyber about, including a range of activity we and partners have attributed to Russia. We’ve seen what looks like some spill over of activity affecting other countries. And we’ve seen indications that Russia’s cyber operatives continue to look for targets in countries that are opposing their actions,” the GCHQ director said. GCHQ is the signals and cyber intelligence agency of the U.K. and an equivalent of the U.S. National Security Agency (NSA). Is Putin Thinking Cyberattack? On the eve of the Russian invasion of Ukraine, Russian hackers launched a cyberattack against the Ukrainian military’s secure communications in an attempt to frustrate or takedown altogether its command and control (C2) functions. The idea was to prevent commanders from effectively and timely communicating with one another and their troops as the Russian ground and air forces were launching their operations. However, the attack spilled over and took down satellite communications in other countries, disrupting operations and internet service for thousands. “Today, in support of the European Union and other partners, the United States is sharing publicly its assessment that Russia launched cyber attacks in late February against commercial satellite communications networks to disrupt Ukrainian command and control during the invasion, and those actions had spillover impacts into other European countries. The activity disabled very small aperture terminals in Ukraine and across Europe. This includes tens of thousands of terminals outside of Ukraine that, among other things, support wind turbines and provide Internet services to private citizens,” the U.S. Department of State stated last week in a press release In addition to that cyberattack, the Russian intelligence services had been targeting Ukraine with repeated cyberattacks in the years and months before the invasion. “The UK’s National Cyber Security Centre (NCSC) assesses that the Russian Military Intelligence was almost certainly involved in the 13 January defacements of Ukrainian government websites and the deployment of Whispergate destructive malware. The NCSC also assesses that it is almost certain Russia was responsible for the subsequent cyber-attack impacting Viasat on 24 February,” the U.K. government announced.

#### Russian cyberattacks are coming and NATO is vulnerable- cyberwar is the lynchpin of Russia’s strategy of countering the US

**Dolan 2/15/22**

Dr. Chris J. Dolan is a Professor of Political Science and Director of the Master’s of Science Intelligence and Security at Lebanon Valley College; NATO Must Boost Hybrid Warfare Defenses; Just Security; https://www.justsecurity.org/80176/nato-must-boost-hybrid-warfare-defenses/

Russia could launch a conventional military invasion of Ukraine at any moment, but it could also destabilize and undermine it without ever firing a shot. Russian military exercises and positioning are powerful tools of unpredictability that keep NATO and Ukraine off balance while Russian operatives and their proxies wage a hybrid war through covert operations, coordinated disinformation campaigns, and cyber attacks. To build resilience against hybrid warfare, NATO should collaborate with the private sector and devote more resources to technology literacy and innovation.¶ Russia’s Hybrid Warfare Strategy¶ Russia’s strategy is centered on promoting a narrative of grievances. Russia believes the United States is using Ukraine and promoting NATO expansion to contain Russian national security interests and encroach on its traditional spheres of influence. It also contends that Ukraine should return to the Minsk Agreements and end its attempt to win back Donbas. These are false narratives because sovereign and independent states have the freedom to determine their own path and seek membership in any alliance. And it would be madness for the Ukrainian government to retake Donbas given the Russian military presence there. The Russian rhetoric is a trojan horse created by the Kremlin to renegotiate the end of the Cold War and redraw European borders the same way Russia did when it illegally annexed Crimea in 2014.¶ **The effectiveness of the Russian narrative depends on combining conventional military positioning with hybrid tactics** or “active measures.” Hybrid actions taken in the so-called “gray-zone” typically consist of measures short of conventional warfare such as limited strikes, special operations forces, raids, cyber attacks, and covert influence operations. **Hybrid warfare is a central element of Russia’s military strategy**, in which operatives remain just below the radar and work with proxies to stage false flags to justify an invasion. To crush the Prague Spring in 1968, Soviet operatives in Czechoslovakia planted weapons in packages labeled “Made in the USA,” which were published in Soviet state-controlled outlets as signs of a U.S.-led plot. The KGB ran active measures during the Soviet war in Afghanistan in the 1980’s, often using “false bands” of Afghan units posing as CIA-backed guerillas to justify Soviet military operations.¶ Misinformation and disinformation are quickly and efficiently distributed through news channels and social media to influence public opinion. Russian state-owned outlets Russia Today (RT), Tass, and Sputnik have a strong presence on Facebook, Twitter, YouTube, and Telegram, echoing the Kremlin’s position and portraying NATO and the United States as aggressors. In 2013-2014, Russian state media framed the Maidan protests that toppled Ukrainian President Viktor Yanukovych as “fomented by the U.S. in cooperation with fascist Ukrainian nationalists” that were used as a pretext for Russia’s little green men to seize Crimea.¶ One Russian-backed channel on YouTube is НАШ or NASH TV, which has been promoting Russia’s narrative until it was banned in Ukraine. Founded by former pro-Russia Ukraine parliament member Yevheniy Murayev, NASH TV is a Kremlin mouth piece flooding viewers with anti-American and anti-NATO falsehoods. Last month, the United Kingdom accused Russia of attempting to overthrow Ukrainian President Volodymyr Zelensky and replace him with Murayev. This is the same approach used by Russia when it seized Crimea and installed Sergey Aksyonov as the so-called Prime Minister of Crimea.¶ Sustained Russian information operations reinforce specific elements in Moscow’s narrative of grievances. First, NATO’s eastward expansion since the end of the Cold War is the real threat, not Russia. Second, Ukraine and Georgia joining NATO would threaten the European security order. Third, the annexation of Crimea and support for separatists in Donbas are liberations of Russian-speaking communities.¶ Troll factories and bots spread large volumes of fake news stories, making it almost impossible to counter the steady deluge of disinformation. On January 31, it Western media reported that Russia planted fake stories about bomb threats against Ukrainian schools and shopping malls, forcing children to online learning and closing businesses. Just last week, U.S. officials uncovered a plot by Russian intelligence to fabricate a propaganda video portraying fake explosions, corpses, and grieving women designed to legitimate a Russian invasion to protect civilians in Ukraine.¶ **Russia supplements information operations with cyber attacks**. Russian hackers recently breached Ukrainian networks, replacing publicly facing websites with messages in Ukrainian and Polish designed to look like a Polish cyber operation. Russian cyber attacks targeted Georgian networks during the 2008 South Ossetia War and again in 2015 when Sandworm, a hacking group linked with Russian intelligence, took down Ukraine’s power grid.¶ **Russian state-sponsored cyber attacks targeting Ukraine can devastate U.S. and NATO networks.** The 2017 Notpetya and WannaCry attacks spread throughout the world soon after hitting their targets. In the 2020 Solar Winds hack, cyber criminals directed by Russian intelligence inserted malicious code into updates in Orion software that infected servers used by the U.S. Treasury, Energy, and Defense Departments, as well as Microsoft, Intel, and Cisco. The U.S. Cybersecurity and Infrastructure Security Agency recently warned **U.S. networks are vulnerable to more Russian cyber attacks**.¶ Russia also uses blended cyber operations, in which governments tolerate cyber criminals and ransomware groups operating in their countries. For example, the 2021 cyber attacks against Colonial Pipeline, which controls much of the fuel along the U.S. East Coast, were launched by criminal group Darkside operating in Russia. Darkside locked up Colonial Pipeline’s networks and held data hostage until it paid a ransom of $5 million.

#### NATO-Russia cyber war is increasing—5 eye warns necessitates protection

Nick Corbishley**;** April 22**,** 2022; writer for Naked Capitalism; The Russia-NATO Cyber War Is Escalating Fast; Naked Capitalism; <https://www.nakedcapitalism.com/2022/04/are-we-in-the-first-ever-global-cyber-war.html>;

Eight cybersecurity authorities from the so-called “Five Eye” nations (United States, United Kingdom, Australia, Canada and New Zealand) released a joint statement on Thursday warning that more malicious cyber activity is on the way as Russia’s invasion of Ukraine continues to undermine geopolitical stability. Before we look at the statement in any depth, an important five-pronged caveat is needed: Both the US and the UK are among the primary antagonists in NATO’s ongoing war with Russia; They both have significant offensive cyber war capabilities of their own; US intelligence agencies, at Obama’s behest, have drawn up a list of potential overseas targets for cyber attacks; Both countries have surreptitiously conducted vast surveillance programs, targeting not only their own populations but also citizens and government leaders of other countries; The world right now is in the grip of the biggest information war of this century. As such, any information coming out of the Five Eyes’ intelligence services should be treated with a healthy dose of skepticism. That having been said, here are the first three paragraphs of the missive: The cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom are releasing this joint Cybersecurity Advisory. The intent of this joint CSA is to warn organizations that Russia’s invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and U.S. allies and partners. Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks (see the March 21, 2022, Statement by U.S. President Biden for more information). Recent Russian state-sponsored cyber operations have included distributed denial-of-service (DDoS) attacks, and older operations have included deployment of destructive malware against Ukrainian government and critical infrastructure organizations. Additionally, some cybercrime groups have recently publicly pledged support for the Russian government. These Russian-aligned cybercrime groups have threatened to conduct cyber operations in retaliation for perceived cyber offensives against the Russian government or the Russian people. The document also emphasizes the frontline role likely to be played by Russian state actors, including the Russian Federal Security Service (FSB), the Russian Foreign Intelligence Service (SVR), Russian General Staff Main Intelligence Directorate (GRU), GRU’s Main Center for Special Technologies (GTsST) and the Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM) of the Russian Ministry of Defense. Clearly, Russia has the capability to launch a barrage of cyber attacks against the west; the question is: does it want to? The authors of the document urge critical infrastructure organizations to take immediate steps to protect against cyberattacks. Those steps, they say, should include patching known exploited vulnerabilities, updating software, enforcing multi-factor authentication, securing and monitoring remote desktop protocol (RDP) and other “potentially risky” services, and providing end-user security awareness and training. As The Register, a British technology news website, notes, if any of these recommendations come as a surprise to critical infrastructure operators, “we’re screwed”. The warning from the “Five Eye” nations comes just days after NATO began (as Bloomberg puts it) “the largest and most complex ‘live-fire’ cyber defense exercises” ever conducted. More than 2,000 people from 32 nations were expected to participate in the war game, which began on Tuesday in Tallinn, Estonia. They include representatives of five to 10 large global financial institutions, including Santander and Mastercard. This is all happening as fears rise that the boundaries of the cyber war between Russia and NATO could soon spread beyond Europe, where attacks have been registered not only in Ukraine and Russia but also Poland and Finland. On March 21, President Joe Biden warned American businesses to prepare themselves for cyberattacks. Russia is likely to deploy cyber attacks as a form of retaliation against US sanctions, Biden said, adding that Russia has “a very sophisticated cyber capability,” which Putin “hasn’t used… yet” but which forms “part of his playbook.”

### Russia Capable

#### Russia absolutely has the capability

**Tidy, 22** (Joe Tidy, 3-22-2022, accessed on 6-16-2022, BBC News, "The three Russian cyber-attacks the West most fears", https://www.bbc.com/news/technology-60841924)ao

However, Russia is a cyber-superpower with a serious arsenal of cyber-tools, and hackers capable of disruptive and potentially destructive cyber-attacks. Ukraine has remained relatively untroubled by Russian cyber-offensives but experts now fear that Russia may go on a cyber-offensive against Ukraine's allies. "Biden's warnings seem plausible, particularly as the West introduced more sanctions, hacktivists continue to join the fray, and the kinetic aspects of the invasion seemingly don't go to plan," says Jen Ellis, from cyber-security firm Rapid7. Here are the hacks that experts most fear. BlackEnergy - targeted critical infrastructure attack Ukraine is often described as the hacking playground of Russia, which has carried out attacks there seemingly to test techniques and tools. In 2015 Ukraine's electricity grid was disrupted by a cyber-attack called BlackEnergy, which caused a short-term blackout for 80,000 customers of a utility company in western Ukraine. Nearly exactly a year later another cyber-attack known as Industroyer took out power for about one-fifth of Kyiv, the Ukrainian capital, for about an hour. The US and EU named and blamed Russian military hackers for the attacks. "Russia could absolutely try to execute an attack like this against the West as an illustration of capabilities and to make a statement," says Ukrainian cyber-security responder Marina Krotofil, who helped investigate the power cut hacks. "However, no cyber-attack against a power grid has resulted in an extended interruption of power supply. Executing cyber-attacks on complex engineering systems in a reliable way is extremely difficult and achieving a prolonged damaging effect is sometimes impossible due to in-built protections." Experts like Ms Krotofil also hypothesise that this could backfire on Russia too, as the West is most likely to have a decent foothold in Russian networks too. NotPetya - uncontrollable destruction NotPetya is thought to be the most costly cyber-attack in history and has been blamed on a group of Russian military hackers by the US, UK and EU authorities. The destructive software was hidden in an update of popular accounting software used in Ukraine, but spread worldwide destroying the computer systems of thousands of companies and causing approximately $10bn (£7.5bn) of damage. North Korean hackers are accused of causing huge disruption with a similar attack a month earlier. The WannaCry "worm" (a kind of virus) scrambled data on approximately 300,000 computers in 150 countries. The UK's National Health Service was forced to cancel large numbers of medical appointments. "These kinds of attacks would cause the greatest opportunity for mass chaos, economic instability, and even loss of life," says Ms Ellis. "It might sound far-fetched, but critical infrastructure often depends on connected technologies, just as much as every other part of our modern lives, and we have seen the potential for that with the impact of the WannaCry on UK hospitals." However, computer scientist Prof Alan Woodward, from the University of Surrey, says such attacks carry risks for Russia too. "These types of uncontrollable hacks are much more like biological warfare, in that it's very difficult to target specific critical infrastructure in specific places. WannaCry and NotPetya saw victims in Russia too." Colonial Pipeline - cyber-criminal attacks intensify In May 2021, a state of emergency was declared in a number of US states after hackers caused a vital oil pipeline to shut down. Colonial Pipeline carries 45% of the east coast's supply of diesel, petrol and jet fuel and the supply led to panic at the pumps. This attack wasn't carried out by Russian government hackers, but by the DarkSide ransomware group, which is thought to be based in Russia. The pipeline company admitted to paying criminals $4.4m in hard-to-trace Bitcoin, in order to get computer systems back up and running. A few weeks later meat supplies were affected when another ransomware crew called REvil attacked JBS, the world's largest beef processor. One of the big fears experts have about Russian cyber-capabilities is that the Kremlin may instruct cyber-crime groups to co-ordinate attacks on US targets, to maximise disruption. "The benefit of instructing cyber-criminals to carry out ransomware attacks is the general chaos they can cause. In large enough numbers they can cause serious economic damage," Prof Woodward says. "It also comes with the added bonus of plausible deniability as these groups are a step removed from an attack by the Russian state." How could the US respond? In the highly unlikely case that a Nato country is on the receiving end of a cyber-attack that causes loss of life or huge irreparable damage, then this could trigger Article 5, the alliance's collective defence clause. But experts say this would drag Nato into a war it does not want to be a part of, so any response is more likely to be from the US and close allies. President Biden has already said that "we are prepared to respond" if Russia launches a large attack on the US. However, the unprecedented cyber-chaos seen in Ukraine in recent weeks from vigilante hackers on either side of the war shows how easily things can escalate. So any action is likely to be extremely carefully considered.

### Miscalculation

#### Failure to coordinate with allies causes cyber attacks to generate miscalculation that escalates conflict with Russia

Alina Polyakova and Mathieu Boulègue in 2021

President and CEO of the Center for European Policy Analysis (CEPA) as well as an adjunct professor of European studies at the Johns Hopkins University’s School of Advanced International Studies (SAIS) AND Senior Research Fellow, Russia and Eurasia Programme @ Chatham House; The Evolution of Russian Hybrid Warfare: Conclusion; https://cepa.org/the-evolution-of-hybrid-warfare-conclusion/

The current Russian leadership has no incentive to dial back its efforts to undermine Western cohesion, especially since the assessment in Moscow is that these are largely succeeding. The West should, therefore, expect more, not less, tactical exploitation of the logics of chaos for the foreseeable future. Despite individual countries becoming more resilient to Russia’s evolving hybrid warfare, as seen in the cyber arena in Estonia and to some extent, the United Kingdom, the problem remains that the broader Western alliance as a whole is still underprepared to cope with and respond effectively to Russian destabilization.¶ As a result, miscalculation and overreach by both sides in crisis scenarios are increasingly more likely and outcomes more unpredictable. Geopolitical competition will look less like a cold war and more like a constant barrage of violent episodes, low-threshold probes of Western readiness, and strategic deception and obfuscation of targets and intentions. Russia’s resolve to engender global chaos could unintentionally lead to an escalatory cycle. This danger will be compounded by Russia’s relentless effort to probe NATO’s coherence and ability to defend its member states.¶ Without equal assessment and adaptation to Russia’s evolving tactics of hybrid war, Western policies will become less effective over the long run. Despite growing sophistication in certain domains, such as cyber, Russian influence attempts are often messy and opportunistic, taking advantage of weaknesses within target states’ systems.¶ Moscow has also shown itself to be effective at identifying and filling, with minimal resources, power vacuums left behind by Western, and in particular U.S., disengagement. Comprehensive measures to address these vulnerabilities should necessarily also restrict the potential entry points for Russian influence attempts.

### Deterrence

#### NATO must improve its cyber defense capabilities to credibly deter war

Lindley-French ’22 (Julian is a fellow at the Canadian Global Affairs Institute and chair of The Alpen Group, 2-1, 22, To keep the peace, NATO must be ready to fight the wars, https://ipolitics.ca/2022/02/02/to-keep-the-peace-nato-must-be-ready-to-fight-the-wars/)

The NATO alliance is now facing what could be the most complex set of challenges in its history. Given the nature and extent of the threats against citizens of the alliance from Vancouver to Vilnius, urgency must be the hallmark of Strategic Concept 2022 — in essence, the alliance’s manifesto — to more clearly stress defence against, and deterrence of, Russian aggression in the region. **Russia continues to pose the most immediate threat to NATO** (also called the North Atlantic Alliance). The latter will continue seeking dialogue with Russia and honouring the NATO-Russia Founding Act, even though Russia continues to breach the values, principles, trust, and commitments that were meant to underpin the NATO-Russia Council. Much will depend on Russia’s aggression toward Ukraine, and the alliance can’t stand aside. NATO should launch a Ukrainian Deterrence Initiative to provide military equipment and training, as well as enhance Ukraine’s resilience. **Terrorism continues to challenge the rules-based international order by undermining democracy and stability** across the globe. **China’s rise as a military power will be the main cause of change in the coming decade**. While NATO must seek to maintain a constructive dialogue with China, possibly through some form of NATO-China Council, Beijing’s growing influence and power present challenges that the alliance must address. NATO must also grasp failure, and reflect on hard lessons from the chaotic and tragic withdrawal from Afghanistan. The need for realistic political objectives allied to strategic patience must be reinforced by strengthened political cohesion and the equitable sharing of risk and cost. Mass disruption and mass destruction are merging into a continuum of risk, challenge, and threat, which the alliance must contend with across a broad spectrum of tasks, from defence and deterrence to engagement. Strategic Concept 2022 must reset NATO’s purpose. The alliance will continue to lead the collective defence of Europe in accordance with Article 5 of the Washington Treaty. **NATO remains vital to effective crisis management**, and has a critical role to play in promoting co-operative security with partners in and around Europe and across the wider world. Something old, something new? The principle of resilience, making civil society more robust, is anchored in Article 3 of the alliance’s founding treaty. NATO has also reaffirmed that national and collective resilience is a vital component of credible deterrence and defence***. Cyberattacks and information warfare on critical civilian and military infrastructures are now deemed clear and present dangers, and must be countered.*** But it’s deterrence and defence that must remain NATO’s core business. ***If the alliance is to remain credible as a peacekeeper,* NATO must always be a capable warfighter. NATO forces must meet the challenge of the fast-changing character and conduct of warfare, which now stretches across a mosaic of information war, cyberwar, and increasingly precise and rapid “hyper wa**r.” U.S. armed forces will continue to lead NATO for operations in Europe, but they’re engaged with the world. By 2030, a more equitable sharing of alliance burdens is needed, built on a commitment by the European allies to field 50 per cent of NATO’s minimum military requirement. Call it European strategic autonomy or strategic responsibility; either way, it realizes that greater European military capability will be vital. By 2030, Canadian and European allies must be able to deploy a NATO Allied Command Operations Mobile Heavy Force (AMHF). By consolidating all Allied Rapid Response Forces into a single pool of forces, the AMHF could act in any and all emergencies as a high-end first responder NATO Future Force that reinforces rather than drains the Americans. Fail to act now, and Europe could face a digital Pearl Harbor from which it wouldn’t recover. **A catastrophic “bolt from the blue” would combine strategy, capability, new technologies of intelligent design, artificial intelligence, Big Data, quantum computing, etc., to decisively change the character of warfare, and Europe with it.** By 2030, NATO must be a very different alliance, because it will be in a very different place. Otherwise, it could fail, although any such failure might not be the catastrophic demise some have predicted for so long. A Potemkin NATO would simply be yet more European-defence pretence: a pretty, reassuring façade of false security. Strategic Concept 2022 is the best chance NATO leaders have to set the alliance on course for 2030. Collectively, they must generate the necessary will, vision, and leadership.

### Impact – Russia War

#### NATO-Russia war goes nuclear and kills billions

Majumdar 18 (Dave Majumdar (the defense editor for the National Interest). “Doomsday: Why a War with Russia Would Go Nuclear (And Kill Billions of People).” The National Interest. January 25, 2018. <https://nationalinterest.org/blog/the-buzz/doomsday-why-war-russia-would-go-nuclear-kill-billions-24214>)

A NATO counter-offensive would be bloody and fraught with escalatory risk—but it’s one of the probable outcomes of a Russian invasion. In that eventuality, Russian conventional forces—of which only a portion are well trained and well equipped—would likely be severely damaged or even destroyed. Moreover, if NATO forces hit targets inside Russia or crossed over into Russian territory, Moscow might conclude that there is a danger to the existence of the state. After all, Moscow has expressed concerns in the past that regime change by the West is an all too real danger. In that situation, Russia might counter advancing NATO forces with its arsenal of tactical nuclear weapons. While a recent RAND Corporation study concluded that Russia could overrun NATO’s member states Estonia, Latvia and Lithuania in the Baltics within sixty hours, the war games did not simulate the use of nuclear weapons. If, however, a war were to breakout between NATO and Russia, nuclear weapons would certainly come into play—especially if the conflict were going poorly for Moscow. Unlike the Soviet Union, which had a stated “no first use” policy, modern Russia explicitly rejected that pledge in 1993. In fact, as Moscow’s conventional forces continued to atrophy during the economic and social meltdown of the 1990s, Russia developed a doctrine called de-escalation in 2000 . Simply put, if Russia were faced with a large-scale attack that could defeat its conventional forces, Moscow might resort to nuclear weapons. In 2010, Russia revised the doctrine somewhat as its conventional forces started to recover from the aftermath of the Soviet collapse—the current version states Moscow would use nuclear weapons in situations “that would put in danger the very existence of the state.”

#### Russia war is the only actual extinction risk

Farquhar et al ‘17 (Sebastian Farquhar, DPhil from the University of Oxford in Cybersecurity and AI. Stefan Schubert, PhD in philosophy and postdoc at London School of Economics, where he combined his research with outreach work in the field of political rationality. Owen Cotton-Barratt, DPhil in pure mathematics, Research Fellow at the University of Southampton, former Director of Research at the Centre for Effective Altruism. Haydn Belfield, Policy Associate to the University of Oxford’s Global Priorities Project, former Senior Parliamentary Researcher to a British Shadow Cabinet Minister. John Halstead, Global Priorities Project, a collaboration between the Centre for Effective Altruism and the Future of Humanity Institute, part of the University of Oxford. Andrew Snyder-Beattie, fellow in the Emerging Leaders in Biosecurity Initiative from the Johns Hopkins Center for Health Security. “Existential Risk: Diplomacy and Governance”. Global Priorities Risk 2017. <https://www.fhi.ox.ac.uk/wp-content/uploads/Existential-Risks-2017-01-23.pdf>) swap

The bombings of Hiroshima and Nagasaki demonstrated the unprecedented destructive power of nuclear weapons. However, even in an all-out nuclear war between the United States and Russia, despite horrific casualties, neither country’s population is likely to be completely destroyed by the direct effects of the blast, fire, and radiation.8 The aftermath could be much worse: the burning of flammable materials could send massive amounts of smoke into the atmosphere, which would absorb sunlight and cause sustained global cooling, severe ozone loss, and agricultural disruption – a nuclear winter. According to one model 9, an all-out exchange of 4,000 weapons10 could lead to a drop in global temperatures of around 8°C, making it impossible to grow food for 4 to 5 years. This could leave some survivors in parts of Australia and New Zealand, but they would be in a very precarious situation and the threat of extinction from other sources would be great. An exchange on this scale is only possible between the US and Russia who have more than 90% of the world’s nuclear weapons, with stockpiles of around 4,500 warheads each, although many are not operationally deployed.11 Some models suggest that even a small regional nuclear war involving 100 nuclear weapons would produce a nuclear winter serious enough to put two billion people at risk of starvation,12 though this estimate might be pessimistic.13 Wars on this scale are unlikely to lead to outright human extinction, but this does suggest that conflicts which are around an order of magnitude larger may be likely to threaten civilisation. It should be emphasised that there is very large uncertainty about the effects of a large nuclear war on global climate. This remains an area where increased academic research work, including more detailed climate modelling and a better understanding of how survivors might be able to cope and adapt, would have high returns.

### Impact – laundry list

#### Populism, econ, grid, health care

Pelletier 22 [Justin Pelletier is the business director for Eaton Cybersecurity Security Assessment and Forensic Examination (SAFE) Lab in RIT's Center for Cybersecurity ,The Conversation Us Russian Cyberattacks against the U.S. Could Focus on Disinformation Scientific American 1-28-2022 <https://www.scientificamerican.com/article/russian-cyberattacks-against-the-u-s-could-focus-on-disinformation/>] 6/14/2022

As tensions mount between Russia and the West over Ukraine, the threat of Russian cyberattacks against the U.S. increases. The Department of Homeland Security issued an intelligence bulletin on Jan. 23, 2022, warning that Russia has the capability to carry out a range of attacks, from denial-of-service attacks on websites to disrupting critical infrastructure like power grids.

“We assess that Russia would consider initiating a cyber attack against the Homeland if it perceived a US or NATO response to a possible Russian invasion of Ukraine threatened its long-term national security,” the DHS stated in the bulletin, which it sent to law enforcement agencies, state and local governments, and critical infrastructure operators.

Cybersecurity experts are concerned that in the wake of recent cyberattacks by hackers affiliated with Russia, the Russian government has the capability to carry out disruptive and destructive attacks against targets in the U.S. The SolarWinds attack, uncovered in December 2020, gave the perpetrators access to the computer systems of many U.S. government agencies and private businesses. The DHS and FBI accused Russian hackers in March 2018 of infiltrating U.S. energy and infrastructure networks.

Russian cyberattacks could include continued attempts to diminish Americans’ confidence in elections, undermine economic stability, damage the energy grid, and even disrupt health care systems.

While some components of these systems almost certainly remain vulnerable to Russian-aligned hackers, the Russian government is likely to think twice before unleashing highly disruptive attacks against the U.S., because the U.S. government could interpret such attacks, particularly those targeting critical infrastructure, as acts of war. The DHS bulletin stated that Russia has a high threshold for initiating disruptive attacks. As a researcher who studies cyberwarfare, I believe a more likely threat from Russian hackers is launching disinformation campaigns.

DISTRACT, DISTORT AND DIVIDE

Americans can probably expect to see Russian-sponsored cyber activities working in tandem with propaganda campaigns. These activities are likely to be aimed at preventing a unified response to Russian aggression in Ukraine.

Russian military doctrine includes the well-evolved concept of information confrontation, which uses cyber means to create doubt about what is true. Russia’s information warfare strategy seeks to manipulate information and relationships.

The specific maneuvers aim to bolster narratives, people and groups that support Russian interests and undermine those that are counter to Russian interests. The maneuvers, which include dismissing and distorting information and undermining opinion leaders, are carried out in the press and on social media.

Russian intelligence operatives are skilled at using technology, including amplifying misinformation through fake accounts on popular social media platforms. In effect, Russia uses social and other online media like a military-grade fog machine that confuses the U.S. population and encourages mistrust in the strength and validity of the U.S. government.

Repressive governments like those in Russia and China have perfected the manipulation of online information as a way to control their own populations. Democracies are especially vulnerable to these techniques, given the open exchange of ideas and lack of centralized control over sources of information.

In addition, U.S. society is polarized, and that polarization is occurring at an increasing rate. A study by researchers at the University of Oxford examined Russia’s computational propaganda against the U.S. between 2013 and 2018 and found that it was designed to boost U.S. political polarization.

PLAUSIBLE DENIABILITY

Though the Russian government commonly operates through its intelligence services, including the technical experts in the GRU military intelligence service and the spymasters in the FSB domestic intelligence service, it also uses criminal groups to achieve its aims.

History shows that Russia is most likely to recruit proxies to carry out cyberattacks that disrupt decision-making so that the attacks don’t point directly back to the Kremlin. There is no foggier battlefield than cyberspace. That is one of the main benefits of cyberspace as an element of national power – a cyberattack almost always allows for plausible deniability.

On Jan. 14, 2022, Russia arrested members of the Russian-based cyber gang REvil who were responsible for the 2021 ransomware attacks against meat supplier JBS Foods, headquartered in Greeley, Colorado, and the Colonial Pipeline, headquartered in Alpharetta, Georgia. The unusual move caused cybersecurity analysts to wonder about Russia’s motive, including speculation about making it easier for the government to deny a connection to the cyberattacks.

U.S. CYBER DEFENSES

National cyber defense is inherently challenging, but the U.S. is far from defenseless. Several analysts have noted that the U.S. is the most capable cyber power in the world. The U.S. also has 20 years of experience dealing with Russian cyber aggression.

The Biden administration’s tough stance on Russian hacking has made some progress. And though disinformation is among the murkiest of cyber strategies, cybersecurity experts are making headway on that front, too.

CAUSE FOR CONCERN BUT NO REASON TO FEAR

Cyber activity that creates room for Russia to present the seizure of Ukraine as a fait accompli is much more likely than a crippling cyberattack. Though Russia might temporarily deter a U.S. response to Russian moves in Ukraine by disrupting U.S. critical infrastructure, Americans are likely to present a unified and powerful response to such an overt attack. I believe Russia is more likely to prefer a path of insidious political polarization to weaken U.S. geopolitical influence.

Even if Russia were to launch extensive cyberattacks against the U.S., the average American is unlikely to be harmed. The disruption of natural gas and food supplies would clearly have a significant economic impact, but it is extremely rare for a cyberattack to lead to loss of life.

If you are worried about the situation in Ukraine and wondering what you can do to defend against Russian cyberattacks, I recommend tuning out divisive rhetoric and cultivating common ground with Americans whom you might not agree with. Though there are many issues U.S. society is working through, Americans can still try to find some general agreement in the principles of the American experiment.

### Impact – Econ

**Decline would collapse deterrence----that causes extinction but keeping it solves the case**

**Tønnesson 15** (Research Professor, Peace Research Institute Oslo; Leader of East Asia Peace program, Uppsala University, 2015, “Deterrence, interdependence and Sino–US peace,” International Area Studies Review, Vol. 18, No. 3, p. 297-311)

Several recent works on China and Sino–US relations have made substantial contributions to the current understanding of how and under what circumstances a combination of nuclear deterrence and economic interdependence may reduce the risk of war between major powers. At least four conclusions can be drawn from the review above: first, those who say that interdependence may **both inhibit and drive conflict** are right. Interdependence raises the cost of conflict for all sides but asymmetrical or unbalanced dependencies and negative trade expectations may generate tensions leading to trade wars among interdependent states that in turn **increase the risk of military conflict** (Copeland, 2015: 1, 14, 437; Roach, 2014). The risk may increase if one of the interdependent countries is governed by an inward-looking socio-economic coalition (Solingen, 2015); second, the risk of war between China and the US should not just be analysed bilaterally but include their allies and partners. Third party countries could drag China or the US into confrontation; third, in this context it is of some comfort that the three main economic powers in Northeast Asia (China, Japan and South Korea) are all deeply integrated economically through production networks within a global system of trade and finance (Ravenhill, 2014; Yoshimatsu, 2014: 576); and fourth, decisions for war and peace are taken by very few people, who act on the basis of their future expectations. International relations theory must be supplemented by foreign policy analysis in order to assess the value attributed by national decision-makers to economic development and their assessments of risks and opportunities. If leaders on either side of the Atlantic begin to seriously fear or anticipate their own nation’s decline then they may blame this on external dependence, appeal to anti-foreign sentiments, contemplate the use of force to gain respect or credibility, adopt protectionist policies, and ultimately **refuse to be deterred by** either **nuclear arms** or prospects of socioeconomic calamities. Such a dangerous shift could happen **abruptly**, i.e. under the instigation of actions by a third party – or against a third party. Yet as long as there is both nuclear deterrence and interdependence, the tensions in East Asia are unlikely to escalate to war. As Chan (2013) says, all states in the region are aware that they cannot count on support from either China or the US if they make provocative moves. The greatest risk is not that a territorial dispute leads to war under present circumstances but that **changes in the world economy** alter those circumstances in ways that render inter-state peace more precarious. If China and the US fail to rebalance their financial and trading relations (Roach, 2014) then a trade war could result, interrupting transnational production networks, provoking social distress, and exacerbating nationalist emotions. This could have unforeseen consequences in the field of security, with nuclear deterrence remaining the only factor to protect the world from Armageddon, and unreliably so. **Deterrence could lose its credibility: one of the two great powers might gamble that the other yield in a cyber-war or conventional limited war**, or third party countries might engage in conflict with each other, with a view to obliging Washington or Beijing to intervene.

### Impact – Grid

#### A cyber attack on the power grid causes nuclear war

Tilford 12 (Robert, Graduate US Army Airborne School, Ft. Benning, Georgia, “Cyber attackers could shut down the electric grid for the entire east coast” 2012, <http://www.examiner.com/article/cyber-attackers-could-easily-shut-down-the-electric-grid-for-the-entire-east-coa> \*\*\*we don’t agree with the ableist language)

To make matters worse a cyber attack that can take out a civilian power grid, for example could also cripple [wreck] the U.S. military. The senator notes that is that the same power grids that supply cities and towns, stores and gas stations, cell towers and heart monitors also power “every military base in our country.” “Although bases would be prepared to weather a short power outage with backup diesel generators, within hours, not days, fuel supplies would run out”, he said. Which means military command and control centers could go dark. Radar systems that detect air threats to our country would shut Down completely. “Communication between commanders and their troops would also go silent. And many weapons systems would be left without either fuel or electric power”, said Senator Grassley. “So in a few short hours or days, the mightiest military in the world would be left scrambling to maintain base functions”, he said. We contacted the Pentagon and officials confirmed the threat of a cyber attack is something very real. Top national security officials—including the Chairman of the Joint Chiefs, the Director of the National Security Agency, the Secretary of Defense, and the CIA Director— have said, “preventing a cyber attack and improving the nation’s electric grids is among the most urgent priorities of our country” (source: Congressional Record). So how serious is the Pentagon taking all this? Enough to start, or end a war over it, for sure. A cyber attack today against the US could very well be seen as an “Act of War” and could be met with a “full scale” US military response. That could include the use of “nuclear weapons”, if authorized by the President.

### Impact – Disease

#### An effective health care system is key to preventing the spread of disease

Peterson 14 (Kimberly Ann Petersen, Captain, Fremont, CA, Police Department. “The Affordable Care Act: A Prescription For Homeland Security Preparedness?” Submitted in partial fulfillment of the requirements for the degree of Master Of Arts Security Studies (Homeland Security and Defense) from the Naval Postgraduate School. September 2014. https://calhoun.nps.edu/bitstream/handle/10945/43979/14Sep\_Petersen\_Kimberly.pdf?sequence=1)

An effective health surveillance system requires that those stricken by illness or disease—whether accidentally contracted or intentionally afflicted—seek treatment from a health care professional. The health care professional works to diagnose the problem, prescribe care, mitigate further spread, and report the illness as necessary to the health care community and possibly the government. This process is critical to our nation’s security in the event of a bioterror attack, such as with an Ebola virus or anthrax attack. The same holds true in managing contagious diseases such as influenza or newly emerging diseases. The sooner an illness or disease is correctly diagnosed, the more options remain available to help mitigate the spread or effect. Delays in diagnoses and therefore the development of appropriate treatments can have a limiting effect on both the health care community’s and the homeland security community’s choices and options in managing the spread and effect of the affliction. Jack Hadley’s analysis showed statistically significant and positive support for the hypothesis that having health insurance or greater medical care use improves health: seven of the 10 natural experiments analyzed, six of the seven longitudinal studies, 29 of 35 of the observational studies showed “statistically significant results consistent with a positive relationship between health insurance or medical care use and health.”170 According to author G. Kenny, the uninsured received only 55 percent of the medical services received by the insured.171 Increased health insurance coverage correlates with an increased use of health care services,172 which is likely to increase the chance of earlier identification and mitigation of disease. This is good news for homeland security. The uninsured are more than four times more likely than the insured to delay needed medical care or forego it altogether due to cost concerns.173 By increasing the number of insured Americans, we also increase the likelihood that those with contagious diseases will seek treatment earlier on, allowing health professionals to identify, treat and mitigate disease spread more successfully. This would include diseases of concern to the homeland security community such as influenza virus, or any disease that has the ability to spread from person-to-person. A 2012 report from the Office of the Director of National Intelligence focused on “megatrends” and future possibilities for the global world in the year 2030.174 One area of focus was the increasing likelihood that viruses previously unknown in humans would continue to cross over from the animal reservoir to humans due to increased livestock production and human encroachment into the jungles. Examples of prior occurrences include a prion disease in cattle that jumped to humans in 1980 to cause variant Creutzeldt-Jacob disease in humans and the bat corona virus transferring to humans in 2002, known now as SARS.175 These diseases can be devastating to the human population, due to the lack of prior exposure, as well as the lag-time required to diagnose the disease and develop treatments. The same is true for any emerging disease, regardless of source. Early detection, identification, and mitigation are particularly critical with emerging diseases. New viruses appear on a daily basis. Viruses utilize RNA rather than DNA in the reproductive process. The RNA process is not as exact as the DNA process, and the reproductions vary in their genetics compared to the parent. This phenomenon is termed “antigenic drift,” and it makes viruses a moving target in terms of vaccination and treatment. As an example, there are multiple strains of the rhinovirus (the common cold) circulating at any one time. By the time a rhinovirus has passed through a given population, it will be genetically different than the strain that touched off the contagion. Early medical care, diagnosis, and treatment are particularly critical when dealing with newly emerging diseases that are more dangerous than the rhinovirus, such as hemorrhagic viruses like the Ebola virus. These viruses have an extremely high mortality rate, as high as 90 percent in some cases,176 and for many there are no known cures. When there are no cures for such deadly diseases early identification and quarantine become the primary management tools. Increased health insurance coverage makes the U.S. better positioned to find and manage emerging diseases earlier on in an outbreak. The same holds true for the health surveillance system as it relates to food safety: an increase in the number of Americans with health insurance is likely to increase the health surveillance system’s ability to help us in spotting food-safety issues. More insured people will seek medical care earlier on, which allows the surveillance system to pick up on patterns sooner.

#### Infectious disease causes extinction

Casadevall 2012 - Department of Microbiology and Immunology and theDivision of Infectious Diseases of the Albert Einstein College of Medicine  
Arturo, "The future of biological warfare," Volume5, Issue5, Thematic Issue: Bioterrorism Research September 2012 Pages 584-587

Existential threats to humanity

In considering the importance of biological warfare as a subject for concern it is worthwhile to review the known existential threats. At this time this writer can identify at three major existential threats to humanity: (i) large-scale thermonuclear war followed by a nuclear winter, (ii) a planet killing asteroid impact and (iii) **infectious disease**. To this trio might be added climate change making the planet uninhabitable. Of the three existential threats the first is deduced from the inferred cataclysmic effects of nuclear war. For the second there is geological evidence for the association of asteroid impacts with massive extinction (Alvarez, 1987). As to an existential threat from microbes **recent decades have provided unequivocal evidence for the ability of certain pathogens to cause the extinction of entire species**. Although infectious disease has traditionally not been associated with extinction this view has changed by the finding that a single chytrid fungus was responsible for the extinction of numerous amphibian species (Daszak et al., 1999; Mendelson et al., 2006). **Previously**, the view that infectious diseases were not a cause of extinction was predicated on the notion that many pathogens required their hosts and that some proportion of the host population was naturally resistant. However, **that calculation does not apply to microbes that are acquired directly from the environment and have no need for a host**, such as the majority of fungal pathogens. For those types of host–microbe interactions **it is possible for the pathogen to kill off every last member of a species without harm to itself**, since it would return to its natural habitat upon killing its last host. Hence, from the viewpoint of existential threats environmental microbes could potentially **pose a much greater threat to humanity than** the **known pathogenic microbes**, which number somewhere near 1500 species (Cleaveland et al., 2001; Taylor et al., 2001), especially if some of these species acquired the capacity for pathogenicity as a consequence of natural evolution or bioengineering.

## NATO Unity Advantage Extensions

### NATO Unity Low/Collapsing

#### Hungarian ties with Russia are deepening – Ukrainian support sits badly with them.

Yana Dlugy 6-16 [Yana Dlugy is a contributing writer with the Briefings team at The New York Times, and has reported from abroad for more than 20 years. She has been on several postings in Moscow, including for Newsweek and Agence France-Presse, and has also been based for AFP in Kyiv, the Middle East and Europe. “European Leaders Offer Support”. June 16, 2022. https://www.nytimes.com/2022/06/16/briefing/russia-ukraine-war-eu-france-germany-italy-hungary.html]

Transcarpathia, in western Ukraine, is home to 150,000 ethnic Hungarians. The region ended up within Ukraine after centuries of European conquests and often cruel border adjustments. (When I reported from Ukraine, I wrote about the village of Selmentsi that was cleaved in half in 1945, separating families and friends. It wasn’t until 2005 that a border crossing through the village was opened.) The community’s kinship with Hungary, which lies just to the south, has contributed to its ambivalence about the war and to tensions with fellow Ukrainians, my colleague Erika Solomon reports. Hungary’s leader, Viktor Orban, is President Vladimir Putin’s closest ally in the E.U. and the Hungarian broadcasts that most people watch in Transcarpathia are often sympathetic to Moscow’s version of events. In this poor region, Orban has given funding for schools, churches, businesses and newspapers. He has also encouraged Hungarians to claim citizenship. Tensions have been rising for years. After Russia annexed Crimea in 2014, Ukrainian nationalists marched through the city of Uzhhorod with chants of “Magyars to the knife,” referring to Hungarians. A Hungarian cultural center in the city was set ablaze twice in 2017. Authorities said they believe Moscow was behind the provocations. Some ethnic Hungarians in Transcarpathia feel loyal to Ukraine, but say they owe their livelihoods to Hungarian funding. “When we go to Hungary, we feel like Ukrainians,” Zoltan Kazmér said. “When we are in Ukraine, we feel like Hungarians.”

#### Turkish resistance to accepting Finland and Sweden into NATO is causing rifts with the US and other NATO member states – Russian arms sales create defence system disunity.

Umut Uras 5-17 [Umut Uras is a senior producer with experience covering the Cyprus dispute, Turkish politics and EU affairs. “Why does Turkey oppose Finland and Sweden’s NATO membership?”. May 17, 2022. https://www.aljazeera.com/news/2022/5/17/why-turkey-opposes-finland-and-swedens-nato-membership]

Erdogan on Monday accused the two Nordic countries of backing “terrorism”. “Neither of these countries have a clear, open attitude towards terrorist organisations,” Erdogan said, referring to the Kurdistan Workers’ Party (PKK), which Ankara has designated a “terrorist group”, and other armed Kurdish groups active in Turkey and its periphery. “How can we trust them?” On the same day, Foreign Minister Mevlut Cavusoglu slammed Finland and Sweden for not extraditing suspects wanted in Turkey despite Ankara’s requests. The wanted individuals were either accused of having links to the PKK or to the Gulen movement, which is blamed by Turkey for a 2016 coup attempt that killed hundreds of people. In response, the Finnish foreign minister, Pekka Haavisto, said that while he was surprised at Turkey’s stance, he did not want to “bargain” with Ankara. Erdogan also targeted Stockholm in his remarks for its arms sanctions against Turkey. Sweden has frozen arms sales to Turkey since 2019 over Ankara’s military operation in neighbouring Syria. The Turkish military has carried out several cross-border operations in Syria since 2016, targeting ISIL (ISIS) and Kurdish fighters seen as “terrorists” by Ankara. Turkey controls swaths of territory in northern Syria and has been accused by some NGOs of forcing out local residents.

Mensur Akgun, professor of international relations at Istanbul’s Kultur University, told Al Jazeera that Ankara has also sought to use Sweden and Finland’s membership bid as leverage to fix the pressing issues it has with the United States, a staunch supporter of the bids. “Ankara has been under US sanctions over F-35 fighter jets and is not happy about it,” Akgun said. Turkey’s purchase of the Russian S-400 defence system has been one of the key issues that have strained relations between Turkey and the US in recent years. In July 2019, the US removed Ankara from its key F-35 fighter jet programme days after Turkey received the first delivery of the Russian S-400s. The US and NATO allies say the use of a Russian missile defence system by a NATO member is dangerous for NATO’s own defence systems, but Turkey says it decided to buy the missile system after then-President Barack Obama’s administration stalled on a sale of the US Patriot air defence system, widely used by NATO member states. Turkey has also condemned Washington’s support for armed Kurdish groups in Syria. The US recognises the PKK as a “terrorist” organisation but has militarily and politically supported the Kurdish People’s Protection Units (YPG), a Syrian offshoot of the former, particularly during the height of the fight against ISIL in the 2010s.

#### Turkish-Greek disputes in the Aegean Sea are disunifying relations within the southern NATO block – meetings collapsing now.

Daily Sabah 6-15 [Turkish based news organization. “NATO urges Turkey, Greece to resolve disagreements over Aegean”. June 15, 2022. https://www.dailysabah.com/politics/diplomacy/nato-urges-turkey-greece-to-resolve-disagreements-over-aegean]

Stoltenberg's comments came two weeks after President Recep Tayyip Erdoğan declared Turkey would no longer participate in regular high-level meetings with Greek leaders intended to foster cooperation between the two countries. Erdoğan raised the stakes last week, warning Greece to demilitarize its Aegean islands and saying he was “not joking.” He spoke during Turkish wargames near the Greek islands that included an amphibious landing scenario. Greek Prime Minister Kyriakos Mitsotakis responded that he would not engage in a "ping-pong" of personal insults with Erdoğan. The two NATO allies have long been at odds over a number of issues including offshore rights, ownership of uninhabited islets, competing claims over jurisdiction in the Eastern Mediterranean, overlapping claims over their continental shelves, maritime boundaries, airspace, energy, the ethnically split island of Cyprus, the status of the islands in the Aegean Sea and migrants. They have come close to war three times in the past half-century, while NATO stepped in when a dispute over drilling rights for potential oil and gas deposits in the Eastern Mediterranean Sea led to a tense naval standoff in the summer of 2020. Turkey says Greece is stationing troops on islands in the Aegean in violation of peace treaties signed after the World Wars, demanding that Greece demilitarize its eastern islands, citing the 20th-century treaties that ceded sovereignty of the islands to Greece. Greece counters that the islands need defenses given threats of war from Turkey, which has NATO's second-biggest military and maintains a large landing fleet on its Aegean coast. Turkey in recent months has stepped up criticism of Greece stationing troops on islands in the eastern Aegean, near the Turkish coast and in many cases visible from shore. These islands were required to be demilitarized under the 1923 Treaty of Lausanne and the 1947 Treaty of Paris, so any troops or weapons on the islands are strictly forbidden.

### Cyber Disunity Internals

#### Russian cyber warfare is undermining NATO decision-making and unity

Franz-Stefan Gady 21, Research Fellow for Cyber, Space and Future Conflict, International Institute for Strategic Studies. “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro. Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus. This publication is the result of the Conference “NATO Decision-making: promises and perils of the Big Data age”, organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. <https://www.iai.it/sites/default/files/978195445000.pdf> //pipk

This chapter seeks to offer preliminary answers to two questions. First, to what degree will Artificial Intelligence (AI)-enabled information warfare exacerbate hybrid threats to NATO decision-making? Second, what can NATO countries do to alleviate the threat? To narrow the research scope, this chapter will principally look at threats posed by Russian AI-enabled information warfare operations under the concept of gibridnaya voyna. The study argues that given that AI-enabled information warfare has the potential to amplify societal polarization, elite disagreement within domestic politics, and reshape the perception of the “Russian threat” in NATO member countries, it can have a direct negative impact on national and NATO decision-making. Such operations, however, only amplify existing symptoms of polarization and disagreement found within NATO member states and are not their root causes. The chapter concludes that NATO must better integrate tech-centric so-called “whack-a-troll” tactics with a whole-of-nation strategy to better safe-guard NATO decision-making and alliance cohesion. Renewed discussion of whole-of-society defense concepts to inform national security strategies may be useful in this regard.

Introduction NATO defines hybrid threats as threats that “combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces” (2019). Such hybrid methods are used to blur the line between war and peace and “attempt to sow doubts in the minds of target populations.” NATO further emphasizes that “[t]he speed, scale and intensity of hybrid threats have increased in recent years.” The latter can partially be traced back to various technological advances including in the fields of Artificial Intelligence (AI) and offensive cyber capabilities, utilized in conjunction with deliberate attempts by competitor nations to undermine the political cohesion of NATO member states from within.

Hybrid threats pose a number of unique challenges to political decision-making within both NATO member states and the Alliance’s various deliberative bodies, where decisions are based on the principle of consensus preceded by consultation processes (NATO, 2020). In particular, meddling by outside powers in political processes by means of influence operations, broadly defined as “organized attempts to achieve a specific effect among a target audience,” is one of the top concerns of NATO leadership (Thomas et al., 2020). In particular, Russian tactical-operational influence operations under the concept of gibridnaya voyna (‘hybrid warfare’) have been receiving a great deal of attention since 2014. As Ofer Fridman notes, such operations target society at large, seeking to undermine political cohesion in an adversary state by employing methods that amplify the divisions and polarizations among its citizens (2018).

#### Hybrid cyber ops against NATO undermine cohesion through disinformation- new NATO strategy is key

Harlan Ullman, 1-30-2022, "The Russia crisis has exposed why NATO needs a strategy shift," Atlantic Council, <https://www.atlanticcouncil.org/blogs/new-atlanticist/the-russia-crisis-has-exposed-why-nato-needs-a-strategy-shift/>

**The standoff over Ukraine has underscored a pressing need for NATO. Even though NATO leaders agreed to its new military strategy of defense and deterrence** in 2019, given the events in Ukraine, **that strategy appears dated.**¶Why?¶ First, Russia has shown it is prepared to use its military in anger and certainly as a threat. And it has modernized its conventional and nuclear forces. NATO has not begun a major modernization for either its conventional or nuclear forces. And the current strategy, at least the [parts](https://www.nato.int/cps/en/natohq/news_185000.htm) of the classified guidance that have been [revealed in public](https://www.act.nato.int/articles/shape-cos-visits-act), offers rhetoric and not substantial guidance on modernization.¶ Second, while NATO created centers of excellence to deal with specific aspects of hybrid war, **the Alliance still has not produced a viable and comprehensive counter-gray area/hybrid-war strategy with corresponding capabilities. Russia calls these operations “active measures” that include cyber,** propaganda, **misinformation, disinformation, and information operations to erode the will and cohesion of NATO.**¶Third, while advanced technology has generated revolutionary advances in military capability, conversely, it also has created greater vulnerabilities—particularly in command-and-control and logistics. Effectively targeting these vulnerabilities will disrupt any offensive.¶ In the 1940 Battle for France, had British and French forces sustained air and long-range artillery attacks on the many miles of German convoys crowding major roads driving west, one of the greatest traffic jams in history would have resulted. That did not happen.¶ Fourth, while NATO spends many times more collectively on defense than Russia does, costs are rising faster than defense-spending increases for virtually every item from people to pencils to precision weapons. As an ironic result, the more is spent on defense, the more [NATO’s forces shrink in numbers](https://www.amazon.com/Ever-Shrinking-Fighting-Force-Arnold-Punaro/dp/1735911402).¶ All these factors would seemingly demand a major strategy review. The Ukraine crisis intensifies this urgency. The question is whether NATO will take note.

#### Successful Russian cyber ops undermine NATO cohesion by spreading disinformation that erodes political support

Oscar Jonsson in 2021

scholar of strategy, emerging technology and Russia who is founder of Phronesis Analysis and Researcher at Swedish Defence University; FROM EASTERN FLANK TO WESTERN ELECTIONS: RUSSIAN OPERATIONS AGAINST THE EU AND NATO; The Center for European Policy Analysis; https://cepa.org/the-evolution-of-russian-hybrid-warfare-eu-nato/

The conduct of modern conflict is constantly developing with organizational and technological innovation, and through interactions with the participants. Russia’s leadership has notably had a more difficult task as the world has become more aware of its nonmilitary influence since the 2016 U.S. presidential election. The big technology companies — Facebook, Twitter, and Google — also seem to have woken up to the fact that they are key arenas for the information conflict, and have started to take countermeasures. On the other hand, hybrid warfare still favors the attacker as few costs are imposed. Moreover, the conditions for such warfare were particularly favorable during the Trump presidency and the higher demand for information in the pandemic.¶ It is critical to put Russian influence operations in perspective. It is incorrect to dismiss them as unsuccessful simply because both NATO and the EU are intact, or because many of the posts coming from the IRA have low viewership and low levels of interaction. In fact, Russia, starting from a limited power position, is attempting to impact the world’s most powerful political union, the EU, and the world’s most powerful military alliance, NATO, by using relatively cheap means.¶ Moreover, the aggregate impact of flooding the media with fake news is often bigger and more important than interactions with individual pieces of content. This can be seen in a study of the media landscape in Michigan in the lead up to the 2016 U.S. presidential election. It found that sensational and conspiratorial material as well as fake news was shared a lot more on social media than well-researched news, the proportion of well-researched news being shared was the lowest ever the day before the election, and that Trump-related hashtags by far surpassed Clinton-related ones.33¶ That being said, Russian disinformation attempts can hardly be so effective as Trump himself stating that it would be the most fraudulent election ever.34 Nonetheless, it is lazy analysis to simply state that Trump was more harmful than foreign meddling as that is a false dichotomy. More correctly, the most effective influence operations have always been about exploiting existing divisions and local actors. For example, Trump described Montenegro as “very aggressive” and said that defending it would lead to World War III.35 The question is, where did those views originate? It is hard to believe that they originated from U.S. intelligence briefs. That narrative was only being pushed by the Russian disinformation machinery. This illustrates the fact that the impact of disinformation cannot merely be measured through Facebook interactions, it can also be seen in a president’s comments that draw either directly from Russian sources or, more likely, from sources that are susceptible to Russian disinformation.¶ Even if Russian influence operations in 2016 did not sway a single voter, they sharpened the polarization in U.S. politics and society. This was manifested in the country being tied up for years in debates on the extent of collusion by the Trump campaign with the Russians and impeachment procedures.¶ The threat from Russian influence operations remains real, even though they are, by their very nature, unlikely to have an immediate or obvious impact. The EU and NATO are dependent on political support from their member states. In these states, there is some opposition to both institutions that can be amplified and exploited by malign Russian actors.

#### Cyber ops are key to Russia’s revisionist strategy by undermining support for Western governments

Oscar Jonsson in 2021

scholar of strategy, emerging technology and Russia who is founder of Phronesis Analysis and Researcher at Swedish Defence University; FROM EASTERN FLANK TO WESTERN ELECTIONS: RUSSIAN OPERATIONS AGAINST THE EU AND NATO; The Center for European Policy Analysis; https://cepa.org/the-evolution-of-russian-hybrid-warfare-eu-nato/

The cyber domain is another area which holds a lot of promise for a revisionist power like Russia to offset a more prosperous and superior West. Russia is skilled at combining the use of different domains of influence. It is a sophisticated cyber actor that has the “full range of capabilities for undertaking actions in cyberspace …. It implements a very advanced offensive program.”29 These capabilities were shown in Russia’s interference in the 2016 U.S. presidential election and are a reminder that the most significant impact of its operations was not through fake social media accounts, but the hack-and-leak operation against the Democratic National Committee (DNC), which started with a cyber intrusion.30 U.S. intelligence agencies concluded that the DNC hack sought “to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump.”31¶ Following the exposure of its meddling, including by the Mueller report, Russia improved its modus operandi with increased operational security and more stealthy operations.32¶ This included “a partly successful attempt to interfere, via hack-and-leak, in the French presidential elections of 2017 and almost certainly in the United Kingdom in 2019.”28

### China Internal

#### China is also increasing attacks on NATO members.

Conklin ’22(Audrey Conklin is a digital reporter for FOX Business and Fox News. “Chinese cyberattacks on NATO countries increase 116% since Russia’s invasion of Ukraine: study”; Fox Business; March 26, 2022, <https://www.foxbusiness.com/technology/chinese-cyberattacks-nato-increase-ukraine>)

Cyberattacks against NATO countries originating from Chinese IP addresses have increased 116% since Russia invaded Ukraine on Feb. 24, new research shows. Cyberattacks from Chinese IPs have also risen 72% worldwide, according to trends analyzed before and after Russia's invasion of Ukraine by cybersecurity firm Check Point Research. "As the Russia-Ukraine conflict intensifies, we grew curious around cyber attacks originating from China. We’re seeing significant increases in cyber attacks that originate from Chinese IP addresses," Omer Dembinsky, data group manager at Check Point Software, the software arm of Check Point, said in an emailed statement. He noted that while Check Point researchers cannot attribute the attacks to the Chinese government, "as it is difficult to determine attribution in cyber security without more evidence," it is clear to researchers that "hackers are using Chinese servers to launch cyber attacks world-wide, especially NATO countries." Last week, attacks from Chinese IP addresses on countries around the globe were 60% higher than the first three weeks of the war in Ukraine. The increase in attacks from Chinese servers is also significantly higher than the increase in cyberattacks over all since Russia's invasion began, researchers noted. "The servers are likely used by hackers within China and abroad," Dembinsky said. "The trend can have many meanings. For example, the increase can indicate where it is now easy or cheap to set up and operate a service or where it is more opportune to hide the real origin of the attack. It can also indicate how global cyber traffic is being routed at this moment in time." The FBI earlier this week announced it would be partnering with the private sector to combat foreign cyberattacks against U.S. entities.

### Populism Internal

#### Populism link & internal.

Frederick et al. ’17 — Bryan; Ph.D. in international relations, Johns Hopkins University School of Advanced International Studies; M.A. in international relations and international economics, Johns Hopkins University School of Advanced International Studies; B.A. in philosophy, Williams College. Other Contributors: Matthew Povlock, Stephen Watts, Miranda Priebe, Edward Geist. 2017; “Assessing Russian Reactions to U.S. and NATO Posture Enhancements.”; *RAND Corporation*; <https://www.rand.org/pubs/research_reports/RR1879.html>; //CYang

While we assess that a Russian attack on NATO in the near-term is highly unlikely, it also seems probable that Russia will explore other avenues to signal its displeasure with ongoing U.S. and NATO posture enhancements. Russia has already announced that it intends to adjust its domestic force posture on its western borders to compensate for a larger NATO presence. In the past, Russia has used a variety of mechanisms to respond to U.S. and NATO actions that it perceives as threatening; such mechanisms include withdrawing from multilateral security treaties, sending forces for provocative out-of-area deployments in the Americas, and threatening to base Iskander missiles in Kaliningrad, among others. Other options to protest U.S. and NATO enhancements in the near-term could include targeting cross-domain areas of asymmetric concern to the United States and NATO, such as the implementation of the Iran nuclear deal, increasing support for far-right Western political parties, and cyber attacks on politically or economically sensitive Western targets

### Impact – Populism

#### Populism structurally guarantees more conflict and heightens escalation risks

Drezner 17 – PhD, Professor of Int’l Politics (Dan, “The Angry Populist as Foreign Policy Leader: Real Change or Just Hot Air?, *41 Fletcher F. World Aff. 23*, Lexis)

Leaders who rise to power in lower-probability scenarios are also likely to have a greater appetite for risk in foreign affairs. This matters, as Jeff Colgan notes: "risk tolerance leads to aggression in international affairs because it increases the perceived payoff of risky gambles." 17 Populist leaders more closely resemble revolutionaries than more established politicians. And as Colgan warns, "the ambition of revolutionary leaders also contributes to aggression. Ambition makes it more likely that a leader will reject the status quo internationally as well as domestically." 18 We can see this kind of ambition on display among elected populists. Hugo Chávez [\*30] persistently proposed radical alternatives to the Washington Consensus. One longtime friend of Viktor Orbán noted, "he has always wanted to upset the status quo, to become a change-maker." 19 Orbán himself, in a meeting with Polish Law and Justice Party head Jaroslaw Kaczynski, proposed a "cultural counter-revolution" in Europe. 20 Donald Trump's inaugural address categorically rejected the postwar liberal order, arguing in favor of an "America First" approach to international relations. Populists are therefore more likely to pursue high-risk, revisionist foreign policies. Populist leaders also care about recognition by others, and will be quick to anger if that recognition is not forthcoming. Populists build their legitimacy on their support from "their" people, but part of that support comes from displays of dominance over others. Russian president Vladimir Putin is well-known for his over-the-top efforts to look strong and powerful. These range from his shirtless photos to videos of him weightlifting to scoring eight goals in an exhibition game with former NHL All-Stars. 21 In Erdogan's first two years as Turkey's president, the government has prosecuted more than 1,800 cases of Turkish citizens insulting him--including a former Miss Turkey. 22 Donald Trump has insulted anyone who has criticized him since he started running for president, ranging from erstwhile GOP rivals to federal judges to media outlets to a former Miss Universe to Meryl Streep. When dealing with domestic rivals and critics, such displays of dominance are an easy strategy for elected leaders to pursue. Populist leaders engage in such behavior to project their strength and mastery over the political fates. It is tricky to do this on the international stage, however. Populist leaders will therefore be more concerned than most politicians about the personal respect afforded to them by others. At the international level, this leads to one of two outcomes: recognition by other heads of state, or a denunciation of leaders who fail to confer such recognition. If populists cannot exploit the respect conferred by others, they will be quick to reject and delegitimize the leaders who spurn them. We can see this kind of pattern at work in how populist leaders have reacted to setbacks on the global stage. Vladimir Putin began his tenure in office with a much warmer attitude towards the West. During the first decade of this century, however, Putin lost an ally during Ukraine's Orange Revolution, and witnessed NATO expanding to Russia's borders. It was at this point that Putin began adopting a more hostile attitude towards the West. After President Obama cancelled a meeting with Duterte, the Filipino president responded with a series of tirades insulting the American president. 23 In Trump's first week as president, he faced pushback from the [\*31] Mexican president Enrique Peña Nieto on his policies for the southern border. In response, Trump tweeted that Peña Nieto should not bother coming to Washington. The Mexican president responded by canceling his visit. Populists do not possess a monopoly on anger in politics, but most populists tend to project anger as part of their leadership style. Based on their pathway to power and their philosophy of governance, it should not be surprising that they are commonly associated with that emotion. As previously noted, populist parties do particularly well after financial crises. They are adept at exploiting the (often justified) anger that voters possess towards authorities that were in charge when the crisis happened. Former UKIP leader Nigel Farage warned of "political anger" if the United Kingdom did not follow through on Brexit. In a press conference blasting the United States, Duterte said, "If you Americans are angry with me, then I am also angry with you." 24 During one of the GOP primary debates, Donald Trump explicitly stated, "I will gladly accept the mantle of anger." Trump famously refuses to apologize when he makes controversial or problematic statements. 25 Numerous press reports suggest that Trump lost his temper with the Australian prime minister in their first phone conversation. This wave of populist anger reverses a centuries-long western effort to contain that emotion in international relations. 26 Recent scholarship on emotions in world politics suggest that sustained levels of anger carry risks in world politics. Anger was valorized in societies with strong honor cultures and warrior castes, biologically conditioning citizens towards that feeling. Furthermore, as Neta Crawford notes, "threats that evoke anger (if they are associated with perceived insults) tend to decrease the perception of a threat and simultaneously heighten risk-taking behaviors on the part of those who feel angry." 27 This is particularly true if populist leaders find ways to institutionalize anger and resentment through new laws, executive orders, or bureaucratic structures. This tendency towards angry rhetoric can be exaggerated through misperception and mistranslation. Conventional foreign policy leaders are prepped to stay within the lanes of "accepted" diplomatic discourse, so that observers can detect subtle shifts in phrasing as a foreign policy signal. In contrast, populists scorn diplomatic language as exercises in sophistry and hypocrisy. They rely on language designed to appeal to their base, which increases the likelihood that outside observers misconstrue their words. Angry tirades from leaders like Trump, Duterte, or Iran's Mahmoud Ahmadinejad have been mistranslated--and usually in a direction that [\*32] paints the leader as more bellicose than intended. 28 Populist leaders will be reluctant to correct such misperceptions, because that would require them to engage in the diplomatic discourse they have derided. Displays of righteous indignation might play well with a populist leader's domestic base. The international effect of angry outbursts, however, is to narrow the zone of cooperation between countries. If a leader unleashes an angry tirade against another country, that is sure to gain considerable public attention in both nations. This automatically raises the "audience costs" for both leaders. The larger the audience that is paying attention to any dispute, the greater the political costs a leader can suffer if they back down in that dispute. 29 Displays of temper make it harder for the populist to compromise, but it will also make it more politically difficult for the object of the tirade to make any concessions. Through effects on leaders and populations, provocations make negotiations more costly and conflict escalation more likely. 30 Perhaps the most important intellectual trait that populist leaders share is their tendency to think like hedgehogs. According to the classical Greek poet Archilochus, "a fox knows many things, but a hedgehog one important thing." Isaiah Berlin popularized that quote, arguing that intellectuals could be divided into foxes and hedgehogs. This works for decision-makers as well. Foxes will possess the necessary metacognition to adapt to new facts and new circumstances; hedgehogs will rely on their core beliefs, fitting the world into their preexisting worldview. 31 Populists are hedgehogs: the one big thing that they know is to reject the elites and technocrats who heretofore governed their country. As Philip Tetlock observed more than a decade ago, foxes and hedgehogs have different strengths when it comes to thinking about the world. 32 Foxes are much better than hedgehogs in their predictive accuracy about world events; simply put, foxes are better at incorporating new information and updating how they think about the world. Hedgehogs are better than foxes at anticipating big and unexpected events happening in the world, such as the collapse of the Soviet Union, the 9/11 terrorist attacks, and the 2008 financial crisis. Anticipating those events requires an assuredness about the way the world works that hedgehogs are more likely to possess. The effects of these different intellectual styles on foreign policy are straightforward. As hedgehogs, populists are more likely to have their expectations confounded in world politics. At the same time, populist foreign policy leaders will face psychological and domestic political barriers to admitting error or reversing a failing policy. Any public recognition of a misstep demonstrates a leader's fallibility--which is problematic for leaders [\*33] who claim that they can divine the general will of the people. At the same time, as hedgehogs, populists will be reluctant to take any action that deviates from the way that they think the world works. Stepping back, we can proffer some tentative predictions of how populist foreign policy leaders will behave in the coming years. Populist foreign policy leaders are likely to reject the pre-existing liberal international order and espouse a strong form of ethnic nationalism. They might try to create alternative international arrangements to the status quo, but these efforts are likely to be Potemkin efforts, with more pomp and circumstance than substance. Populist leaders will have greater appetites for risk and ambition on the global stage. These heads of state will crave recognition from their fellow world leaders, and be quick to anger if they are spurned in this area. These displays of anger could become institutionalized and will increase the audience costs of all the involved actors, making cooperation less likely. And populists are less likely to correctly perceive how the world works, and more likely to hold firm with policies that are not viewed as working terribly well. One disturbing conclusion to draw from this particular constellation of traits is that populist leaders are more likely to foment international crises. Breaking with pre-existing global governance structures can guarantee a crisis escalation. An international crisis can trigger rally-round-the flag effects within the domestic population and make it easier for a leader to suppress domestic dissent. At the extreme, one could envision populists threatening or launching diversionary wars to appeal to a nationalist base in times of trouble. Vladimir Putin employed this tactic. In early 2014, he was still reeling from protests over his return to the Russian presidency, and a slowdown in the Russian economy. He responded by annexing the Crimea after the fall of his ally in Ukraine, and bankrolling a secessionist conflict in Eastern Ukraine. These efforts caused his public support to skyrocket even though the Russian economy contracted in 2014 and 2015. It should be stressed that these are all probabilistic statements. Many of these traits are hardly unique to populists; other heads of state are likely to display some subset of these leadership traits. Still, this combination of [\*34] attributes suggest that the world is experiencing an increase in the number of revisionist, risky, and violent actions in world politics.

### Impact – Laundry List

#### NATO is key to solving the biggest threats to global security

Burns ’18 (Nicholas Burns - a former under secretary of state and ambassador to NATO, teaches diplomacy and international relations at Harvard. “What America Gets Out of NATO.” The New York Times. 7/11/18. https://www.nytimes.com/2018/07/11/opinion/what-america-gets-out-of-nato.html?)

Donald Trump prepared for this week’s NATO summit by doing what no president had done before — making a case that the alliance is a bad deal for the American people. Last week in Great Falls, Mont., he said that he had told Chancellor Angela Merkel of Germany, “I don’t know how much protection we get by protecting you.” Mr. Trump has been even tougher on the European Union, branding it “as bad as Nafta” and adding, “Sometimes our worst enemies are our so-called friends.” I have visited four European countries during the last two weeks, and it has been shocking to see how far from grace the United States has fallen in the eyes of its allies. European leaders point to Mr. Trump’s support for anti-democratic populists in Hungary, Poland and Italy. They view his recent Twitter attack on Ms. Merkel as a transparent attempt to push her from office. Many fear he may now remove American sanctions against Moscow over its occupation of Crimea after his meeting with President Vladimir Putin of Russia in Finland next week. Confidence in Mr. Trump has plummeted so much that the German foreign minister, Heiko Maas, recently grouped “Donald Trump’s egotistic policy of America First” along with Russia and China as global concerns. None of this, of course, is likely to disturb Mr. Trump, who remains steadfast in his belief that whatever benefits the United States gained from the trans-Atlantic alliance in the past, the country no longer profits. But he’s wrong — there are compelling reasons that NATO in particular will be a distinct advantage for America’s security far into the future. First, NATO’s formidable conventional and nuclear forces are the most effective way to protect North America and Europe — the heart of the democratic world — from attack. Threats to our collective security have not vanished in the 21st century. Mr. Putin remains a determined adversary preying on Eastern Europe and American elections. NATO is a force multiplier: The United States has allies who will stand by us, while Russia has none. And while it’s true that most of America’s NATO allies need to increase their defense spending under the treaty, they’re not freeloaders: The United States has relied on NATO allies to strike back against Al Qaeda in Afghanistan and the Islamic State in the Middle East. European troops have replaced American soldiers in peacekeeping missions in Bosnia and contribute the large majority in Kosovo. Our NATO allies are also getting better about contributing their fair share. They have increased their defense spending by a total of more than $87 billion since Mr. Putin annexed Crimea in 2014. Fourteen more allies will reach NATO’s military spending target — 2 percent of gross domestic product — by 2024. Mr. Trump would be smart to claim credit for this at this week’s summit. A second reason for maintaining the trans-Atlantic alliance is America’s economic future. The European Union is our country’s largest trade partner, and its largest investor. The United States and the European Union are the world’s two largest economies, and can steer global trade to their advantage if they stick together. More than four million Americans work for European companies in the United States. Forty-five of the 50 states export more to Europe than to China. Mr. Trump is right that the two sides are also economic competitors, and trade disputes are inevitable. His predecessors kept this tension in balance lest there be damaging consequences for American businesses, workers and farmers — a good reminder for Mr. Trump, whose ill-conceived trade war with Canada and Europe risks harming the American economy. Third, future American leaders will find Europe is our most capable and willing partner in tackling the biggest threats to global security: climate change; drugand cybercrime cartels; terrorism; pandemics and mass migration from Africa and the Middle East. And America’s NATO allies will continue to be indispensable in safeguarding democracy and freedom, under assault by Russia and China.

#### NATO alliance is key to the economy and solve global security issues – terrorism, climate change, and pandemics

**Burns**, former American NATO ambassador, July 11, **18** (Nicholas, “What America Gets Out of NATO”, <https://www.nytimes.com/2018/07/11/opinion/what-america-gets-out-of-nato.html>) DR

None of this, of course, is likely to disturb Mr. Trump, who remains steadfast in his belief that whatever benefits the United States gained from the trans-Atlantic alliance in the past, the country no longer profits. But he’s wrong — there are compelling reasons that NATO in particular will be a distinct advantage for America’s security far into the future. First, NATO’s formidable conventional and nuclear forces are the most effective way to protect North America and Europe — the heart of the democratic world — from attack. Threats to our collective security have not vanished in the 21st century. Mr. Putin remains a determined adversary preying on Eastern Europe and American elections. NATO is a force multiplier: The United States has allies who will stand by us, while Russia has none. And while it’s true that most of America’s NATO allies need to increase their defense spending under the treaty, they’re not freeloaders: The United States has relied on NATO allies to strike back against Al Qaeda in Afghanistan and the Islamic State in the Middle East. European troops have replaced American soldiers in peacekeeping missions in Bosnia and contribute the large majority in Kosovo. Our NATO allies are also getting better about contributing their fair share. They have increased their defense spending by a total of more than $87 billion since Mr. Putin annexed Crimea in 2014. Fourteen more allies will reach NATO’s military spending target — 2 percent of gross domestic product — by 2024. Mr. Trump would be smart to claim credit for this at this week’s summit. A second reason for maintaining the trans-Atlantic alliance is America’s economic future. The European Union is our country’s largest trade partner, and its largest investor. The United States and the European Union are the world’s two largest economies, and can steer global trade to their advantage if they stick together. More than four million Americans work for European companies in the United States. Forty-five of the 50 states export more to Europe than to China. Mr. Trump is right that the two sides are also economic competitors, and trade disputes are inevitable. His predecessors kept this tension in balance lest there be damaging consequences for American businesses, workers and farmers — a good reminder for Mr. Trump, whose ill-conceived trade war with Canada and Europe risks harming the American economy. Third, future American leaders will find Europe is our most capable and willing partner in tackling the biggest threats to global security: climate change; drug and cybercrime cartels; terrorism; pandemics and mass migration from Africa and the Middle East. And America’s NATO allies will continue to be indispensable in safeguarding democracy and freedom, under assault by Russia and China. Mr. Trump’s campaign to undermine the European Union and diminish America’s leadership in NATO serves none of these interests. He seems driven by resentment about European trade surpluses and low defense budgets, issues that blind him to all the other benefits Americans derive from our alliance with Europe and Canada. Mr. Trump may believe his blistering attacks on Europe’s trade policies and defense budgets are a good negotiating tactic before the summit. But in fact they have already done enormous damage. While **he cannot** outright **kill NATO** — the American public and Congress support it too strongly — he has eroded significant levels of trust and good will. As it became clear during my recent visits across Europe, a dangerous breach has opened in the trans-Atlantic alliance — by far the worst in seven decades. Mr. Trump wants Americans to believe that their allies are simply taking advantage of them. On Sept. 11, 2001, I witnessed a far different reality as American ambassador to NATO. Canada and the European allies volunteered within hours of the attacks to invoke Article 5 of the NATO treaty, which compels all members to respond to an attack on any single member, for the first time in history. They came to our defense when we most needed them. They sent troops to fight with us in Afghanistan. They are still there with us 17 years later. Are we now going to throw off that mutual protection, and go it alone in a dangerous 21st-century world? That would be a historic mistake. But that is where we may find ourselves if Mr. Trump’s anti-Europe vendetta continues.

#### NATO is key---it’s a full-spectrum force multiplier and guarantees multilateral logistics

Weinrod 16 - Former Secretary of Defense Representative Europe and Defense Advisor to the U.S. Mission NATO (W Bruce, “We Still Need NATO,” The American Interest, https://www.the-american-interest.com/2016/01/15/we-still-need-nato/)

Not only does NATO remain relevant, but more importantly it continues to support and advance U.S. security interests—though again, often in ways that do not make headlines and that casual observers rarely appreciate in full. Most fundamentally, NATO provides a standing multilateral military capability that can deter or be deployed should a significant security threat arise. Because NATO has a military capability in place, the core elements for mobilization, deployment, and sustainment of substantial multilateral military forces already exist. The ongoing training, exercises, and regular communication among the national militaries of NATO members allows them to jump-start preparations and actions when needed without very lengthy preparatory work. This can allow the U.S. government to proceed in shaping and leading military coalitions more quickly, at less cost and with greater effectiveness, than if NATO did not exist and its functional equivalent had to be invented from scratch at a moment’s notice. While the U.S. government retains the capacity and the right to act unilaterally if and when necessary, it makes sense for it to act with others whenever possible, whether through NATO or ad hoc coalitions of the willing. A multilateral framework can provide both political cover and military resources, and the United States very much can benefit from both. The United States also benefits significantly from NATO’s logistics capabilities. Pontificating about grand strategies sounds impressive, but for military effectiveness and success, logistics capabilities are what really count. For example, while NATO did not formally participate in the 1991 Gulf War, NATO resources, supplies, bases, and other infrastructure provided crucial support prior to and during the U.S.-led coalition military action to force Saddam Hussein out of Kuwait. The coalition in effect borrowed NATO capacities already in existence, and benefitted greatly from equipment compatibility and common training and resources. Other coalitions of the willing assembled under U.S auspices and utilizing NATO resources can follow the same approach. In addition, the U.S. government has access to the numerous military facilities and resources that member nations make available to NATO. A good example is Incirlik Air Base in Turkey, now being used against ISIS in what is not a formal NATO operation. As importantly, working through NATO usually makes it relatively routine for host governments to agree to U.S. requests to use facilities within their territory for military-related purposes. Without NATO, in order to fulfill its security responsibilities, the U.S. government would need to develop and maintain a complex network of bilateral and multilateral security agreements and arrangements that would seek to maintain the kind of connectivity and flexibility that NATO already provides. Further, the U.S. government would need not only agreements to access such military facilities but also would likely need to obtain specific approval from the host nation for each use and perhaps even in some cases legislative approval. In general, it is much simpler, faster, and easier politically and otherwise for nations to grant the United States the use of their facilities within a NATO framework than it would be to have to grant permission to the United States on their own. Over recent decades NATO has, as noted above, developed a global security network that reflects formalized relationships with non-NATO nations. For the United States, this brings the advantage that it can work through NATO to develop or enhance security relationships with states that belong to the PFP, the MD, the ICI, and NATO bilateral security relationships. Working through NATO provides an extra dimension to U.S. efforts to enhance the military capacities of friends and allies in various regions who, with training and assistance, can provide supplementary support to NATO or U.S.-led operations. NATO also supports U.S. interests by providing a multilateral framework for a U.S. presence in nations where the U.S. government wishes to help train and also enhance its military contacts, but where unilateral U.S. military involvement might be politically contentious.

### Impact – Democracy

#### Democracy solves extinction

Carla Zoe Cremer & Luke Kemp 21, The Future of Humanity Institute, Oxford. Centre for the Study of Existential Risk, Cambridge. "Democratising Risk: In Search of a Methodology to Study Existential Risk" <https://arxiv.org/ftp/arxiv/papers/2201/2201.11214.pdf> //pipk

There is an intimate and neglected relationship between existential risk and democracy. Democracy must be central to efforts to prevent and mitigate catastrophic risks. It is also an antidote to many of the problems manifest in the TUA. Do those who study the future of humanity have good grounds to ignore the visions, desires, and values of the very people whose future they are trying to protect? Choosing which risks to take must be a democratic endeavour. We understand democracy here in accordance with Landemore as the rule of the cognitively diverse many who are entitled to equal decision-making power and partake in a democratic procedure that includes both a deliberative element and one of preference aggregation (such as majority voting)45,115. Decision-making procedures are not either democratic or non- democratic, but instead lie on a spectrum. They can be more or less democratic, inclusive, and diverse. We posit three reasons for why we should democratise research and decision-making in existential risk: the nature of collective decision-making about human futures, the superiority of democratic reason, and democratic fail-safe mechanisms. Avoiding human extinction, or crafting a desirable long-term future, is a communal project. Scholars of existential risk who take an interest in the future of Homo sapiens are choosing to consider the species in its entirety. If certain views are excluded, the arguments for doing so must be compelling. Democracy will improve our judgments in both the governance and the study of existential risks. Asking how our actions today influence the long-term future is one of the most difficult intellectual tasks to unravel, and if there is a right path, democratic procedures will have the best shot at finding it. Hong and Page116,117 demonstrate both theoretically and computationally that a diverse group of problem-solving agents will show greater accuracy than a less diverse group, even if the individual members of the diverse group were each less accurate. Accuracy gains from diversity trump gains from improving individual accuracy. Landemore115, builds on this work to advance a probabilistic argument that inclusive democracies will, in expectation, make epistemically superior choices to oligarchies or even the wise few. This is supported by promising results in inclusive, deliberative democratic experiments from around the world 118. In the long run, democracies should commit fewer mistakes than alternative decision-making procedures. If this is true, it should improve the accuracy of research efforts and decision-making. We are more likely to make accurate predictions about the mechanisms of extinction, probable futures, and risk prevention if the field invites cognitive diversity, builds flat institutional structures, and avoids conflicts of interest. Thereare many ways to consider the interests of the many. Democratic assemblies could allow global citizens to deliberate about the futures they prefer, citizens could be surveyed, and the field of ERS itself could be diversified. At the moment, the field is, as many academic disciplines are, unrepresentative of humanity at large and variably homogenous in respect to income, class, ideology, age, ethnicity, gender, nationality, religion, and professional background. The latter issue is particularly true of existential risk, which, despite being an inherently interdisciplinary endeavour, is at the highest levels dominated by analytic moral philosophers. We need to be vigilant to what perspectives are not represented in the study of existential risk. An awareness of bias will go some way towards mitigating its negative effects. To get close to replicating the cognitive diversity found among humans, we must begin by inviting different thinkers with different values and beliefs into the field. Democracies can limit harms. Any approach to mitigating existential threats could create response risks, and the TUA seems particularly vulnerable to this. Despite good intentions and curiosity-driven research, it could justify violence, dangerous technological developments, or drastically constrain freedom in favour of (perceived) security. If we hope to explore ideas but minimise harms, democracies can be used to moderate the measures taken in response to harmful ideas. It seems, for example, vanishingly unlikely that a diverse group of thinkers or even ordinary citizens would entertain the idea of sacrificing 1 billion living, breathing beings for an infinitesimal improvement in reaching an intergalactic techno-utopia. In contrast, the TUA could recommend this trade-off. The democratic constraint of extreme measures may simply be a form of collective selfinterest. Voters are unlikely to tolerate global catastrophic risks (GCRs), which incur the death of a sizeable portion of the electorate, if they know they themselves could be affected. We expect that scholars who do not support sacrificing current lives in the name of abstract calculations, but would still like to explore the use of expected value theory in existential risk, will be in support of democratic fail-safe mechanisms. Empirically, this fail-safe mechanism seems to work. Even deeply imperfect democracies, like the ones we inhabit now, often avert detrimental outcomes. Democracies prevent famines 119 (although not malnutrition)120. They make war — a significant driver of GCRs — less likely 121. The inclusion of diverse preferences in democracies, such as those achieved through women’s suffrage, further decreases the likelihood of violent conflict 122. Citizens often show a significant risk aversion in comparison to their government. While surveys are notoriously difficult to collect and interpret, existing data suggest that the public has little support for nuclear weapons use 123–125, but strong support for action against climate catastrophe 126–128. We can further show that when citizens deliberately engage with the subject at hand, their concern and readiness for action often increases 118. For example, citizen assemblies on climate change have recommended widespread policy-changes across sectors, amendments to incentive structures and laws against ecocide to reach emissions targets 129. Indeed, many lament that when it comes to genetically modified organisms and nuclear power, citizens are far too riskaverse130 . The problem is not that the public is riddled with cognitive biases that make them unconcerned about global catastrophes. Democratic debate cannot be an afterthought. Navigating humanity through crises will involve many value-laden decisions under deep uncertainty. Democratic procedures can deal with such hard choices. Greater cognitive diversity should be represented amongst scholars of ERS. Recommendations on policies that would reduce risk should be passed through deliberative assemblies and await the approval of a wider pool of ordinary citizens, as they will be the ones who will bear this risk. A homogenous group of experts attempting to directly influence powerful decision-makers is not a fair or safe way of traversing the precipice.

### Impact – Solves China

#### NATO cohesion is key to maintain US hegemony and influence globally against a rising China

Ben Hodges in 2018

Lieutenant General (ret.) Ben Hodges, Pershing Chair in Strategic Studies, Center for European Policy Analysis, Former Commanding General, U.S. Army Europe; Why the United States Needs a Cohesive NATO; The German Marshall Fund of the United States (GMF); is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together; https://www.gmfus.org/news/why-united-states-needs-cohesive-nato

If a conflict with China arises, the United States will need a strong, cohesive NATO, as well as other partnerships around the world to maintain order and security in Europe’s neighborhood, and perhaps even beyond. The United States remains committed to Europe’s security and stability. But it also expects its European allies to pick up their share of the burden for collective security so as to help maintain order in the continent and around the globe. It is of vital importance to the United States that its defense and security relationship with European countries, especially within NATO, not only remains healthy but is correctly oriented to current and likely future challenges.¶ Several things remain to be achieved if Europe and the United States in this regard. First, they must build a common approach not only in defense, but across economic, information, and political domains. Second, they must solve the continued inequity in burden sharing that hinders a stronger relationship between them and erodes the confidence of many Americans in the efficacy of NATO. Third, it is necessary to achieve greater coherence on NATO’s eastern flank, particularly in the Black Sea region. Fourth, NATO must continue its efforts to improve its deterrence capability against Russia’s aggressive behavior.¶ The interests and responsibilities of the United States are global, with freedom of navigation on the seas and preservation of the global commons being prime examples. Its allies and partners benefit from these freedoms as well, but these have now come under threat, most notably in the South China Sea and with China’s growing control over much of the infrastructure of the world, particularly in Europe and Africa. The threat from China is real and growing, and if it materializes the United States will need a strong, cohesive NATO, as well as other partnerships around the world to maintain order and security in Europe’s neighborhood, and perhaps even beyond, while the majority of its forces and capabilities, particularly air and naval ones, are operating in the Pacific theater.¶ The stability, security, and economic prosperity of the United States are directly linked to that of Europe. The bulk of its global economic relationships are in North America and the European Union, and the majority of its most reliable allies and partners are in Europe. To give but one example, the shared intelligence obtained from Europe is essential to the implementation of the recently published U.S. National Defense Strategy. In this context, it is of vital importance to the United States that its defense and security relationship with European countries, especially within NATO, not only remains healthy but is correctly oriented to current and likely future challenges.

#### NATO cohesion key to US hegemony- frees up resources and provides support for global operations

Ben Hodges in 2018

Lieutenant General (ret.) Ben Hodges, Pershing Chair in Strategic Studies, Center for European Policy Analysis, Former Commanding General, U.S. Army Europe; Why the United States Needs a Cohesive NATO; The German Marshall Fund of the United States (GMF); is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together; https://www.gmfus.org/news/why-united-states-needs-cohesive-nato

A war between China and the United States is not inevitable, but the next 15 years could see the eruption of such a conflict. While this may not reach the threshold of full-scale war or a nuclear conflict, the leaders of the Chinese Communist Party (CCP) have set their country on a trajectory that will lead to a strategic situation that may result in sustained armed conflict, potentially stretching across the Pacific region, in all domains. Furthermore, the combination¶ of China’s huge population, export-oriented economy, and lack of natural resources could generate an inexorable push towards conflict.¶ The CCP leadership has emphasized the development of military capabilities that could deny the U.S. Navy access to the South China Sea, including long-range air and missile defense and anti-ship capabilities. This anti-access area denial (A2AD) capability does not depend on a large Chinese navy but instead uses well-protected, land-based systems. The creation of artificial islands in the region, most of which are already being armed and garrisoned with A2AD capabilities, are violations of international law and agreements that clearly demonstrate the CCP’s strategy and intentions.¶ Enforcement of freedom of the seas and recognized international waters by the United States and others is necessary to counter these policies. In one recent demonstration of CCP intent, there was a near-collision incident between Chinese and U.S. Navy ships, caused by unsafe and unprofessional behavior by the Chinese one. Statements by the China’s minister of defense during his recent visit to the Pentagon, including demands that the U.S. forces stay away from the articifial islands, indicate that his country will continue to push aggressively its territorial claims.¶ Meanwhile, in Europe China has become an increasingly significant and potentially divisive influence in a variety of aspects; especially in infrastructure, technology transfer, and trade. The Belt and Road Initiative has resulted in dramatic increases in Chinese investment in Europe, control of hundreds of European companies, and ownership or control of more than 10 percent of Europe’s ports.¶ These developments, and the CCP’s strategy and behavior, are cause for concern about the potential for conflict with China within the next 15 years. They also show why the United States must prepare for this eventuality.¶ During the Cold War, the United States used a “two and a half wars” framework for force structure. This was not a strategy, but rather a mechanism meant to assess how much capability and capacity its armed forces needed to deter effectively and, if necessary, win simultaneous conflicts in two different operational theaters and “hold” in a third, minor theater at the same time, for as long as necessary.¶ Today, and for the foreseeable future, the United States can no longer exercise this capability and capacity. Therefore, in the event of conflict with China, it will need a strong, cohesive NATO as well as partnerships around the world in order to continue deterring a revanchist Russia and to carry on counter-terrorism operations in the Middle East while the majority of U.S. forces and capabilities are operating in the Pacific.

## Solvency Extensions

### S – Info Sharing

#### Information sharing is the lynchpin to effective NATO cybersecurity.

Daniel & Kenway ’20 (Michael Daniel currently serves as President and CEO of the non-profit Cyber Threat Alliance (CTA). Joshua Kenway is a Cybersecurity Associate at the Cyber Threat Alliance and a Research Fellow with the Algorithmic Justice League. “Repairing the Foundation: How Cyber Threat Information Sharing Can Live Up to its Promise and Implications for NATO,” in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis,* December 2020, <https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf>)-mikee

Cyber threat information sharing has bedevilled the cyber security community for at least two decades. Faulty assumptions have prevented this fundamentally sound concept from achieving its potential. But while information sharing is a tough problem, it is not an insoluble one. If the cyber security community adopts different underlying assumptions for information sharing then the volume, quality, and utility of the exchanged information can increase. In turn, more effective, relevant information sharing will enable defenders to better understand and anticipate adversaries, develop mechanisms to disrupt adversary activities more strategically, and raise the level of cyber security across the digital ecosystem. Under these circumstances, cyber threat information sharing can finally live up to its promise to enable better cyber security for everyone. For NATO, updating programmes to reflect these revised information sharing assumptions would require significant changes to current operations. First, overcoming the technical, economic, legal, and cultural barriers to sharing relevant, actionable information across member countries and economic sectors will require sustained attention, prioritisation, and funding from NATO’s senior leadership. Absent such attention, the barriers will likely prove insurmountable. Second, NATO should build on its existing MISP [Malware Information Sharing Platform] use to create a more comprehensive system of information sharing that broadens the types of information shared and widens the number of recipients. Third, NATO should consider how to better leverage industry for technical information, while enriching that information with government-derived information about context, attribution, and intent. If NATO shifted its approach to information sharing as suggested, the Alliance would have the opportunity to assume a leadership position in this area. If not, NATO will continue to struggle to make information sharing live up to its promise.

#### Status Quo Information Sharing Is Lacking – technical data is not the only form of information that is valuable

Daniel & Kenway ’20 (Michael Daniel currently serves as President and CEO of the non-profit Cyber Threat Alliance (CTA). Joshua Kenway is a Cybersecurity Associate at the Cyber Threat Alliance and a Research Fellow with the Algorithmic Justice League. “Repairing the Foundation: How Cyber Threat Information Sharing Can Live Up to its Promise and Implications for NATO,” in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis,* December 2020, <https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf>)

The assumption that cyber threat information is equivalent or primarily composed of technical data severely limits the potential value of information sharing. Technical data, while necessary, is not the only form of information that can provide value. For example, a warning from the US Federal Bureau of Investigation (FBI) that a specific Chinese cyber group is targeting a US company with cyber-enabled theft of intellectual property would be a useful piece of non-technical intelligence for that company. Written advisories about vulnerabilities and associated patches are critical to organisations using vulnerable software or hardware; in fact, such information is far more useful to most organisations than technical data on one of the many variations of the LockerGoGo malware. The most common interpretation of information is too narrow. B. Every Organisation Should Produce and Consume Technical Data If the underlying assumption is that information sharing means technical information, then it logically follows that most policies, infrastructure, and programmes for sharing are built around the idea that most organisations should produce and consume technical information. If everyone were to collect, share, and consume such data, the thinking goes, security would improve across the ecosystem. The problem with this logic is that most organisations are lousy at collecting, producing, and consuming technical data—and always will be. Most companies do not have the capability to identify a malware binary, analyse it, and use the resulting information, nor would they know how to handle a malicious domain name. As a practical matter, this situation will not change; no country will have enough cyber security professionals for every organisation to have this capacity. Small and medium businesses do not and will not have the resources to collect, process, share, and consume technical data regularly. This limitation does not mean such organisations would not benefit from cyber threat information sharing; rather they need different information. Neither is this approach economically efficient. Most organisations do not need access to technical data in real-time. Despite the rapidly changing nature of cyber threats in a technical sense, for most organisations, cyber security requirements and best practices do not change much from day to day. 2 For example, see the Cybersecurity Information Sharing Act of 2015 (Consolidated Appropriations Act of 2016, Division N, Cybersecurity Information Sharing Act of 2015) and the Automated Indicator Sharing Program (DHS Cybersecurity and Infrastructure Security Agency, 2020). 182 In addition, not every business has in-house technical accounting or legal skills—why should cyber security be different? Current practice does not sufficiently differentiate between organisations in terms of what information they should share under what circumstances and how frequently. C. Information Sharing is Easy In January 2008, the US government started the Comprehensive National Cybersecurity Initiative (CNCI), formalising it in National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 (The White House, 2010). ‘Connect the Centers,’ one of CNCI’s twelve lines of effort, focused on information sharing with the goal of linking the US government’s cyber centres into one common operating picture; over the long-term, it was intended to incorporate the private sector. Everyone assumed that this element would be the easiest to implement and the first to be completed. However, thirteen years later, this element is arguably one part of the CNCI vision that remains unrealised as the cyber security centres are not seamlessly connected and many silos remain stubbornly in place. A similar situation has played out in the private sector with the creation of Information Sharing and Analysis Centers (ISACs). The assumption was that companies would eagerly join these organisations, share what they knew and consume the information shared by others. Yet, more than twenty years after the concept was formalised into national legislation, many sectors are just now forming an ISAC and, even in the most successful of them, the percentage of participants that actively share information is widely understood within the industry to remain low. Public sector efforts to share information with the private sector have suffered analogous problems. The US government created the Automated Indicator Sharing (AIS) programme as a free service for general businesses, but few organisations have signed up and even fewer contribute to the programme (Marks, 2018). This is unsurprising if we look at what is being shared; a US government report from 2018 suggested that just two or three out of the 11,447 indicators submitted to AIS by the Department of Homeland Security were ‘malicious and related to cyber incidents [… while] many of the indicators received were false positives or redundant information’ (DHS Office of Inspector General, 2017: p. 15). The three examples highlight that information sharing is difficult for a variety of reasons. Simply creating programmes and establishing sharing mechanisms is insufficient without addressing obstacles to sharing actionable information. These include underlying factors such as over-classification, reputational risk, and legal concerns, as well as operational hurdles around validation, standardisation, timeliness, and automation (Zibak & Simpson, 2019).

#### NATO should increase their information sharing among organizations – organizations can develop better practices and defensive measures

Daniel & Kenway ’20 (Michael Daniel currently serves as President and CEO of the non-profit Cyber Threat Alliance (CTA). Joshua Kenway is a Cybersecurity Associate at the Cyber Threat Alliance and a Research Fellow with the Algorithmic Justice League. “Repairing the Foundation: How Cyber Threat Information Sharing Can Live Up to its Promise and Implications for NATO,” in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis,* December 2020, <https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf>)

The new information sharing presumptions proposed in this chapter—careful consideration of information type and relevance, comparative advantage in information production, how to overcome existing context-specific bar- 188 riers, and how to create and maintain trust—make the cyber threat information sharing landscape far more complex than most people envision. Yet, this very complexity provides an opportunity for simplification: rather than everyone trying to share everything all the time, organizations can concentrate on the information types most relevant to them. Information sharing architectures, policies, and systems should assist organizations in focusing their information sharing activities. Although identifying all the implications is beyond the scope of this chapter, some more prominent ones are worthy of mention. Few organizations will share every type of cyber threat information. Most organizations should focus on the types of information most relevant to their business model. For example, under this paradigm, only organizations with strong technical capabilities would share technical cyber threat information: cyber security providers, telecommunications companies, Internet Service Providers (ISPs), Managed Security Service Providers (MSSPs), and large, multinational companies in critical industries. Government agencies would focus less on producing stand-alone technical indicators of compromise (IOCs), which industry has in abundance, and more on combining that information with strategic and tactical warning about specific threats, since their comparative advantage lies in their intelligence and law enforcement capabilities. Most citizens, businesses and organizations would primarily consume information about best practices and defensive measures. The focus of information sharing programs should change. Since most organizations do not need to produce or consume technical cyber threat information, government cyber security initiatives should reflect this. These programs should instead encourage most organizations to hire a cyber security vendor or MSSP. Those service providers would consume the technical, contextual, vulnerability, and exploitation information and use it to make security adjustments such as updating blacklists or prioritizing patches. Most organizations would primarily consume updates to best practice and strategic or tactical warnings. This change would make information sharing programmed more relevant and cost-effective. Information sharing programs need to build trust. Since trust is a key component for effective information sharing, programs, structures, and architectures need to build trust over time. Policies and structures should include operational processes designed to enhance confidence and trust when personal rapport among stakeholders may be lacking, particularly when programs are starting (see Sauerwein et al., 2017; Sillaber et al., 2016; Vázquez et al., 2012; Wagner et al., 2019). For example, CTA’s information sharing rules specify the nature and scope of the sharing commitment, how members should handle shared information, and what enforcement mechanisms and penalties will be applied for violating those rules. Such clarity and consistency help new members trust that other members will treat their information properly. 189 Information sharing products can incorporate more than one information type. Since the different information types are interdependent, any given sharing product can contain more than one type. For example, CTA members share technical indicators and tactical context (and occasionally attribution) through the same automated system and standard format (Cyber Threat Alliance, 2020). A more rigorous conceptual framework for information sharing does not require a rigid division among the information types from a software or process flow perspective. Reducing the number of organizations expected to share technical information would make achieving speed and scale easier. Abandoning the idea that all organizations everywhere should engage in technical cyber threat information sharing makes overcoming the barriers to technical sharing easier. Under this assumption, the number of organizations with the combination of willingness, relevance, and capability to engage in technical cyber threat sharing decreases to a large but manageable number (Aspen Cybersecurity Group, 2018). At this size, having most of these organizations participating in formal information sharing groups becomes a reasonable goal. The information sharing burden would decrease while the value would go up, increasing the likelihood that organizations voluntarily participate in such activities. By focusing sharing activities on the most relevant information types, the time and monetary investment for most organizations would decrease. At the same time, the connection between shared information and the organization’s mission or business model would become clearer, thereby increasing its value, and making that value easier to assess. The decreased burden and increased value would expand the number of organizations that participate in sharing activities. Additional standard formats for non-technical information types would emerge, along with systems to share those formats with increasing degrees of automation. On the technical side, several standard formats now facilitate automated information sharing, such as the STIX (MITRE Corporation, 2012) and MITRE’s Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) frameworks (MITRE Corporation, 2020). More rigorously dividing cyber threat information into different types would encourage other formats to emerge and organizations to adopt them. Standard formats make consumption of information easier for the recipient. Increased automation would increase speed and scale, making sharing more effective. Effective cyber threat information sharing requires planning, long-term investment, and sustained commitment. For example, technical cyber threat information sharing is not merely a matter of adopting a technical standard and installing software. It takes engineering and analytic time on an ongoing basis as well as maintenance of the technology and processes. Similarly, consuming cyber security best practices is not a one-time endeavor; organization’s must incorporate regular review and implementation into their business processes. Absent a long-term commitment from organizational 190 leadership, sharing usually withers after an initial burst of enthusiasm. Cyber security should take on the same status as other business enablers, such as accounting, legal affairs, and communications; like these areas, cyber security should be a function that all organization’s budget for and sustain over the long-term.

#### Rebuilding information networks through organized sharing is vital – effective information sharing shields from cyberattacks

Daniel & Kenway ’20 (Michael Daniel currently serves as President and CEO of the non-profit Cyber Threat Alliance (CTA). Joshua Kenway is a Cybersecurity Associate at the Cyber Threat Alliance and a Research Fellow with the Algorithmic Justice League. “Repairing the Foundation: How Cyber Threat Information Sharing Can Live Up to its Promise and Implications for NATO,” in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis,* December 2020, <https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf>)

These incorrect assumptions have undermined information sharing as an effective tool against cyber threats, yet policies, structures, and processes must be based on assumptions about the overall environment in order to function. As a replacement for the faulty assumptions explained above, this chapter proposes four alternative presumptions to enable effective information sharing. First, cyber threat information consists of multiple information types across different levels, with distinct value to different consumers, meaning that information sharing needs to be tailored and nuanced. Second, for this reason, relevance and comparative advantage should drive sharing activities. Third, effective information sharing efforts must overcome context-specific technical, economic, legal, and cultural barriers; and fourth, trust is a necessary component of information sharing. The rest of this section will explore these alternative presumptions in greater detail. A. Types of Cyber Threat Information Chismon and Ruks (2015) assembled a useful taxonomy of cyber information categories based on the kind of decisions the information informs. A modified version of their taxonomy is shown in Table I. As detailed in Table I, different categories of information, from technical to strategic, are intended for different consumers. However, information across the four levels—technical, tactical, operational, and strategic—is interrelated. For example, technical and tactical information can be combined to generate operational cyber threat information to improve organisational understanding of an impending attacker’s methods and capabilities (Chismon & Ruks, 2015). Similarly, post-incident analysis of technical cyber threat information often provides the foundation for the implementation of a tactical level decision. A holistic assessment of technical, tactical, and operational inputs drives the output of strategic cyber threat information. Despite these complex relationships, this taxonomy provides a useful way to think about cyber threat information and is indicative of why technical data-sharing should not be the sole focus of information sharing programmes. Smaller or less mature organisations are unlikely to find much utility in technical or tactical information sharing, while even larger organisations may miss out on key operational or strategic information insights if they focus exclusively on the technical information. For this reason, the Cyber Threat Alliance (CTA), which includes established cyber security vendors and related enterprises, shares a total of ten types of actionable cyber threat information across these four categories, as recalled by the authors and detailed in Table II. Understanding the value of these various forms of cyber threat information requires taking a more mature and nuanced view than the simplistic assumption that more information sharing means better security. This expanded conceptual framework for cyber threat information sharing reflects the diversity of information that industry leaders already know must be shared to strengthen defences. Each type informs a different aspect of cyber security and has a different value in different situations. Broad adoption of this (still high-level) extension to the framework provided by Chismon and Ruks (2015) would enable cyber security practitioners to develop more nuanced and useful policies for information sharing. B. Relevance and Comparative Advantage in Information Sharing In other disciplines, from finance to health to politics to sports, organisations do not produce and consume the same information equally. Instead, wide variation occurs based on relevance to business models, missions, and perceived benefits. Cyber security practitioners and policymakers should expect cyber threat information sharing to behave similarly. Different organisations should produce and consume different types of information based on two principles: relevance and comparative advantage. These two concepts should drive who should be sharing what information with whom, in what detail, and at what periodicity. 1) Relevance of Information Companies, non-profit organisations, and government agencies all have goals or missions and employ specific business models to achieve those goals. Information sharing should relate directly to an organisation’s goals and business model. Thus, a cyber security vendor should share technical cyber threat information at speed and at scale continuously because it is directly relevant to their business model. Conversely, a medium-sized manufacturer primarily needs strategic and operational level cyber threat information— strategic warnings, best practices, and tactical warnings (e.g., if a government learns that the business or its industry is being targeted)—all of which need only to be updated when a change has occurred. Technical cyber threat information provided at scale to this business would simply not be useful. 2) Comparative Advantage of Information Sharing Even if some organisations can produce certain information types, others might be more efficient at that work. For example, although governments can use their intelligence and law enforcement capabilities to collect, process, and produce technical cyber threat information, they do not have a comparative advantage in that information type. Private sector companies can perform that function just as efficiently. However, governments have a comparative advantage in other categories, such as attribution of cyber attacks, strategic warnings, and tactical warnings, which benefit from nation-state-level intelligence capabilities and authorities. As in other activities, the principle of comparative advantage should determine which organisations should be collecting, processing, sharing, and consuming different types of information. C. Technical, Economic, Legal and Cultural Barriers At first glance, the barriers inhibiting information sharing seem quite varied. However, a closer review shows they fall into four categories: technical, economic, legal, and cultural. While their specific manifestations and relative significance will vary across sharing contexts, these barriers can combine in various ways to create a formidable obstacle to sharing. Technical barriers prevent information from moving rapidly at scale or in easily consumable formats. For example, inconsistent definitions and terminology and difficulty in achieving interoperability and automation remain significant obstacles (Zibak & Simpson, 2019). In turn, these barriers often inhibit the usability or reliability of shared information (ENISA, 2017). Economic barriers stem from the inability to identify a clear return on investment from sharing activities. Organisations ‘participate in sharing networks when their return is more than the cost to participate’ (Vázquez et al., 2012: p. 432). This problem can be compounded by first-mover disadvantage, given that ‘establishing threat intelligence sharing infrastructure is expensive … [while] in the long run, intelligence sharing could help bring down the overall security cost’ (Zibak & Simpson, 2019: p. 7). Absent a clear and immediate prospect of a return on investment, proponents often have difficulty making the business case to establish, invest in or sustain sharing activities. Legal barriers come from uncertainty about what information can be shared under what circumstances or unanswered questions about liability, fines, or prosecution. These uncertainties deter organisations from sharing. Privacy laws can hinder sharing by inadvertently classifying certain cyber threat information as private and thereby limiting how it can be used or distributed (Panda Security, 2018). These legal concerns require sharing organisations to undertake extensive consideration of their potential implications (Borden et al., 2018; Albakri et al., 2019). Finally, cultural barriers can also impede sharing (Luiijf & Kernkamp, 2015). For cyber security companies, it can be hard to overcome the idea that retaining unique data yields a competitive advantage. For other organisations, it can be hard to overcome sentiments such as ‘no one would target me’, ‘cyber security is too complex for executives and non-technical employees to understand’, or ‘falling victim to hackers is inevitable, so why bother?’ For governments, long-standing views about the appropriate respective roles of the public and private sectors get in the way of cooperation and sharing. The good news is that, over the last twenty years, practitioners have developed ways to overcome these barriers. The bad news is that none of these methods is frictionless or cost-free. For example, adopting technical standards for information sharing may require organisations to adjust business processes or infrastructure; high initial costs may need to be met with loans that are paid back by future sharing participants; legal consultations may be needed to shape sharing rules; and reluctant executives may need the benefits of information sharing to be explained in bottom-line terms. Across the board, information sharing requires organisations to expend resources, either money or time. These costs can decrease but do not disappear. Yet, to be worthwhile, information sharing needs to be sustained and organisations have to pay a long-term, regular cost for engaging in information sharing activities. This requirement, in turn, means that information sharing requires incentives to achieve the scope, scale, and speed required for effective cyber defence. Such incentives can range from the individual (avoiding the costs of a cyber incident) to the public (government grants) to the avoidance of sticks (fines or penalties for not engaging in appropriate sharing). Regardless, information sharing laws, policies, programmes, and structures should assume that information sharing is resource-heavy and requires sustained investment to occur. D. Trust as a Necessary Component of Information Sharing Experience from previous initiatives and programmes demonstrates that information sharing only occurs when the providers and recipients have a degree of trust. As noted by Wagner et al. (2018), trust ‘plays a critical role in sharing’ (p. 5). The European Network Information Agency (ENISA) observes that in situations where trust between members of the community is diminishing or non-existent the value of information shared is undermined (ENISA, 2013). For information sharing to work, it is necessary to ‘foster confidence for stakeholders that the provided information will be acted upon as intended’ (Wagner et al., 2018: p. 5). Information providers have to understand who will receive their information, what they will do with it, and what level of information sharing-related risk to expect, while information recipients want to know where the information came from and its reliability. To reach this level of confidence, information sharing organisations should ‘provide control mechanisms to specify what information is shared, how much of it and with whom’ (Sauerwein et al., 2017: p. 845). According to ENISA (2012, cited by Vázquez et al., 2012: p. 433), the use of intentionally carefully designed trust-building mechanisms, such as ‘the policies, membership rules, requirement for security clearance and interaction type’ can be beneficial in the context of information sharing and will support the creation of trust. Absent trust, information sharing will not occur no matter what structures and incentives are put in place. Trust does not require that the participants all like each other, nor does it mean they share everything. Trust means that participants have a reasonable belief that all other participants will adhere to the agreed rules.

### S – Transparency

#### Transparency is key- NATO should be clear about capabilities to bolster cyber deterrence

Susan Davis 19, general reporter of NATO, “NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE”, STC, https://www.nato-pa.int/download-file?filename=sites/default/files/2019-09/148%20STC%20Davis%20-%20NATO%20IN%20THE%20CYBER%20AGE%20-%20fall%20revision%20-%20clean%2011.9.19.pdf

If one only looked at the bad cyber news flooding media outlets, policymakers could easily lose hope. However, this report’s in-depth analysis of Allied and NATO cyber strategies, policies, and activities has shown that NATO is strengthening cyber security, defence, and deterrence along all dimensions. The new cyber space doctrine to be adopted by the end of 2019 will be another crucial step. This progress should not lead to complacency. NATO must remain laser-focused on cyber attacks that could threaten an Ally’s territorial integrity, political independence, or national security and could, thus, lead them to invoke Article 5. The NATO PA resolution the Rapporteur will present for adoption at the Annual Session will represent the Assembly’s overall cyber policy recommendations. However, the Rapporteur would like to propose the following set of recommendations for the Committee’s endorsement. She urges the Committee to closely follow progress on these recommendations through all instruments available. The Alliance should continue to complement cyber security and defence measures with strategies of cyber deterrence. **NATO should maintain a cyber deterrence policy of ambiguity**. The Alliance should not set thresholds for when a cyber attack is sufficiently harmful to cross the threshold to an armed attack as well as for what the possible collective response would be if that threshold was crossed. Allies and NATO should continue to signal their resolve and credibility to deter cyber attacks. NATO should therefore remain as transparent as possible when it comes to its cyber capabilities. In areas where public disclosure is not an option, communicating with potential opponents through non-public channels should happen as frequently as possible.The Alliance should continue to seek to reduce escalatory risks through clear diplomatic messaging and engagement, a high level of transparency on cyber capabilities and policies, and support to norm-development and confidence-building measures in cyber space.

### S – Public-Private Info

#### NATO must strengthen public private partnerships and information sharing to counter emerging cyber threats and enhance deterrence

Lete & Dege ‘17[Bruno & Daiga; 2017; senior fellow or security and defense policy in GMF’s security office; trainee in office, “NATO cybersecurity: a roadmap to resilience, <https://www.gmfus.org/sites/default/files/NATO%2520Cybersecurity_edited.pdf>]

The core of NATO cybersecurity efforts lie at the member-state level. NATO is responsible for protecting its own institutional information and communication systems, but it has little say in coordinating how member states develop their national cyber defense capabilities. Despite having signed the Cyber Defense Pledge at the Warsaw NATO Summit, many member states still struggle to implement and evaluate their national cyber-security plans. As a result NATO’s efforts at developing uniform, alliance-wide cybersecurity are undermined by significant inconsistencies across the national level of the member states and NATO’s collective security and deterrence in cyberspace still show serious vulnerabilities against the backdrop of a growing number of attacks. For NATO to operationalize cyberspace as a domain of NATO defense policy and planning — as was agreed at the NATO Warsaw Summit — the Alliance should have authorizations from member states to do more than just provide advice, expertise, training, or education. Similar to how NATO coordinates Allied military forces in the conventional domain, NATO could also be asked to evaluate how member states can develop, synergize, and complement their mutual national cyber defenses. At a minimum, NATO should develop standards and better indicators that allow a standardized measurement of a nation’s annual progress — and should be tasked with testing and measuring members’ capabilities annually. To achieve this objective, a strong cooperation with the European Union is essential. NATO and the EU could work together to design minimum cybersecurity requirements and benchmarks that would also be adopted by the European Defense Agency. Rapid Assessment and Decision-Making Tools The scale, speed, and intensity of today’s cyber-attacks demand a new approach to respond at the political, military, and civilian level. To develop a rapid decision-making process when facing a cyber-attack NATO can take a few effective measures across its organization. First, more resources must be allocated to accurately and quickly detect and define hostile cyber actions. Further work on indications, warnings, and situational awareness is critical. In this context, NATO’s various civil and military intelligence units, inter alia, could have a useful role. In addition, the Supreme Allied Commander Europe (SACEUR) could be granted more powers by the North Atlantic Council in authorizing some of the preparatory procedures. At the same time, NATO headquarters should increase the number of exercises that test rapid decisions-making procedures in complex and demanding cyber crisis-conflict scenarios. Much can also be done at the member-state level. Allies and willing partners should continue to work on improving and updating threat assessments, and facilitating closer intelligence cooperation. In this light, Allies should identify information sharing as a clear requirement and task. NATO could also intensify its interaction with national intelligence services and establish supply chain management partnerships with national industries. Cyber threats come in the form of networks and it takes a similarly well-organized network of international and cross-sector cooperation to defeat those threats. Common Rules of Engagement NATO has not commonly defined the circumstances, conditions, degree, and manner in which the use of force may apply if one of its member states suffers a cyber-attack. Triggering the authorization to use force in the context of Article 5 may be more obvious if a member state faces a large-scale, devastating cyber-attack where the source of the attack can be clearly attributed. But the need is much more urgent to define when and how NATO must respond against the day-to-day cyber intrusions that fall below the threshold of being perceived as a clear act of aggression. NATO policy still allows for too many gray zones that are being exploited by adversaries who are clever enough not to cross a line that would trigger a common response from the Alliance. Cybersecurity incidents like the alleged Russian hack of the Democratic National Committee’s emails show that the United States and the NATO Allies are still unclear about the conditions and manner to respond in cyberspace. The Tallinn Manual published by the NATO CCDCoE offers a set of guidelines on how states can define rules of engagement, countermeasures, retaliation operations, and other forms of response within the context of the international law if they are to face an act of cyber aggression. But NATO is still far removed from having adopted a common view and interpretation on the subject. The North Atlantic Council would still need to assess each individual cyber-attack case by case without the support of standard measurement tools and indicators that can help NATO formulate a proportionate political or military response. As more cyber policies and laws are taking shape, NATO could demonstrate political, military, and intellectual leadership by clearly defining rules of engagement in cyberspace. Consider Offensive Cybersecurity NATO now recognizes a serious cyber-attack as a potential Article 5 trigger. But the doctrine and crisis management conditions enshrined in NATO’s cyber policy puts the emphasis on a defensive posture only. As such, the Alliance fails to recognize cyber as a force multiplier that could be of importance to the defense of NATO nations. Russia for instance considers offensive cyber capabilities to be an integral part of its military power and especially as a way to make up for its relative lack of conventional forces compared to NATO. The rise in connectivity, smartphone proliferation, cloud computing, growth of application development, and other technological advances open new avenues to attackers and force defenders to cover an ever-increasing number of fields. In the long run, NATO’s defensive approach is not sustainable. It is time for NATO to start a debate on offensive cybersecurity and map the feasibility of coordinating counter strikes, and to establish a significant offensive cyber capability. NATO could center this debate on projecting offensive cyber warfare capabilities as a means of deterrence, similar to the perceived value of nuclear weapons to deter attacks against NATO. Offensive security will allow the Alliance to better control the virtual battlefield. There are valuable cyber capabilities worth attaining, including the ability to conduct reconnaissance and surveillance, intercept communications, or deny resources and access. NATO may find increasing support to have a conversation on offensive cyber security with its allies. As member states are increasingly preoccupied with defense and deterrence issues in cyber-space they will show more receptivity to cooperation with NATO on developing centralized offensive cyber capabilities. NATO and Cyber Industry Cooperation Cybersecurity is largely market-driven. Government intelligence capabilities increasingly find it hard to keep up with the requirements for combating the surge in cyber threats. NATO should play a crucial role in facilitating contacts between those member states that seek stronger links with the private sector and encourage the role that industry can play in cyber threat deterrence and intelligence sharing. Flagship initiatives, such as the NATO Industry Cyber Partnership, are important steps in that direction but there is still a need to build more access and trust between NATO governments and industry. Educating member states and partner nations about the role of the private sector in cybersecurity is key. To make the partnership with the industry more effective NATO could play a more important role in mapping and evaluating what kind of cyber defense technologies and intelligence gathering methods the private sector offers, share lessons learned with the member states and encourage capitals to integrate the best practices into capabilities, policy, and implementation planning. NATO can also play an essential role in improving communications and information sharing between the private and the public sectors. More can be done at the NATO level to identify what kind of information between governments and companies can or cannot be shared, to develop standardized methods and formats for information sharing, and to encourage the use of automated platform capabilities to share this information quickly. Build a Robust Public Diplomacy Campaign The first frontier of cyber defense is the individual. Citizens who are digitally empowered, cyber aware, and cyber educated will display a more responsible behavior and automatically increase NATO’s collective security in cyberspace. NATO needs a narrative on why cybersecurity matters beyond public belief that a major cyber-attack is improbable. What can NATO do in cyberspace that national security agencies cannot do? Which level of cybersecurity is needed rather than which one we can afford? NATO societies should be exposed to debate through parliaments, media, nongovernmental organizations, and academia. Externally, the Alliance must adapt to the reality that countries hostile to NATO will continue to use their own cyber capabilities and massive state propaganda organizations to attack NATO systems and discredit everything the Alliance does. NATO has to be able to engage in and win this information war at the elite decision-maker and opinion-former levels rather than simply raise awareness of its existence and activities among a global public.

#### Partnership programs work but are limited—Nato should prioritize partner programs essential for security cooperation

Lisa Aronsson and Brett Swaney 21;

June 14, 2021; Lisa Aronsson is a research fellow, and Brett Swaney is an assistant research fellow, at the Institute for National Strategic Studies at National Defense University.; Atlantic Council; “Three priorities for NATO partnerships in a contested world”;

NATO’s Partnerships programs have provided options for cooperation with non-member states for more than twenty-five years. They’ve proven remarkably flexible and adaptable, serving partners’ as well as NATO’s evolving interests. They helped consolidate democratic transitions in Europe, provided support for NATO-led missions and operations, and strengthened collective defense and deterrence. Through Partnerships for Peace, NATO offers a menu of more than 1,400 activities open to all forty partner states around the world. Partners choose the scope, focus, and intensity of their cooperation with NATO. The arrangement has appealed to a diverse group of states, which NATO organized into the Euro-Atlantic Partnership Council, the Mediterranean Dialogue, the Istanbul Cooperation Initiative, and Partners Across the Globe. In the current environment, however, there is mounting pressure to adapt partnerships to ensure they continue to support NATO’s interests. The patchwork of geographic groupings is increasingly incongruent with today’s challenges. The groups have generally failed to promote security cooperation or political consultations at the regional level. They have also inhibited NATO’s ability to set priorities or steer cooperation with partners towards its own objectives. Moreover, the activities that partner states value most—capacity-building and interoperability, or the ability to link up their forces with NATO’s and act coherently—remain underfunded. As NATO reorients to incorporate China into a broader strategic calculus, how can NATO preserve what works for partners and adapt its partnership policies without defaulting to a one-size-fits-all approach? First, NATO should ensure that capacity-building and additional resilience support remain priorities. China is using its economic leverage to expand its security cooperation, and Beijing, along with Russia, is undermining Alliance credibility. Some partners have become testing grounds for hybrid attacks. Capacity-building helps counter that by strengthening partner institutions and resilience, and a sense of shared security. The Partnership Interoperability Initiative protects hard-earned interoperability with some partners, and the Defence and Related Security Capacity Building (DCB) Initiative already supports Georgia, Iraq, Jordan, Moldova, and Tunisia. The NATO Parliamentary Assembly has recommended more attention to Ukraine, the Western Balkans, and areas with weak institutions or where democracy is undermined. Civil emergency planning through NATO’s Euro-Atlantic Disaster Response Coordination Centre is also valuable. Capacity-building programs are also a path to NATO interoperability for partners, which remains a major driver for cooperation with NATO—even among neutral countries that may never contribute to a NATO military operation. This is because NATO provides internationally recognizable military standards and the ability to plug-and-play into European Union (EU), United Nations, or other multilateral operations. NATO interoperability certification is in demand among partners, as are its robust programs for education, training, and exercises. These activities promote defense and security sector reform, strengthening institutions and transparency. NATO should work to overcome constraints on partner participation in exercises, especially for Japan, South Korea, Australia, and New Zealand. Cooperative security depends on NATO’s centrality as an international standard-setter, a position that cannot be taken for granted. Second, NATO should accelerate internal consultations on China and bring partners in early and often on topics of mutual concern, ensuring NATO decision-making is informed by partners in the earliest stages. This has worked well with Sweden and Finland, but it should work better with NATO’s Indo-Pacific partner states, those along China’s Belt and Road Initiative, and those with high-end cyber or space interests. The old geographic boundaries are being redrawn around these issues. NATO should work to better define mutual expectations and goals with partners and leverage natural groupings around cross-cutting challenges, perhaps by expanded use of 30+N arrangements or revised “framework nation” models, to bypass the gridlock of regional mechanisms. Daniel Hamilton of Johns Hopkins’ School of Advanced International Studies recommends offering Enhanced Opportunities Partnerships to Japan and South Korea in an effort to improve interoperability, information-sharing, and political consultation. Finally, NATO should forge new frontiers in science and technology (S&T) cooperation with partner states and the EU. The Alliance has interests in achieving dominance in Emerging Disruptive Technologies (EDTs) and in setting norms and standards for their incorporation into militaries. NATO boasts renowned research universities and innovation hubs, but so do partner states like Sweden, Finland, Japan, and South Korea, for example. NATO should expand support for S&T collaboration with these partners and others through the Science for Peace and Security Programme (SPS). NATO should also explore other avenues to expand research collaboration with select partners and share lessons learned from public-private partnerships. Partners already stand shoulder-to-shoulder with NATO on cybersecurity, for example, and should be brought into S&T Board and other discussions where possible. A more ambitious NATO-EU relationship in this area would be a force multiplier. NATO also has a related interest in leading the global mission to ensure that EDTs are integrated into modern militaries in ways that are consistent with its values and with the Universal Declaration of Human Rights and United Nations Sustainable Development Goals. So far, the Alliance’s Advisory Group reports that NATO’s EDT strategies are focused internally on harnessing member states’ strengths and building a cohesive Alliance innovation ecosystem that is buttressed by talent development and novel financing initiatives. NATO is expected to release an artificial intelligence (AI) and big data strategy this summer, the first of seven EDT strategies, and it should outline a broader vision that links NATO’s innovation ecosystem with those of its partners. Partners and other like-minded states around the world are already looking to NATO for guidance on AI, codes of conduct for military activity in outer space, and standard-setting for cybersecurity, for example. Looking ahead, NATO partnerships will remain demand-driven, but they should adapt to serve NATO as it grapples with China’s rise while still addressing myriad other challenges. The next Strategic Concept will update the Alliance’s approach to cooperative security. NATO should set a higher level of ambition for partnerships and fund them so that they continue to appeal to such a diverse group of states around the world. Expanding capacity-building to include more resilience support remains paramount, but accelerating political consultations and forging ahead with ambitious S&T cooperation are also important. Failure in these areas risks allowing NATO partnerships to languish and fade into irrelevance at a time when the Euro-Atlantic community most needs a wider network of partners to face a contested world order.

### S – Resilience

#### Intelligence coordination focused on resilience solves cyber offense and defense – the US can lead the way on establishing “safe-to-fail” goals.

Hamilton & Binnendijk ’22 (Daniel S. Hamilton is President, Transatlantic Leadership Network Senior nonresident Fellow, Brookings, Senior Fellow, Foreign Policy Institute, Johns Hopkins University SAIS; Former U.S. Deputy Assistant Secretary of State. Hans Binnendijk is a Distinguished Fellow, Atlantic Council Former Senior Director for Defense Policy, U.S. National Security Council “One Plus Four: Charting NATO’s Future in an Age of Disruption,” NATO Task Force Report, Transatlantic Leadership Network, February 16, 2022, https://www.transatlantic.org/wp-content/uploads/2022/02/NATO-TF-SC-final-feb-16-2022.pdf)-mikee

c. Bolster Deterrence and Defense Against Hybrid Threats Advancing the Alliance’s ability to deter and defend also means prioritizing ways to deal with unconventional conflicts that might hover below the Alliance’s Article 5 mutual defense threshold. These include some types of cyberattacks, energy intimidation, financial destabilization, election interference, and dis- and misinformation campaigns. NATO’s Strategic Communications Center of Excellence Command (CoE STRATCOM) needs creative new steps to detect and counter false information, including real time alerts to Allies on emerging threats and recommended countermeasures. Many relevant competences in Europe fall to national civilian authorities, to the private sector, or to the EU. While NATO can lead in developing and adapting cyber-deterrence and counter-disinformation guidelines and capabilities, better EU-NATO coordination and planning, will be needed. There is greater need to align and intensify action via the Helsinki-based European Center for Countering Hybrid Threats, ensuring there are operational feedin loops to NATO and EU decision-making. NATO and the defense establishments of its members are under constant attack from cyber hackers seeking to penetrate their information systems, extract data and plant viruses that could be used against allies. Digital disruptors target NATO systems, the operational cyber networks needed to execute military missions, and an extensive number of civilian networks that are essential to critical societal functions. Allies have determined that some types of cyber attacks could trigger Article 5 of the North Atlantic Treaty. In the 2016 Cyber Defense Pledge, allies affirmed their individual responsibilities under Article 3 of the Treaty to enhance their cyber defenses. The 2030 Reflection Group highlighted the need to develop both greater collective defense capacity in cyberspace and a more robust consultation framework to facilitate collective defense, crisis management, and cooperative security in the cyber domain.20 These concerns were largely echoed by allies in the 2021 Brussels Summit Communiqué.21 Nonetheless, allies have been reluctant to organize operational capabilities via NATO, and only five member states have announced that they will make sovereign cyber effects available to the Alliance.22 Limited measures thus far undertaken include deployment of cyber defense elements with NATO response forces, where continuous coordination and planning of cyber operations is essential. NATO has also gained initial experience through the SHAPE Cyber Operations Center (CyOC).

Box 1. Enhance Cybersecurity Through “Safe-to-Fail” Principles If NATO is to effectively address the broad range of security challenges emanating from the cyber domain, the Alliance could complement its current collective defense efforts by incorporating cyber resilience and “safe-to-fail” principles into the new Strategic Concept.23 Until now, NATO efforts to operationalize collective defense have relied primarily on ‘fail-deadly’ and ‘fail-safe’ logics in cyberspace. Should deterrence fail, ‘fail-deadly’ means the Alliance responds with the use of deadly force, whereas ‘fail-safe’ efforts are intended to ensure that the Alliance and its members can continue to operate safely and securely in the cyber domain.24 While these two approaches are important, they only apply to a limited band of the full spectrum of threats presented by the cyber domain. Fail-deadly deterrence is only likely to succeed in preventing adversarial states from cyber operations that reach the threshold of armed conflict with destructive physical effects that are quickly attributable.25 It is likely to be ineffective with state or non-state actors inflicting lower threshold attacks for which attribution is difficult. These considerations are further complicated by the differing legal restraints individual allies place on offensive cyber operations. Fail-safe measures also face several challenges. Given the sheer quantity of daily network probes experienced by NATO and individual member states, it is unlikely that every intrusion can be successfully countered or even identified. Highly sophisticated cyber operations are also likely to evade most defensive measures. Moreover, computers and systems increasingly rely on commercially available products and non-NATO-based manufacturers. Defensive strategies will have limited utility if hardware or software components have been preloaded with malware.26 The Alliance and its members need to account for a variety of threats and scenarios for which fail-deadly and fail-safe strategies prove ineffective—such as ransomware attacks, distributed denials of service, exploitation of digital supply chains, or operations conducted by non-state actors. To withstand and bounce forward from such disruptions, NATO should ensure that military cyber functions and capabilities are ‘safe-to-fail’ -- that is, they can fail in ways that do not remove their ability to recover at or above original operating capacity. Incorporating safe-to-fail principles would require the Alliance to fill out the full meaning of Article 3, which is not limited to “self-help” but also includes “mutual aid.” It would mean coordinating with the private sector and de-conflicting economic priorities, as provided under Article 2. It would include developing metrics for assessing Allied operational success in cyberspace, and horizon scanning for emerging cyber technologies that could affect Alliance security.27

The Strategic Concept should take NATO efforts further. The United States might offer to be the framework nation in the next evolution of NATO cyber operations planning and coordination. A full NATO Cyber Defense Forces Headquarters (NCHQ) should be agreed, based on the proven NATO Special Operations Forces Headquarters (NSHQ) model. An NCHQ would improve cooperation among allies and protect NATO’s freedom of action in cyberspace, strengthening deterrence. Such a headquarters should generate the necessary arrangements and readiness to allow nations to plug their capabilities and produce cyber effects should there be a collective decision to do so. It should act to achieve consensus on issues of cyber deterrence, particularly whether individual Alliance cyber defense capabilities alone are adequate or whether capabilities are needed to effectively deter major strikes against NATO networks, the networks of individual nations, or against the critical infrastructures of allied societies (Box 1). It should be linked to the EU’s broader cyber toolbox.28

#### NATO must develop Resilient Cybersecurity Architectures and Active Cyber Defenses- they will make it more difficult for advisories to attack

Kramer et al ‘20

[Franklin](https://www.businessinsider.com/author/ben-winck) D. Kramer; Distinguished fellow and board director at Atlantic Council. Expert in cybersecurity, defense policy, and non-traditional threats; Lauren M. Speranza; Director of the Transatlantic Defense and Security program at the Center for European Policy Analysis (CEPA); Conor Rodihan; Associate director at Scowcroft Center for Strategy and Security; NATO needs continuous responses in cyberspace; Atlantic Council; https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/

First, NATO should require the development and implementation of resilient cybersecurity architectures for itself, its members’ forces, and its key critical infrastructures. A resilient cybersecurity architecture involves an integrated set of capabilities that work as a system to reduce the disruptive effects of cyber adversaries. Key elements of a resilient architecture should include use of private sector cloud technology; zero-trust architecture for effective access management; development of secure hardware capabilities; and machine-learning and artificial-intelligence-augmented cyber defenses. This architecture also needs to be flexible to incorporate emerging technologies as they are developed. NATO itself cannot develop such architectures. It can, however, underscore their necessity and require its members to do so, using the NATO Defense Planning Process (NDPP), acquisition procedures, standards and targets, and innovation from Allied Command Transformation to support a comprehensive research and development effort. In establishing requirements for these resilient architectures, NATO must recognize that one size will not fit all. Not only will requirements differ among military, government, and critical infrastructures operators, but, as has been shown in the development of autonomous vehicles and space capabilities, there are a variety of different approaches that may prove effective. In fact, having diversity within these capabilities will increase resilience by complicating adversaries’ abilities to infiltrate and attack them. Second, NATO, in coordination with its nations, should undertake active cyber defense. Even the best exclusionary capabilities in a cybersecurity resilient architecture can fail due to technical loopholes or human error. As a result, the Alliance needs “active cyber defenses” that can create resilience even when an attacker has breached cyber protections. These capabilities affect only those networks in which operators and owners have installed them and are not for offensive purposes. As the US National Security Agency explains, key elements of active defense capacities include “real-time communications,…sensors that report data on the current state of the network, sense-making analytics to understand the current state, automated decision-making to decide how to react to current state information, and capabilities to act on those decisions to defend the network.” NATO should include such active defense capabilities as a requirement of an overall resilient cybersecurity architecture. As a key element of active cyber defense, NATO must be capable of hunting for adversaries within cyber systems critical to defense. The Alliance should develop highly capable expert hunt teams to review system activities, detect anomalies, and defeat intruders, for example by deleting malware and closing unnecessary ports. NATO can significantly enhance Allies’ active defense efforts by establishing an NDPP requirement for national cybersecurity hunt teams, along with command arrangements for those teams in both hybrid and Article 5 contingencies. It should also establish several NATO Standing Cybersecurity Hunt Teams that would operate with the consent and active partnership of national governments and critical infrastructure network operators. As Microsoft has explained the role of hunt teams, Standing Cybersecurity Hunt Teams, acting in conjunction with national capabilities, can contest the continuous cyber campaigns of Russia and China. According to the US Department of Homeland Security, such hunt teams can conduct deep technical analyses of live networks to identify “previously unobserved threats.” Standing Cybersecurity Hunt Teams, with a focus on active defense, would expand on the capabilities of NATO’s current Cyber Rapid Reaction teams which are limited in numbers and operate reactively. While the cybersecurity of infrastructure and government systems is a national responsibility, a breach of cybersecurity at the national level can have collective consequences. Standing Cybersecurity Hunt Teams can be a capability, as well as connective tissue, to identify and mitigate cyber threats across national boundaries and enhance NATO’s collective defense. Standing Cybersecurity Hunt Teams would be able to utilize information and experience gained from contesting Russian and Chinese cyber-attacks against one ally in the defense of others. A Standing Cybersecurity Hunt Team can also serve in a capacity-building role to help allied nations develop their own cyber capabilities, for example, in conjunction with the NATO Cooperative Cyber Defense Center of Excellence.

### S – Unity

#### Data sharing is key to promoting NATO unity – resolves longstanding challenges and reunites member states over common threats.

Kris Osborn 6-18 [Kris Osborn is the Defense Editor for the National Interest. Osborn previously served at the Pentagon as a Highly Qualified Expert with the Office of the Assistant Secretary of the Army—Acquisition, Logistics & Technology. “A New NATO: Common Data Sharing Systems Coming Soon”. June 18, 2022. https://nationalinterest.org/blog/buzz/new-nato-common-data-sharing-systems-coming-soon-203082]

Interoperability and rapid deployment reinforce one another. The more a multinational force is able to share sensitive information in real-time using common standards, interfaces, or interoperable data links, the faster a NATO force can move into position and conduct joint multi-domain operations. Improving interoperability has been a long-standing challenge for NATO forces. Radio frequencies need to be aligned, computing protocols need to enable data exchanges, and datalinks between separate countries need to operate with interfaces to ensure information transmission. Common command and control systems, fortified by uniform technical standards, can ensure NATO members are increasingly able to act seamlessly in warfare formations on the eastern flank. One clear advantage to this effort can be found in the F-35 stealth fighter, as the aircraft uses a common data link for all F-35s across multiple nations. The F-35s Multifunction Advanced Datalink (MADL) enables F-35s from any country to interact with and share information across a multinational formation of fifth-generation aircraft. The alliance is likely working to move beyond this existing synergy and connect drones, aircraft, ground vehicles, and surface ships from multiple countries in real-time using a common framework. This would allow an F-35 from Poland to send targeting detail to U.S. Abrams tanks positioned to defend Finland or to NATO surface ships in the Baltic Sea trying to disrupt Russian maritime supply lines. NATO will likely seek to build upon the existing framework of its NATO Standardization Agreement 4586 (STANAG 4586) to enable drones from different countries to exchange information in a common format. STANAG 4586 could perhaps be upgraded to reduce latency, prevent hacking, or expanded to other platforms using compatible technical standards, message formats, and protocol. NATO’s ability to rapidly respond relies to a large extent on the alliance’s capacity for common command and control and data exchange, or else forces from different member nations will be alienated from one another in combat environments. Given the number of breakthroughs the U.S. military is achieving with joint information networking, it makes sense that Austin would emphasize ongoing efforts to extend this kind of real-time connectivity among NATO members.

#### Exposing Russian cyber campaigns alone is not enough- only persistent cooperation and coordination among NATO members can forge the political unity necessary to deter Russian attacks

Oscar Jonsson in 2021

scholar of strategy, emerging technology and Russia who is founder of Phronesis Analysis and Researcher at Swedish Defence University; FROM EASTERN FLANK TO WESTERN ELECTIONS: RUSSIAN OPERATIONS AGAINST THE EU AND NATO; The Center for European Policy Analysis; https://cepa.org/the-evolution-of-russian-hybrid-warfare-eu-nato/

The most immediate lesson for Western governments from the U.S. elections in 2016 was not to be quiet about Russian influence operations. The biggest benefit of exposing Russian operations is increasing public awareness of the threat and the determination to devote sufficient time and resources to countering it, which will in the long run change the cost-benefit calculus.38 Moreover, Bellingcat’s investigative journalism has served to expose Russian intelligence operations and has become a headache and source of embarrassment for the Russian leadership.¶ Nonetheless, “naming and shaming” should not be seen as sufficient for deterring Russian operations. After the U.S. elections in 2016, the poisoning of former Russian-British double agent Sergei Skripal in the United Kingdom in 2018, and the poisoning of Navalny in August 2020, it has become clear that the Russian leadership is not too worried about some of its high-profile operations becoming known to the public. On the contrary, the Skripal poisoning was intended to send a signal to other intelligence officers in Russia and also to the West. As “Putin and his inner circle appear to believe that they are in nothing less than a political war, [naming and shaming] will at best influence tactics, not strategy.”39¶ With the Russian leadership committed to the idea that it is in a political war against the EU and NATO, more is needed than simply exposing its malign behaviors. So far, the Western approach has been to primarily rely on sanctions in lieu of stronger policy measures. Sanctions are an alternative to escalation. They satisfy the urge to “do something” rather than fix the underlying problem.40 Moreover, inflicting economic pain is only effective to the extent that economic development is a priority for the Russian leadership. Nonetheless, it is demonstrably subordinate to regime security and great-power status.¶ The EU is responsible for the political response to the challenge from Russia, including sanctions, and has since 2014 taken a wide range of measures to increase preparedness against hybrid threats. These include creating sectoral strategies, establishing expert bodies (Hybrid Fusion Cell, Center of Excellence for Hybrid Threats), creating information-sharing mechanisms, conducting exercises and simulations, partnering with NATO, and increasing investments in cyber defense.41 Most notably, the EU adopted an Action Plan against Disinformation42 and set up an EU versus Disinformation initiative in 2015. In July 2020, the EU also imposed its first-ever sanctions (asset freeze and travel ban) in response to cyberattacks on individual GRU officers and the responsible center at the GRU.43¶ These are all important steps to improve the infrastructure, but the core problem for the EU and NATO is still political and about unity. Both the EU and NATO have viewed Russian hybrid warfare as more of a nuisance than a fundamental challenge. NATO is primarily responsible for the military instrument, but also has a key role maintaining political unity. The lack thereof was evident when Macron called for a rapprochement with Russia in 2019 while failing to grasp the fact that Russian aggression is premised on the predictability of the West to always return to the negotiating table even though the fundamental problem has not been addressed.¶ Indeed, between Russia’s invasion of Ukraine and Macron’s call for better relations, Russia had not only impacted the U.S. and French elections, it had also used chemical weapons on NATO soil to try and assassinate Skripal, an attempt that resulted in the death of a British citizen.44 Western actions have underlined that the West is unwilling to accept economic pain for geopolitical gain, in a failure to invest more into military and nonmilitary capabilities or impose tougher sanctions.¶ Governments alone cannot solve the problem of Russian influence operations. Big technology companies provide an important arena for these operations. These firms have come a long way since their 2016 laissez-faire approach to beefing up their defenses. Facebook is now more aggressive about taking down coordinated inauthentic behavior, Twitter has banned all political advertising, and Google, Facebook, and Twitter have signed onto the EU’s Code of Practice, which sets a wide range of commitments, including transparency in political advertising and the closure of fake accounts. However, as methods for exposing disinformation are disclosed, Russian strategists will seek to circumvent them.45 The task for the EU and NATO is Sisyphean.¶ Just days before the 2020 U.S. elections, the New York Post ran a story based on leaked (or fake) information against Biden. Twitter was quick to block the story, and Facebook posted warning labels next to it.46 Regardless of the wisdom of those actions, it does show the increased awareness of the big social media companies that staying away from acting is not a strategy.¶ Russia is constantly adapting its hybrid warfare in response to its adversaries’ actions and technological change. As automated bots and hack-and-leak operations are exposed, Russian operations have changed to create more organic-looking means of influence that blend international and domestic issues.¶ The key lesson for Russian strategists so far has been that their operations carry low costs and have potentially very high rewards. As long as this calculus remains in place, these operations will continue. The political unity of the West is fragile and already under great domestic strain — a reality that Russia seeks to amplify and exploit. The fundamental challenge for the West is maintaining political unity to counter Russian operations and successfully deter the most significant ones, including election meddling or the use of chemical weapons on NATO territory.¶ Many other operations, however, such as run-of-the-mill disinformation, cannot reasonably be deterred given the Russian leadership’s conviction that it is in a political war with the West. Such operations will need to be countered with hardened defenses, public-private cooperation, and dedication.

### S – Interoperability

#### Interoperability is key to NATO’s success- ensures efficient and precise action

Easley ‘22 (Mikayla is a journalist, writer, and researcher with experiences working in local news, magazine, and trade publications. She’s currently working as the managing editor of the [*Missouri Information Corps*](https://journalism.missouri.edu/2021/06/missouri-information-corps-launches-second-edition/), a pop-up newsroom covering climate change in Missouri.¶ “WEB EXCLUSIVE: Ukraine Invasion Prompts Plea from French Official to Speed Up NATO Tech Integration”; National Defense Buissness and Tech Magazine; March 9, 2022 ¶ <https://www.nationaldefensemagazine.org/articles/2022/3/9/nato-must-prioritize-system-interoperability-french-defense-official-says>)

Russia’s invasion of Ukraine highlights the need to speed up NATO interoperability, he said. The ability for weapons and other military systems to communicate and share information among NATO allies is one of the most important aspects for the alliance’s success in future fights, Burkhard said during a fireside chat hosted by the Center for New American Security. Collective interoperability is not currently the standard, he noted. For example, Burkhard has witnessed communication issues with the increased deployment of the F-35 joint strike fighter into various NATO ally’s air forces. “The F-35 is designed as a very effective and efficient system,” he said. “It has great qualities, but its design is a very closed system and I think this is a mistake.” NATO militaries must play a decisive role in ensuring network interoperability standards across the alliance, he added. France is also working to improve interoperability within its own armed forces in an effort similar to the U.S. Defense Department’s joint all-domain command and control, or JADC2, which aims to link sensors and shooters at the tactical edge. France’s internal campaign to achieve interoperability is part of its Scorpion program, which “aims at digitalizing all land forces in order to be able to extend information very quickly and also improve [our] operational pace in order to be able to impose our will on opponents,” he said. A document — Burkhard’s Strategic Vision for 2030 — is not unlike modernization plans made by the United States and the United Kingdom to move away from operations against nonstate actors and prepare for potential conflict with adversaries such as China and Russia. An exception the U.S. and U.K. militaries’ desires to shrink the size of its land forces. France will be focusing its attention on upgrading its Army by the year 2030, he noted. This includes the development of two new ground vehicles for the French army to replace the service’s aging vehicles and systems: the Griffon, a multi-role armored vehicle, and the Jaguar, an armored reconnaissance and combat vehicle. Burkhard said the ability of these vehicles and other **new capabilities to connect and share information across domains is “the true driver” for success**. Russia’s operations — which have not gone to Moscow’s plans — signal the true amounts of effort required for high-intensity operations. “It doesn’t mean that we are not able right now ready to engage in a high-intensity conflict, but not with all the assets that were identified or the level of training we [expected] to reach by 2030,” he said.

#### NATO must strengthen its threat identification, network protection, intrusion detection, etc to defend itself against cyber attacks.

SusanDavis 19**,** general reporter of NATO, “NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE”, STC, https://www.nato-pa.int/download-file?filename=sites/default/files/2019-09/148%20STC%20Davis%20-%20NATO%20IN%20THE%20CYBER%20AGE%20-%20fall%20revision%20-%20clean%2011.9.19.pdf

As armed forces around the world, including in potential adversary states, build up their cyber capabilities, NATO and its member states must devise strategies and policies to counter the threat of serious state-directed cyber attacks. Overall, NATO is leaning heavily on the same general strategies it uses to counter other attacks: dissuasion by denial and deterrence by punishment. However, Allies should continue to support work on international norms and engage in serious discussions if and how strategies such as persistent engagement, as outlined above, can supplement overall NATO strategy. 1. Norms in Cyber Space 25. Due to the specific characteristics of malicious cyber code, arms control, disarmament, and non-proliferation measures very likely remain beyond reach for now, most importantly because verification seems impossible. However, the further development of norms in cyber space could become an important pillar of support against such attacks. NATO continues to argue that international law applies to cyber space, including international humanitarian law and the United Nations Charter. This is also in line with the declaration of the 2013 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE, 2013). The Alliance has declared its support for “work on voluntary international norms of responsible state behaviour and confidence-building measures regarding cyberspace” (NATO, 2016b). Allies furthermore made clear that they “stand to benefit from a norms-based, predictable, and secure cyberspace” (NATO, 2018a). However, it is unrealistic to expect that NATO, as an Alliance of 29 sovereign nations, could become the primary driving force for the further development of norms. Instead, individual Allies must continue to drive this effort in the international community and encourage other member states to do the same. 2. Cyber Security and Defence 26. Strategies of dissuasion by denial aim at “dissuading an action by having the adversary see a credible capability to prevent him from achieving potential gains adequate to motivate the action” (Davis, 2014). In other words, the defender must make such an attack look futile: the attacker should either fail or, at the very least, not benefit from a cyber attack (Nye, 2017). Such cyber dissuasion is squarely premised on strong cyber security and defence, which is primarily a national responsibility, but **NATO must and does play a role,** which the next sub-sections show (see also Box 4). 27. In theory, cyber security and defence is a straightforward proposition. Defenders try to reduce vulnerabilities, block access points, and minimise the impact of payloads. Cyber security and defence include a range of preventive, passive, and active measures. Those seeking to protect their networks must strengthen their capabilities in several areas: threat identification; network protection; intrusion detection; responses against attacks; and resilience and recovery (US NIST, n.d.; see Box 5). Determined intruders are often very agile and adapt rapidly to circumvent new cyber security or defence measures. Allies, thus, often turn to more active cyber defence. For example, the US DOD, under its active cyber defence concept, can synchronise defence across all government and critical infrastructure networks. In other words, they defend more than just the networks owned and operated by the DOD. A step beyond is the so-called ‘defend forward’ concept, adopted by the United States in 2018 for example. When defending forward, defenders can cross over into the attacker’s networks to conduct intelligence operations; try to disrupt ongoing or even planned attacks; quickly reverse damage from attacks; and, in extreme situations, punish attackers (Hoffman and Levite, 2017; US DOD, 2018).

### S – Training

#### NATO should enhance cyber protection by developing uniform cybersecurity regulations – aggressive cyberattacks increasing

Lete & Dege ‘17 [Bruno & Daiga; 2017; senior fellow or security and defense policy in GMF’s security office; trainee in office, “NATO cybersecurity: a roadmap to resilience, <https://www.gmfus.org/sites/default/files/NATO%2520Cybersecurity_edited.pdf>]

The core of NATO cybersecurity efforts lie at the member-state level. NATO is responsible for protecting its own institutional information and communication systems, but it has little say in coordinating how member states develop their national cyber defense capabilities. Despite having signed the Cyber Defense Pledge at the Warsaw NATO Summit, many member states still struggle to implement and evaluate their national cyber-security plans. As a result NATO’s efforts at developing uniform, alliance-wide cybersecurity are undermined by significant inconsistencies across the national level of the member states and NATO’s collective security and deterrence in cyberspace still show serious vulnerabilities against the backdrop of a growing number of attacks. For NATO to operationalize cyberspace as a domain of NATO defense policy and planning — as was agreed at the NATO Warsaw Summit — the Alliance should have authorizations from member states to do more than just provide advice, expertise, training, or education. Similar to how NATO coordinates Allied military forces in the conventional domain, NATO could also be asked to evaluate how member states can develop, synergize, and complement their mutual national cyber defenses. At a minimum, NATO should develop standards and better indicators that allow a standardized measurement of a nation’s annual progress — and should be tasked with testing and measuring members’ capabilities annually. To achieve this objective, a strong cooperation with the European Union is essential. NATO and the EU could work together to design minimum cybersecurity requirements and benchmarks that would also be adopted by the European Defense Agency. Rapid Assessment and Decision-Making Tools The scale, speed, and intensity of today’s cyber-attacks demand a new approach to respond at the political, military, and civilian level. To develop a rapid decision-making process when facing a cyber-attack NATO can take a few effective measures across its organization. First, more resources must be allocated to accurately and quickly detect and define hostile cyber actions. Further work on indications, warnings, and situational awareness is critical. In this context, NATO’s various civil and military intelligence units, inter alia, could have a useful role. In addition, the Supreme Allied Commander Europe (SACEUR) could be granted more powers by the North Atlantic Council in authorizing some of the preparatory procedures. At the same time, NATO headquarters should increase the number of exercises that test rapid decisions-making procedures in complex and demanding cyber crisis-conflict scenarios. Much can also be done at the member-state level. Allies and willing partners should continue to work on improving and updating threat assessments, and facilitating closer intelligence cooperation. In this light, Allies should identify information sharing as a clear requirement and task. NATO could also intensify its interaction with national intelligence services and establish supply chain management partnerships with national industries. Cyber threats come in the form of networks and it takes a similarly well-organized network of international and cross-sector cooperation to defeat those threats. Common Rules of Engagement NATO has not commonly defined the circumstances, conditions, degree, and manner in which the use of force may apply if one of its member states suffers a cyber-attack. Triggering the authorization to use force in the context of Article 5 may be more obvious if a member state faces a large-scale, devastating cyber-attack where the source of the attack can be clearly attributed. But the need is much more urgent to define when and how NATO must respond against the day-to-day cyber intrusions that fall below the threshold of being perceived as a clear act of aggression. NATO policy still allows for too many gray zones that are being exploited by adversaries who are clever enough not to cross a line that would trigger a common response from the Alliance. Cybersecurity incidents like the alleged Russian hack of the Democratic National Committee’s emails show that the United States and the NATO Allies are still unclear about the conditions and manner to respond in cyberspace. The Tallinn Manual published by the NATO CCDCoE offers a set of guidelines on how states can define rules of engagement, countermeasures, retaliation operations, and other forms of response within the context of the international law if they are to face an act of cyber aggression. But NATO is still far removed from having adopted a common view and interpretation on the subject. The North Atlantic Council would still need to assess each individual cyber-attack case by case without the support of standard measurement tools and indicators that can help NATO formulate a proportionate political or military response. As more cyber policies and laws are taking shape, NATO could demonstrate political, military, and intellectual leadership by clearly defining rules of engagement in cyberspace. Consider Offensive Cybersecurity NATO now recognizes a serious cyber-attack as a potential Article 5 trigger. But the doctrine and crisis management conditions enshrined in NATO’s cyber policy puts the emphasis on a defensive posture only. As such, the Alliance fails to recognize cyber as a force multiplier that could be of importance to the defense of NATO nations. Russia for instance considers offensive cyber capabilities to be an integral part of its military power and especially as a way to make up for its relative lack of conventional forces compared to NATO. The rise in connectivity, smartphone proliferation, cloud computing, growth of application development, and other technological advances open new avenues to attackers and force defenders to cover an ever-increasing number of fields. In the long run, NATO’s defensive approach is not sustainable. It is time for NATO to start a debate on offensive cybersecurity and map the feasibility of coordinating counter strikes, and to establish a significant offensive cyber capability. NATO could center this debate on projecting offensive cyber warfare capabilities as a means of deterrence, similar to the perceived value of nuclear weapons to deter attacks against NATO. Offensive security will allow the Alliance to better control the virtual battlefield. There are valuable cyber capabilities worth attaining, including the ability to conduct reconnaissance and surveillance, intercept communications, or deny resources and access. NATO may find increasing support to have a conversation on offensive cyber security with its allies. As member states are increasingly preoccupied with defense and deterrence issues in cyber-space they will show more receptivity to cooperation with NATO on developing centralized offensive cyber capabilities. NATO and Cyber Industry Cooperation Cybersecurity is largely market-driven. Government intelligence capabilities increasingly find it hard to keep up with the requirements for combating the surge in cyber threats. NATO should play a crucial role in facilitating contacts between those member states that seek stronger links with the private sector and encourage the role that industry can play in cyber threat deterrence and intelligence sharing. Flagship initiatives, such as the NATO Industry Cyber Partnership, are important steps in that direction but there is still a need to build more access and trust between NATO governments and industry. Educating member states and partner nations about the role of the private sector in cybersecurity is key. To make the partnership with the industry more effective NATO could play a more important role in mapping and evaluating what kind of cyber defense technologies and intelligence gathering methods the private sector offers, share lessons learned with the member states and encourage capitals to integrate the best practices into capabilities, policy, and implementation planning. NATO can also play an essential role in improving communications and information sharing between the private and the public sectors. More can be done at the NATO level to identify what kind of information between governments and companies can or cannot be shared, to develop standardized methods and formats for information sharing, and to encourage the use of automated platform capabilities to share this information quickly. Build a Robust Public Diplomacy Campaign The first frontier of cyber defense is the individual. Citizens who are digitally empowered, cyber aware, and cyber educated will display a more responsible behavior and automatically increase NATO’s collective security in cyberspace. NATO needs a narrative on why cybersecurity matters beyond public belief that a major cyber-attack is improbable. What can NATO do in cyberspace that national security agencies cannot do? Which level of cybersecurity is needed rather than which one we can afford? NATO societies should be exposed to debate through parliaments, media, nongovernmental organizations, and academia. Externally, the Alliance must adapt to the reality that countries hostile to NATO will continue to use their own cyber capabilities and massive state propaganda organizations to attack NATO systems and discredit everything the Alliance does. NATO has to be able to engage in and win this information war at the elite decision-maker and opinion-former levels rather than simply raise awareness of its existence and activities among a global public.

### S – NATO Key

#### Reinforcement of NATO crucial - The invasion of Ukraine shows the need for a greater strategic cooperation against Russia

Cordesman and Hwang 2/16/22

Anthony H. Cordesman is the Emeritus Chair in Strategy at the Center for Strategic and International Studies (CSIS). He has previously served in the Office of the Secretary of Defense, the National Security Council, the State Department, and the Department of Energy. Grace M. Hwang holds Ph.D. & M.S. degrees in Biophysics and Structural Biology from Brandeis University. Her doctoral dissertation was on computational neuroscience where she specialized in analyzing cohorts of human brainwaves to understand the neural basis of visual and verbal memory formation. She developed novel nonparametric statistical techniques for high-dimensional data that enabled robust across- and within-subject multi-factorial analysis. NATO and Ukraine: Reshaping NATO to Meet the Russian and Chinese Challenge, CSIS, <https://csis-websiteprod.s3.amazonaws.com/s3fspublic/publication/220216_Cordesman_NATO_Ukraine.pdf?cS8vKRNOdoYvg3t_y6QMZMSCpadAo90a>

If the Ukraine crisis ends in anything other than a major conflict, the U.S. and its NATO allies must now take a far **more serious** look at how they are shaping the future defense of Europe, the Atlantic, and the Mediterranean if NATO is to hold together; create an effective structure of deterrence and defense; and ensure that the West, other democracies, and other major powers can compete with both Russia and China. In doing so, the U.S. and all of its strategic partners in NATO must focus on correcting the major shortfalls in the military and deterrent capabilities of each member state, instead of fixating on NATO-wide concepts or common funding efforts. This is not simply a matter of setting broad priorities and issuing new strategies. Military reality is not an exercise in writing more vague generic statements of good intentions. The Russian threat to Ukraine has made it all too clear that the U.S. and its allies must create and actually implement meaningful force plans instead of issuing more strategic rhetoric. NATO must work together to assess the role each country should play in creating a more effective alliance rather than referring to NATO-wide generalities. Member countries must develop credible Cordesman: NATO and the Lessons of the Ukraine Crisis February 16, 2022 4 force plans, programs, and priorities that reflect the radically different capabilities of given NATO countries, and they must find solutions to their radically different funding needs and capabilities by developing a suitable mix of very different national defense budgets. In doing so, the U.S. must fully recognize its own blunders in focusing on burden-sharing. The U.S. needs to fully consult with its NATO and other strategic partners. The U.S. needs to make it clear that there is no case for some “European” solution to Western security, and it must avoid any future cases like the casual way in which the U.S. engaged Australia and the UK in a closer alliance by suddenly substituting U.S. nuclear submarines for French conventional submarines. As is the case in the Middle East and the rest of the world, the U.S. cannot afford to constantly raise new series of doubts about the ability to rely on the U.S. as a strategic partner. The U.S. also needs to revitalize its focus on NATO and Europe. China’s emergence as a major strategic challenge is all too real, but Europe and Russia are just as critical to an effective U.S. strategic posture as are China and Asia. The recent U.S. focus on the Chinese threat is all too necessary, but so is the U.S. focus on NATO, Russia, and the rest of the world. The U.S. must treat all its strategic patterns as real partners, and the U.S. needs to recognize that its strategic force plans must continue to be global – not swing from region to region. At the same time, Europe needs to be far more realistic about its strategic dependence on U.S. forces and the major shortfall in most European forces. European members of NATO need to do far more to improve the modernization, interoperability, sustainability, and deployment capabilities of many of its member states. They need to recognize there is no credible European alternative to NATO and an Atlantic alliance, and they should focus on nation-by-nation force improvements, rather than burden-sharing and arbitrary spending levels. As the following summary analysis of current national forces shows, NATO not only must deal with many individual sets of national military weaknesses, it must address a wide range of **“emerging and disruptive**” technologies that are steadily reshaping military forces, tactics, and capabilities.1 Once again, it must be stressed that this cannot be done by announcing new NATO strategies in broad terms or setting common goals for the entire alliance. It also cannot be done by repeatedly issuing equally vacuous national defense white papers that do not commit countries to specific actions, plan, programs, and budgets or that do not honestly address the problems in current national forces. Both the U.S. and European nations need to properly assess national defense spending levels in terms of actual country’s individual military requirements and spending capability. NATO-wide quotes are pointless. At the same time. Such efforts need to be driven by net assessments of the relative size of Russian and Belarusian military forces, modernization, and spending, and they need end the present emphasis on burden-sharing by arbitrary percentage of GDP and equipment spending. The following data on Russian, U.S., and NATO European military spending alone make it clear that the U.S., all other member countries, and NATO as an organization need to use such net assessments of their present and future capability to **deter and defend against Russia**, determine what actions member countries should actually do to improve their forces, and set individual national goals for given forces on modernization at a time when there is an ongoing revolution in military affairs that will last for at least the next few decades. They also need to plan collectively Cordesman: NATO and the Lessons of the Ukraine Crisis February 16, 2022 5 to deal with the ongoing emergence of China as a far larger and more effective military superpower than Russia – and in doing so to create a stable balance of deterrence in dealing with both Russia and China.

#### Nato key to Global stability—Nato radiates security

David Wemer; July 5, 2018; ”Here’s why the United States needs NATO”;New Atlantist;https://www.atlanticcouncil.org/blogs/new-atlanticist/here-s-why-the-united-states-needs-nato/

NATO promotes peace within Europe and deters major US adversaries from launching large-scale conventional wars. World War II cost the United States more than 400,000 lives and an estimated $4.1 trillion (in 2011 dollars). NATO has been key to preserving peace within the European continent and preventing other adversaries from launching a major conventional war. According to credible sources, a major conventional war today could cost the United States upwards of $2.5 trillion per year. NATO also promotes the American values of democracy and rule of law. Twenty-six of the twenty-nine NATO member states were labelled as “free” by Freedom House in 2018. By comparison, just 39 percent of the world’s population lives in “free” countries. NATO is a force multiplier that gives the United States access to military tools in greater numbers than it can achieve by itself. Non-US NATO members have 1,857,000 active duty service members and 1,232,290 reservists. The seven largest non-US NATO member armies have the same number of active duty troops as the United States (1.3 million). Non-US NATO members can deploy 6,983 battle tanks, 34,000 armored vehicles, 2,600 combat aircraft, 382 attack helicopters, 252 major naval craft (including submarines), and 1,582 patrol and surface combatants. France and the United Kingdom alone provide 30 percent of the Alliance’s ballistic-missile-submarine fleet. NATO’s European members are beginning to host the first stages of the Alliance’s new ballistic-missile-defense system aimed at preventing long-range attacks by rogue states on the United States and Europe. NATO members frequently share intelligence across the Alliance, aiding US operations and intelligence-gathering. The United Kingdom, France, and Germany alone add 40,000 intelligence personnel to the Alliance’s intelligence capabilities. Non-US NATO members host twenty-eight US main operating bases in Europe, which cut down on the time needed for the United States to respond to a crisis and are critical for US missions in the Middle East and North Africa. In 2009, for example, Germany contributed $800 million to offset and improve its US bases. NATO undertakes numerous missions to protect member states and promote security around the globe. NATO has five active missions around the world deploying 18,000 troops. Since the end of the Cold War, NATO has completed thirteen missions including two in the United States (Hurricane Katrina relief and post-9/11 air reconnaissance patrol). NATO allies contributed thousands of troops to the International Security Assistance Force in Afghanistan, including 38,000 in 2011, saving the United States an estimated $49 billion that year. The operation in Afghanistan was the first and only time NATO’s mutual defense commitment was invoked. Non-US members sustained more than 1,000 combat deaths in Afghanistan, with an additional one hundred lost by NATO partners. Non-US NATO members contributed more than 60 percent of assets for Operation Unified Protector in Libya. Non-US Coalition members flew one-third of all coalition airstrikes against the Islamic State of Iraq and al-Sham (ISIS) in Operation Inherent Resolve. NATO’s Operation Ocean Shield against piracy in the Gulf of Aden has been led at different times by Denmark, Spain, Norway, Italy, the Netherlands, the United Kingdom, and Portugal. NATO supports and protects the economies of Europe, which are critical to the health of the US economy. US trade with the European Union reached $699 billion in 2015, only made possible because of the security and stability provided by NATO. US exports to the former Communist NATO member states (not including East Germany) grew from $0.9 billion in 1989 to $9.4 billion in 2016. Non-US NATO members rely heavily on the US defense industry to supply their forces. Currently, European members are planning to purchase as many as 500 new F-35s from the United States.

#### NATO is key to preventing war– it keeps Russia at bay

Hooker 4/21/22

*Dr. Richard D. Hooker, Jr. is a nonresident senior fellow with the Atlantic Council* [ March 2022 “How the West can manage escalation in Ukraine and beyond.” https://www.atlanticcouncil.org/in-depth-research-reports/report/managing-escalation-in-ukraine/. Accessed 26 Apr. 2022.

Moscow’s invasion of Ukraine is transforming Europe’s security architecture, as well as NATO’s strategic priorities and its defense and deterrence posture. Russia’s ruthless aggression and NATO’s response increase the possibility of purposeful or inadvertent escalation in Europe. Whether this takes the form of heightened conflict in Ukraine, increased tension across the whole or parts of NATO’s eastern flank—from Ukraine and the Black Sea to the Baltic Region and the High North—or in non-kinetic, subthreshold domains, understanding how these dynamics might degrade transatlantic stability is critical. This study will seek to identify key rungs on the escalation ladder around the war in Ukraine; assess how the current crisis might escalate inside Ukraine and across NATO’s eastern flank; explore how the US and NATO posture can prevent or limit escalation; and offer recommendations for how the United States and NATO can adapt their strategy, posture, and activities to manage escalatory dynamics. In response to the invasion of Ukraine, the West has imposed stinging sanctions, disrupting the Russian economy and forcing the Kremlin to burn through its financial reserves. Major Russian banks have been disconnected from SWIFT, the international system that facilitates financial transactions, while some oligarchs have been sanctioned. Many allies and partners have provided massive financial and material aid—in the form of funding, as well as anti-tank and air-defense systems and other military equipment—to bolster Ukrainian resistance. This assistance has helped to stiffen an already stout Ukrainian defense, which has inflicted heavy losses on the Russian military. Vladimir Putin now faces the real possibility of a stalled offensive, or even outright defeat. In this circumstance, Russia still has cards to play. Failure in Ukraine places Putin’s political survival at risk and he is, therefore, unlikely to withdraw. His present difficulties are more likely to provoke escalation within or around Ukraine, both in the military realm and in other domains. As he climbs the escalation ladder, Putin’s risk tolerance will increase, as his key subordinates will surely realize. The ultimate risks, however, are removal from office, imprisonment, or even execution. Accordingly, Putin is far more likely to press harder in Ukraine than to acquiesce to a negotiated settlement that leaves him without tangible gains.¶ The following discussion of Russian escalatory options is linked to the progress of the campaign in Ukraine and presents alternate scenarios based on Russian progress or failure and the degree to which the West provides critical support and/or direct intervention. Escalatory steps are described in ascending order of severity and risk. Response options to control or mitigate Russian escalation follow. It is important to note that Russian, Ukrainian, and Western perspectives or “lenses” on what is escalatory may differ significantly in both time and space. This factor must be borne in mind when assessing adversary actions. ¶As Putin and his senior advisers consider options, conditions on the ground will drive their calculus. Should the Russian military manage to recover its footing and resume progress, however halting, more extreme options may be held in reserve. If the campaign evolves into a “frozen” conflict, like the Donbas but on a larger scale, Putin’s focus will shift to destabilizing the Volodymyr Zelenskyy regime in Kyiv and sanctions relief. Should Ukraine achieve decisive success in recovering its national territory, Putin’s survival may be at risk, and incentives to employ harsher and more high-risk measures will grow. Escalation to each of the below “rungs” will depend on Putin’s perception and assessment of how the campaign is progressing and the prospects for ultimate success or failure. Though speculative, likely triggers for escalation into each subsequent phase of the conflict might include: An assessment that the campaign has stalled temporarily and different approaches are needed to regain momentum; An assessment that the campaign has stalled outright and recovery is unlikely without more extreme measures; and An assessment that defeat is imminent, and that Putin may fall from power, placing all his options on the table. As the conflict drags on, NATO and European Union (EU) actions can be decisive one way or the other, as described further below.

### S - US Key

#### US leadership is key.

Williams et al ’21 (Brandon Williams with contributions from Veronica Chinchilla, Evan Lisman, Amanda Tobey, and Emilyn Tuomala. Brandon is a PhD, postdoctoral research fellow at the Center for Global Security Research. “US. AND ALLIED CY BER SECURITY COOPERATION IN THE INDO-PACIFIC,” Center for Global Security Research, March 30, 31 and April 1, 2021, https://www.osti.gov/servlets/purl/1787217)-mikee

Cooperation improves when threat perceptions converge and when the United States exercises thoughtful leadership. It erodes when efforts to promote convergence lapse, when tactical responses take precedence over strategic trust building, and when the United States sets aside the effort to promote cooperation. US. leadership is essential, as every US. ally faces real restraints and limits in improving cyber security on its own. The United States has an abundance of bureaucratic resources compared to its allies, but it still lacks a clear vision on how to build a collective and collaborative capacity in a domain centered on secrecy and rapid response. Leadership must be built on meaningful engagement and consultation on all these matters and an appropriate modesty about our collective capacity to meet the challenges ahead. Looking to the future of cybersecurity cooperation among the United States and its Indo- Pacific allies, it is easy to identify numerous challenges, usually arising from frictions over threat assessments, desired end-states, doctrine, language, and the different public-private sector relationships in each country. But these challenges also represent opportunities, places where concrete progress can be made and where frictions lend themselves to concerted action. Progress in working one will reinforce progress in working the others. Unity of command may be a bridge too far, near-unity of action is attainable. An achievable goal is to a place where the US and its allies can convey to an adversary that ”to beat any one of us, you to have to beat all of us.”

## AT: OCOs DA

### OCOs Solve

#### Developing an integrated OCO doctrine among NATO allies solves cyberconflict

Lewis ’15 [James; October; Director and Senior Fellow, Strategic Technologies Program, Center for Strategic and International Studies; "THE ROLE OF OFFENSIVE CYBER OPERATIONS IN NATO’S COLLECTIVE DEFENCE,” Tallin Paper No. 8, A NATO CCDCOE Publication on Strategic Cyber Security, https://www.ccdcoe.org/uploads/2018/10/TP\_08\_2015\_0.pdf]

The central question for NATO’s cyber doctrine is how the lack of an articulated offensive cyber capability affects its ability to deter or defend. Put another way, can any military force credibly claim to have advanced capabilities if it does not include offensive cyber operations in its arsenal? Offensive capabilities, unlike NATO’s current defensive posture, involve deliberate intrusions into opponent networks or systems with the intention of causing disruption, damage or destruction. The question of NATO and offensive cyber capabilities touches on a range of sensitive political issues that militate against any change in policy in the near term.

The US has always been overly secretive about its offensive cyber capabilities, even after a flood of media leaks have made the most sensitive doctrine publicly available. This secrecy has carried over into NATO, and is unhelpful in that it increases the likelihood of opponents miscalculating as they consider the risks of using force or coercion against NATO members or interests. A lack of public discourse on offensive cyber operations undercuts the legitimacy of NATO operations by failing to build public understanding, and leaves NATO open to charges of sinister plots, since denial of offensive capabilities is not credible when two NATO members are world leaders in cyber operations.

Parallels between cyber operations and nuclear strategy are usually misleading, but cannot always be dismissed. The parallel for NATO is that cyber attack is a “weapon” with both strategic and tactical uses, which only a few NATO members possess. Unlike nuclear weapons, however, the procedures for integrating offensive cyber operations into NATO’s defensive actions are not at all obvious, if they exist. NATO will need to describe how the cyber capabilities possessed by a few of its members will support NATO’s defensive activities, and NATO’s credibility in defence requires some public discussion on the use of offensive cyber operations.

There has been a confusing debate over the merits of cyber deterrence, but one conclusion that we can draw from this discussion is that both the contribution of cyber operations to deterrence and the ability to deter cyber attack work best when embedded in a larger military force structure. Adding offensive cyber capabilities to NATO’s force structure and response doctrine will increase its deterrent capabilities – by how much is unclear, but what is clear is that a failure to add cyber capabilities will erode a credible deterrent as cyber operations are increasingly embedded into military operations.5

Beyond deterrence, two other factors point to the need for additional consideration of NATO’s public posture on offensive cyber operations. The first is that cyber techniques are essential for the kinds of combat operations that NATO forces may carry out in the future. No modern air force would enter into combat without electronic warfare (EW) capabilities; as cyber and EW merge into a single activity, air operations will require cyber support. The same is true for special forces operations. Offensive cyber capabilities will shape the battlefields of the future.

Second, NATO’s potential opponents will use cyber techniques in new ways, in what some have called “hybrid warfare”.6 These include countries traditionally of concern to NATO, but cyber threats could also come from new actors, such as Iran or North Korea, and proxy or non-state actors such as the Syrian Electronic Army. These nations and groups, using cyber techniques, now have new ways to strike NATO countries.

Military doctrine is changing as opponents seek to circumvent US military power and use a blend of political action and “influence operations”, special forces, proxies and irregular units, unconventional tactics and cyber techniques to apply force to gain their ends. Cyber techniques for political action and “influence operations” are not intended to destroy or disrupt, but rather to put coercive political pressure on targets. This new style of warfare will challenge planning for mutual defence. For these reasons, the need for more than defensive or technical cyber capabilities will increase.7

#### NATO OCOs key to win cyberwar---prevents nuclear meltdowns and financial collapse

Iftimie ’20 [Ion A.; May; PhD, Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business; NDC Policy Brief, “NATO's needed offensive cyber capabilities,” no. 10]

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

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.

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 member states.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.

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 web- sites". 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 plat-forms, 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 ■UK

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 do-main. 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 cy-ber 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 Brus-sels 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 opera-tions forces;

• Imposing cyber sanctions;

• Conducting offensive cyber operations to achieve A2/AD effects in the cyber domain;

Offensive cyber operations have already been used for the purpose of achieving A2/AD by NATO member states

• Triggering Article 5 of the Treaty; and

• Conducting offensive cyber operations in com-bination with other maneuver forces across all operational domains.

12 Cyber sanctions are defined here as "the actual or threatened restriction of digital transactions to affect a behavioural change by a NATO adversary through the introduction of psychological pressure against its political leaders and populace"; see A. Iftimie, "Cyber sanctions: weapo- nizing the embargo of flagged data in a fragmented internet", Journal of Information Warfare, Vol.19, No.1, 2020, p.52.

NATO Cyber Rapid Reaction teams are already equipped to conduct defensive cyber operations in support of member states if called upon. A mandate of cyber defence and security implies, however, that NATO also starts to engage in active military measures to deny, degrade, disrupt, deceive, or destroy an adversary's offensive cyber capabilities. This requires the development of not only offensive cyber A2/AD capabilities by Allies, but also the restructuring of the NATO command structures, policies, processes

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

(procurement, intelligence, operations, etc.) and engagements needed to integrate them by the Alliance. NATO coordination with both national and regional entities charged with cyber security aspects will, in particular, need to be enhanced. Many agreements already exist in the realm of defensive cyber at national and regional levels (as seen with the 2016 NATO-EU Technical Arrangement on Cyber Defence), but political consensus among Allies is missing on whether they should be expanded to incorporate the collective use of offensive cyber A2/AD capabilities.

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 re-spond 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.

#### NATO needs to be more offensive when dealing with cybersecurity – waiting to respond will cause NATO to lose the fight in Cyberspace

Kramer et al ‘20

[Franklin](https://www.businessinsider.com/author/ben-winck) D. Kramer; Distinguished fellow and board director at Atlantic Council. Expert in cybersecurity, defense policy, and non-traditional threats; Lauren M. Speranza; Director of the Transatlantic Defense and Security program at the Center for European Policy Analysis (CEPA); Conor Rodihan; Associate director at Scowcroft Center for Strategy and Security; NATO needs continuous responses in cyberspace; Atlantic Council; https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/

Third, NATO should coordinate a strategy of persistent engagement to reduce Russian and Chinese activities to undercut the Alliance in cyberspace. The concept of persistent engagement was developed by US Cyber Command, but the rationale likewise applies to NATO, deriving from the need to combat the continuous campaigns of cyberattacks coming from Russia and China. Persistent engagement involves tracking adversaries, understanding their goals, analyzing the tools used for attacks, and taking actions to degrade their capabilities to blunt ongoing, or prevent future, attacks. The Alliance needs a persistent engagement cyber strategy as a key element of its deterrence and defense. Customary international law, including the law of countermeasures, pleas of necessity, and other cyber norms, provides the international legal basis for a strategy of persistent engagement. Because NATO Allies have already been attacked and are continuously being targeted by these adversaries, offensive actions to counter such activities are justified, as long as they are conducted proportionately. While persistent engagement arguably could increase instability in cyberspace, Alliance inaction is far more dangerous. If Russia and China perceive no consequences to their malign actions in cyberspace, they will only continue and even intensify them. Inasmuch as NATO capabilities generally reside in nations, NATO nations are the appropriate vehicle to implement persistent engagement. However, many Allies lack the capacity to undertake persistent engagement on their own. As a result, NATO should leverage its collective nature to help Allies coordinate a strategy of persistent engagement. NATO should focus its persistent engagement efforts in three areas of high consequence to member nations: 1) disruptions of key critical infrastructure (e.g. electric grids, telecommunications networks, energy pipelines, and finance systems); 2) cyber espionage to undermine NATO military capabilities and advanced defense technologies; and 3) manipulation of Allies’ democratic processes, such as elections. NATO support to Allies in these areas is fundamental to its core task of collective defense and security. To accomplish persistent engagement effectively in an Alliance context, NATO should leverage its intelligence and defense planning capacities to develop a system for Allies to constantly track cyber threats from Russia and China. Through its Intelligence and Security division, NATO should gather intelligence on which Allied critical infrastructure, military capabilities, or democratic processes are being targeted. Using this information, NATO’s Cyberspace Operations Center (CYOC) could outline ways to diminish Russian and Chinese capabilities to execute such attacks. The CYOC should share its analyses with pre-designated Allies who would work with targeted countries and employ their own cyber effects against the identified threats. Nine NATO nations have already volunteered to provide such effects in support of NATO activities. These cyber-capable Allies would be responsible for persistently disrupting adversaries’ cyber activities based on NATO’s guidance. This model would make NATO’s CYOC a planning hub for an Alliance-wide approach to persistent engagement. It would allow NATO to empower its members to take individual or multilateral actions against adversaries’ hybrid campaigns in cyberspace. While NATO remains a defensive alliance, waiting to respond to each cyber incident it suffers will cost NATO the “fight” in cyberspace. Facing continuous hybrid campaigns from Russia and China, NATO needs a more proactive cyber approach to support Allies, even before the Article 5 collective defense threshold is met. By building resilient cybersecurity architectures, adopting active cyber defense, and coordinating a strategy of persistent engagement, the Alliance can create its own continuous response campaign to effectively respond to attacks in cyberspace.

#### Cyber intelligence solves and is better suited than deterrence---the US can effectively reduce the fog of war and reduce the severity of OCOs

Rovner 20—Associate professor in the School of International Service at American University, in 2018 and 2019 he served as scholar-in-residence at the National Security Agency and U.S. Cyber Command [Joshua Rovner, 3/26/2020, “The Intelligence Contest in Cyberspace”, Lawfare Blog, <https://www.lawfareblog.com/intelligence-contest-cyberspace>] AMarb

The ongoing competition in cyberspace is largely an intelligence contest. Although the technology is different, the underlying contest exhibits all the characteristics of traditional spy-versus-spy battles.

An intelligence contest is an effort to steal secrets and exploit them for relative advantage. Great powers today are using cyberspace with vigor, seeking to steal communications in transit and data at rest. China’s effort to steal intellectual property via cyberspace was famously described as the “most significant transfer of wealth in history.” China has attempted to exploit this effort to improve its military capabilities, with mixed results. Russia has also become more active in cyberspace espionage, targeting the United States and its partners abroad.

Intelligence contests also include sabotage. All bureaucracies suffer from some amount of friction: the inevitable daily hiccups that slow down operations and make organizations less efficient. Sabotage in cyberspace weaponizes friction to undermine rival capabilities and morale. Offensive cyberspace operations are well suited for this task because they offer a range of tools for the saboteur. States can opt for cheap and easy harassment campaigns like denial of service attacks, or they can engineer sophisticated operations against specific facilities. In either case, the benefits to the saboteur are both practical and psychological. Practical results include harm to networks, data, and infrastructure, all of which forces the target to spend time and money on recovery. Psychological results are equally important. It may not be necessary to cause physical damage if personnel in target organizations fall victim to frustration and finger pointing.

Finally, intelligence contests involve efforts to pre-position espionage assets that may be useful in war. Military organizations increasingly rely on cyberspace for organizing and directing conventional campaigns. Intelligence agencies have an obvious interest in monitoring their efforts. Gaining access to adversary networks makes it possible to reduce the fog of war in the case of a conflict. It also suggests the ability to confuse enemies by inhibiting their communications or flooding the zone with disinformation.

Cyberspace is a good venue for intelligence but a bad one for deterrence. It is good for intelligence because the ubiquity of cyberspace in organizational management creates extraordinary opportunities for surveillance. States that depend on cyberspace for normal operations also make themselves vulnerable to sabotage. Even modest offensive cyber operations can inject friction into adversary organizations.

Deterrence is different. It is difficult to deter states from activities below the line of armed conflict because retaliatory threats inherently lack credibility. No one is likely to believe that states will use violence to stop espionage, for instance, which probably explains why small states have spied on large ones for centuries. More importantly, victims are surprisingly tolerant of cyber operations. Research suggests that individuals are less willing to retaliate against cyber blows than physical violence. If this is correct, then strategies based on punishment are likely to fail. Deterrence by denial is also likely to disappoint, because the barriers to entry for espionage and harassment are relatively low. States will continue to conduct cyber intrusions even if previous efforts were unsuccessful.

There are important exceptions to this rule. Deterring major attacks against critical infrastructure is possible, for instance, because these attacks threaten significant harm to civilians. Deterring this kind of cyberspace operation makes sense because anyone considering such an attack would risk a ferocious response. Executing large-scale attacks on infrastructure probably also requires a lot of time, money and organization. Adversaries would surely think twice about that investment, especially if the United States issues clear deterrent threats. But deterrence is mostly irrelevant in cyberspace, because most activities fall well short of threats to infrastructure. Understanding the present problem in terms of deterrence theory is not particularly helpful.

At best, a well-fought intelligence contest can slowly convince adversaries that certain targets and methods are beyond the pale. During the Cold War, Soviet and U.S. intelligence professionals came to observe some rules of the game. Aggressive counterintelligence methods were expected, for example, but not against family members. Neither side could deter intelligence efforts, but they could structure the contest in order to reduce the risk.

What does the future hold for the intelligence contest in cyberspace? The good news is that the United States is exceptionally well positioned to compete. It possesses extraordinary technical and human resources, in both the public and private sectors. Its intelligence agencies are the largest and richest in the world. It also benefits from decades of experience competing against capable rivals. This is not the first time the U.S. intelligence community has dealt with committed and occasionally ruthless intelligence foes.

The bad news is that it will not be easy to know victory when we see it. Intelligence contests are inherently hard to measure. They are allergic to quantification, and the increasing volume of cyberspace activities means that more attacks will occur even if there is a net gain in cybersecurity. Observers will understandably be skeptical if U.S. officials claim success in the midst of high-profile security incidents. Moreover, progress reports will reflect differing value judgments. Those who believe the government is obligated to protect private firms will view all breaches as failures. Those who believe that the government has no such obligation will likely view private-sector attacks as unfortunate but unrelated to the government’s effort against foreign adversaries.

Although recognizing success will be hard, it is not impossible. Rough indicators may offer useful clues. If rules of the game are taking hold in cyberspace, we should see changes in patterns of cyber operations. Attackers will focus on some types of targets and increasingly ignore others. The percentage of state attacks on private firms and nongovernmental organizations should decrease.

Intelligence should also be able to monitor the frequency and severity of offensive cyberspace operations. Success will obtain when rivals come to see the risks of action and the value of restraint. While they will not cease activities, high-profile damaging attacks will become rare. States will also eschew the use of malware that they cannot control; instead, they will use customized payloads against specific targets and take steps to ensure that they do not inadvertently affect other systems. Fearful of letting their intelligence activities spill into other domains, they will design operations to avoid unwanted contagion.

### Terrorism

#### OCO enabled Intelligence is essential for counterterrorism

Bronk 17—Assistant Professor of computer and information systems at the University of Houston’s College of Technology [Dr. Chris Bronk and Gregory Anderson (Master’s candidate for the Information Systems Security program at the University of Houston and is currently a research assistant under Dr. Chris Bronk and Dr. Arthur Conklin), Winter 2017, “Encounter Battle: Engaging ISIL in Cyberspace”, The Cyber Defense Review, Vol. 2, No. 1, pp. 93-108, <https://www.jstor.org/stable/pdf/26267403.pdf>, Accessed through the Wake Forest Library] AMarb

There will no doubt be difficulties incorporating cyber operations components into overall US strategy countering ISIL and other non-state adversaries; however, it is clear national security leadership in Washington will leverage cyber capabilities more significantly. One issue that will continue to dog offensive cyber operations and intelligence activities is the equities question—should the US government turn over knowledge it accrues regarding cyber vulnerabilities to the technology industry so that they may be repaired. For instance, is it more desirable for USCYBERCOM and the National Security Agency (NSA) to keep information regarding broken encryption implementations or software as was alleged in the Heartbleed bug in the OpenSSL software libraries? Issues such as this will be a major policy question to consider.

Ultimately, the cyber conflict against ISIL will serve as a template for future cyber action against terror groups, insurgents, and violent transnational criminal syndicates. Looking backward, we can see the effective application of robust signals intelligence capabilities have been. Consider US support of Colombian operations against the Fuerzas Armadas Revolucionarias de Colombia (FARC). There can be little doubt that the Colombian military and police were made significantly more effective with the addition of US intelligence capabilities. Policymakers are keen to eradicate or at least damage ISIL but will need to ask how cyber weapons can frustrate it as much as anything else can. The more cyber tactics can short-circuit ISIL’s operational capabilities, the better. What is necessary for US cyber operators are clear objectives from senior leadership on what they want to produce. The engineers that build USCYBERCOM’s tools and the hackers that serve as its operational forces can easily enough push back on what they believe is the art of the possible.

#### Terrorism causes nuclear war

Arguello 18—Founder and chair of the NPSGlobal Foundation, and head of the secretariat of the Latin American and Caribbean Leadership Network, degree in physics, a Master’s in business administration, and completed graduate studies in defense and security, previously worked on nuclear projects for the Argentine National Atomic Energy Commission. She is a member of the Steering Committee of the Fissile Materials Working Group, and a Chatham House Associate Fellow. Since 2010, she has participated in all the official non-governmental events at the Nuclear Security Summits [Irma Arguello and Emiliano J. Buis (a lawyer specializing in international law. He holds a PhD from the University of Buenos Aires (UBA), a Master’s in Human and Social Sciences from the University of Paris/Panthéon-Sorbonne, and a postgraduate diploma in national defense from the National Defense School. Currently he is a professor in international law at UBA, and co-director of the UNICEN Center for Human Rights in Azul. He is also a researcher and professor at the NPSGlobal Foundation), February 2018, “The global impacts of a terrorist nuclear attack: What would happen? What should we do?,” Bulletin of the Atomic Scientists, 74:2, 114-119, Accessed through the Wake Forest Library] AMarb

Though hard to accept, the detonation of a nuclear device – by states or non-state actors – is today a plausible scenario. And while much of the world’s focus has been on the current nuclear weapons arsenals possessed by states – about 14,550 warheads, all of which carry the risk of intentional or unintentional use – the threat of nuclear terrorism is here and increasing. For more than a decade, Al Qaeda, Aum Shinrikyo, and other terrorist groups have expressed their desire to acquire fissile material to build and detonate an improvised nuclear bomb. None of them could fulfill that goal – so far. But that does not mean that they will not succeed in the future. Making matters worse, there is evidence of an illicit market for nuclear weapons-usable materials. There are sellers in search of potential buyers, as shown by the dismantlement of a nuclear smuggling network in Moldova in 2015. There certainly are plenty of sites from which to obtain nuclear material. According to the 2016 Nuclear Security Index by the Nuclear Threat Initiative, 24 countries still host inventories of nuclear weapons-usable materials, stored in facilities with different degrees of security. And in terms of risk, it is not necessary for a given country to possess nuclear weapons, weapons-usable materials, or nuclear facilities for it to be useful to nuclear terrorists: Structural and institutional weaknesses in a country may make it favorable for the illicit trade of materials. Permeable boundaries, high levels of corruption, weaknesses in judicial systems, and consequent impunity may give rise to a series of transactions and other events, which could end in a nuclear attack. The truth is that, at this stage, no country in possession of nuclear weapons or weapons-usable materials can guarantee their full protection against nuclear terrorism or nuclear smuggling. Because we live in a world of growing insecurity, where explicit and tacit agreements between the relevant powers – which upheld global stability during the post-Cold War – are giving way to increasing mistrust and hostility, a question arises: How would our lives be affected if a current terrorist group such as the Islamic State (ISIS), or new terrorist groups in the future, succeed in evolving from today’s Manchester style “low-tech” attacks to a “high-tech” one, involving a nuclear bomb, detonated in a capital city, anywhere in the world? We attempted to answer this question in a report developed by a high-level multidisciplinary expert group convened by the NPSGlobal Foundation for the Latin American and Caribbean Leadership Network. We found that there would be multiple harmful effects that would spread promptly around the globe (Arguello and Buis 2016); a more detailed analysis is below, which highlights the need for the creation of a comprehensive nuclear security system. The consequences of a terrorist nuclear attack A small and primitive 1-kiloton fission bomb (with a yield of about one-fifteenth of the one dropped on Hiroshima, and certainly much less sophisticated; cf. Figure 1), detonated in any large capital city of the developed world, would cause an unprecedented catastrophic scenario. An estimate of direct effects in the attack’s location includes a death toll of 7,300-to-23,000 people and 12,600-to-57,000 people injured, depending on the target’s geography and population density. Total physical destruction of the city’s infrastructure, due to the blast (shock wave) and thermal radiation, would cover a radius of about 500 meters from the point of detonation (also known as ground zero), while ionizing radiation greater than 5 Sieverts – compatible with the deadly acute radiation syndrome – would expand within an 850-meter radius. From the environmental point of view, such an area would be unusable for years. In addition, radioactive fallout would expand in an area of about 300 square kilometers, depending on meteorological conditions (cf. Figure 2). But the consequences would go far beyond the effects in the target country, however, and promptly propagate worldwide. Global and national security, economy and finance, international governance and its framework, national political systems, and the behavior of governments and individuals would all be put under severe trial. The severity of the effects at a national level, however, would depend on the countries’ level of development, geopolitical location, and resilience. Global security and regional/national defense schemes would be strongly affected. An increase in global distrust would spark rising tensions among countries and blocs, that could even lead to the brink of nuclear weapons use by states (if, for instance, a sponsor country is identified). The consequences of such a shocking scenario would include a decrease in states’ self-control, an escalation of present conflicts and the emergence of new ones, accompanied by an increase in military unilateralism and military expenditures.

### North Korea

#### Strategic intel based OCOs enables successful damage limitation against North Korea

Long 17—Senior Political Scientist at the RAND Corporation and non-resident Senior Fellow at the Foreign Policy Research Institute. He was previously an Associate Professor at Columbia University’s School of International and Public Affairs [Austin, 2017, “A cyber SIOP? Operational considerations for strategic offensive cyber planning”, Journal of Cybersecurity, 3(1), 19–28, doi: 10.1093/cybsec/tyw016, Accessed through the Wake Forest Library] AMarb

In contrast, strategic OCO may be very useful for achieving damage limitation objectives, particularly against regional powers like North Korea. Indeed former Deputy Secretary of Defense John Harvey has called for a comprehensive effort to negate North Korea’s nuclear arsenal, including: Cyber capabilities to disrupt warhead arming and firing systems, or cause flaws to be introduced into warhead designs, so that any arriving warheads are duds. On this last point, foreign “assistance” to North Korea’s nuclear program is a problem, but it is also an opportunity. Under such conditions, North Korea’s leaders would no longer “own” their nuclear weapons — in a sense, we would. A bit fanciful? Not necessarily. The technologies, subsystems and capabilities exist today to address each one of these goals notwithstanding the need for a bit of luck here and there. It is well within the realm of technical possibility [23]. Thus, the target choice would be less restricted in planning for damage limitation than in escalation control – essentially everything would be fair game. Yet this has escalation risks unique to OCO – establishing the accesses needed for OCO could be escalatory, as discussed in the next section.

#### Damage limitation based on intelligence solves a nuclear crisis on the Korean peninsula

Manzo 18—Research Analyst at the Center for Naval Analysis [Vince A. Manzo and John K. Warden (Senior Policy Analyst on the Strategic Analysis & Assessments team at Science Applications International Corporation), Policy Roundtable: Are There any Good Choices When it Comes to North Korea?, “The Least Bad Option: Damage Limitation and U.S. Deterrence Strategy toward North Korea”, Texas National Security Review, <https://tnsr.org/roundtable/policy-roundtable-good-choices-comes-north-korea/#article>, language edited change denoted by brackets] AMarb

A central element of U.S. long-term strategy for deterring a nuclear-armed North Korea and assuring South Korea and Japan should be to maintain robust “damage-limitation capabilities” to keep pace with North Korea’s advancing nuclear forces. By damage-limitation capabilities, we mean military capabilities that would allow the United States – in a conflict – to use offensive and defensive means to significantly reduce North Korea’s ability to conduct successful nuclear strikes against it and its allies. Broadly, these capabilities would include three key elements: intelligence, surveillance, and reconnaissance (ISR) capabilities to locate and track North Korean nuclear forces, strike capabilities to ~~disable~~ [stop] nuclear-armed delivery vehicles or disrupt their command and control, and defenses to intercept nuclear-armed missiles once North Korea has launched them.

Of course, the United States has significant ISR, strike, and missile defense capabilities today. But as North Korea’s nuclear weapons force becomes larger and more sophisticated, the United States will need to keep pace, which will require examining North Korean nuclear forces as a network and ensuring that the United States has the appropriate tools to exploit weak points. One key shortcoming of the current U.S. posture is an overreliance on nuclear weapons to conduct strikes against North Korea’s nuclear forces.43 Massive nuclear strikes may not be credible in Pyongyang’s eyes, making it critical that the United States improve its conventional options, particularly against high-value targets like ICBMs. This might involve the deployment of additional strike platforms to the Korean peninsula or the fielding of intercontinental-range conventional strike capabilities.44

Robust damage-limitation capabilities will help the United States disabuse Kim Jong Un of the idea that he can use or threaten to use nuclear weapons to terminate a conventional conflict. Pyongyang knows it cannot match the full military potential of the United States. As a result, Kim has incentives to use nuclear weapons against U.S. forces and bases in the region, while relying on the threat of significant nuclear attacks against U.S. and allied cities to convince the United States to stop fighting.45

But if Kim and his advisers fear that the United States will execute strikes to destroy their nuclear forces – either to preempt its nuclear use during a conventional conflict or to retaliate against a limited nuclear strike –then they will have dramatically less confidence in their ability to coerce or intimidate through the threat or use of force. Recognizing this military disadvantage, Pyongyang will be less likely to go on the offensive, in peacetime or in crisis, or to attempt to end a conflict by conducting limited nuclear strikes.

Washington, on the other hand, would have greater confidence in its ability to deter – and if necessary mitigate – nuclear escalation, which should increase U.S. willingness to stand with allies in the face of aggression. For allies, U.S. damage-limitation capabilities would help to assure them of the credibility of U.S. extended deterrence despite advancing North Korean nuclear capabilities.46

Lastly, damage-limitation capabilities provide Washington with an option to reduce harm to the United States and its allies. A conflict on the Korean peninsula could spiral out of control despite U.S. efforts to de-escalate. Imagine North Korea launching several nuclear strikes and preparing more, regardless of the consequences. In this scenario, the United States and its allies may determine that deterring the next wave of nuclear attacks is not viable and instead seek to disarm North Korea’s nuclear forces. The right mix of offensive and defensive capabilities would save thousands if not millions of American, Korean, and Japanese lives.

### China

#### Chinese cyber hacking through OCOs enables successful military modernization to overtake the US

Johnson 19—Senior staff writer at FCW, covering governmentwide IT policy, cybersecurity and a range of other federal technology issues [Derek B. Johnson, 5/6/2019, “How China uses cyber theft and information warfare”, FCW, <https://fcw.com/articles/2019/05/06/china-information-warfare-dod-report.aspx>] AMarb

Beijing is leveraging increasingly sophisticated cyber operations and widespread theft of technological secrets in the digital domain as one of the key pillars of its military modernization strategy, a new Pentagon report finds.

Cyber and information operations are two areas that are seeing increased investment and emphasis from the Chinese military, according to the report. While traditional intelligence gathering remains an important goal, the use of cyber capabilities to conduct economic espionage has taken greater precedence in recent years.

This strategy not only helps to fuel the technological modernization of the People's Liberation Army (PLA) and other military and intelligence branches, but by targeting the U.S. defense industrial base, it simultaneously closes the gap in capability between China and its greatest military rival.

That reality has forced policymakers in Washington to respond by more aggressively prosecuting and confronting Chinese-directed extralegal activity targeting U.S. technology while giving greater scrutiny to more legal avenues, such as foreign direct investment and research partnerships between U.S. universities and Chinese entities.

While discussing the report, Assistant Secretary of Defense for Indo-Pacific Security Affairs Randall Schriver characterized the threat posed by China's cyber capabilities as "persistent."

"The Chinese remain very aggressive in their use of cyber," Schriver said. "What's changed is our level of awareness and the steps we're taking to reduce our own vulnerabilities and working with partners and allies to do the same."

The report argues that the Chinese government is slowly incentivizing its civilian sector to align its goals and activities with the defense market. The report maintains that the Made in China 2025 plan -- a list of technologies and industrial sectors that China aims to dominate by 2025 -- "directly support[s] military modernization goals by stressing proprietary mastery of advanced dual-use technologies."

U.S. officials also believe the plan is driving cyber and espionage-related theft of U.S. trade secrets. A Navy report earlier this year documented how Chinese hackers were stealing so much intellectual property and classified secrets that it was "materially eroding" U.S. economic and military advantage. Further, FBI officials have claimed that since 2015, the Department of Justice has charged Chinese individuals and entities for stealing trade secrets in eight out the 10 sectors listed in the Made in China 2025 plan.

"China uses a variety of methods to acquire foreign military and dual-use technologies, including targeted foreign direct investment, cyber theft, and exploitation of private Chinese nationals' access to these technologies, as well as harnessing its intelligence services, computer intrusions, and other illicit approaches," the report states.

The PLA also centralized its space, cyber, electronic and psychological warfare operations under a new organization -- the Strategic Support Force -- in 2016. The restructuring seeks to remedy operational coordination challenges that hindered information sharing under the pre-reform organizational structure, and the Pentagon believes it will help yield greater synergy among the different domains. It will also make it easier for the PLA to implement "information blockades" during or prior to a conflict, denying the enemy the information awareness needed to set the conditions for ground or air superiority later on.

Offensive cyber operations are viewed by Beijing as an "effective" means for countering a stronger foe. Chinese cyber operations target critical military and civilian nodes, such as command and control servers and logistics networks, to "deter or disrupt adversary intervention, and to retain the option to scale these attacks to achieve desired conditions with minimal strategic cost."

#### Chinese technological supremacy upends the balance of power ensuring nuclear Armageddon

Kroenig 18—Associate Professor of Government and Foreign Service at Georgetown University and Deputy Director for Strategy in the Scowcroft Center for Strategy and Security at the Atlantic Council [Matthew Kroenig and Bharath Gopalaswamy (Director of the South Asia Center at the Atlantic Council. He holds a PhD in mechanical engineering with a specialization in numerical acoustics from Trinity College, Dublin), 11/12/2018, “Will disruptive technology cause nuclear war?”, Bulletin of the Atomic Scientists, <https://thebulletin.org/2018/11/will-disruptive-technology-cause-nuclear-war/>] AMarb

Recently, analysts have argued that emerging technologies with military applications may undermine nuclear stability (see here, here, and here), but the logic of these arguments is debatable and overlooks a more straightforward reason why new technology might cause nuclear conflict: by upending the existing balance of power among nuclear-armed states. This latter concern is more probable and dangerous and demands an immediate policy response. For more than 70 years, the world has avoided major power conflict, and many attribute this era of peace to nuclear weapons. In situations of mutually assured destruction (MAD), neither side has an incentive to start a conflict because doing so will only result in its own annihilation. The key to this model of deterrence is the maintenance of secure second-strike capabilities—the ability to absorb an enemy nuclear attack and respond with a devastating counterattack. Recently analysts have begun to worry, however, that new strategic military technologies may make it possible for a state to conduct a successful first strike on an enemy. For example, Chinese colleagues have complained to me in Track II dialogues that the United States may decide to launch a sophisticated cyberattack against Chinese nuclear command and control, essentially turning off China’s nuclear forces. Then, Washington will follow up with a massive strike with conventional cruise and hypersonic missiles to destroy China’s nuclear weapons. Finally, if any Chinese forces happen to survive, the United States can simply mop up China’s ragged retaliatory strike with advanced missile defenses. China will be disarmed and US nuclear weapons will still be sitting on the shelf, untouched. If the United States, or any other state acquires such a first-strike capability, then the logic of MAD would be undermined. Washington may be tempted to launch a nuclear first strike. Or China may choose instead to use its nuclear weapons early in a conflict before they can be wiped out—the so-called “use ‘em or lose ‘em” problem. According to this logic, therefore, the appropriate policy response would be to ban outright or control any new weapon systems that might threaten second-strike capabilities. This way of thinking about new technology and stability, however, is open to question. Would any US president truly decide to launch a massive, bolt-out-of-the-blue nuclear attack because he or she thought s/he could get away with it? And why does it make sense for the country in the inferior position, in this case China, to intentionally start a nuclear war that it will almost certainly lose? More important, this conceptualization of how new technology affects stability is too narrow, focused exclusively on how new military technologies might be used against nuclear forces directly. Rather, we should think more broadly about how new technology might affect global politics, and, for this, it is helpful to turn to scholarly international relations theory. The dominant theory of the causes of war in the academy is the “bargaining model of war.” This theory identifies rapid shifts in the balance of power as a primary cause of conflict. International politics often presents states with conflicts that they can settle through peaceful bargaining, but when bargaining breaks down, war results. Shifts in the balance of power are problematic because they undermine effective bargaining. After all, why agree to a deal today if your bargaining position will be stronger tomorrow? And, a clear understanding of the military balance of power can contribute to peace. (Why start a war you are likely to lose?) But shifts in the balance of power muddy understandings of which states have the advantage. You may see where this is going. New technologies threaten to create potentially destabilizing shifts in the balance of power. For decades, stability in Europe and Asia has been supported by US military power. In recent years, however, the balance of power in Asia has begun to shift, as China has increased its military capabilities. Already, Beijing has become more assertive in the region, claiming contested territory in the South China Sea. And the results of Russia’s military modernization have been on full display in its ongoing intervention in Ukraine. Moreover, China may have the lead over the United States in emerging technologies that could be decisive for the future of military acquisitions and warfare, including 3D printing, hypersonic missiles, quantum computing, 5G wireless connectivity, and artificial intelligence (AI). And Russian President Vladimir Putin is building new unmanned vehicles while ominously declaring, “Whoever leads in AI will rule the world.” If China or Russia are able to incorporate new technologies into their militaries before the United States, then this could lead to the kind of rapid shift in the balance of power that often causes war. If Beijing believes emerging technologies provide it with a newfound, local military advantage over the United States, for example, it may be more willing than previously to initiate conflict over Taiwan. And if Putin thinks new tech has strengthened his hand, he may be more tempted to launch a Ukraine-style invasion of a NATO member. Either scenario could bring these nuclear powers into direct conflict with the United States, and once nuclear armed states are at war, there is an inherent risk of nuclear conflict through limited nuclear war strategies, nuclear brinkmanship, or simple accident or inadvertent escalation. This framing of the problem leads to a different set of policy implications. The concern is not simply technologies that threaten to undermine nuclear second-strike capabilities directly, but, rather, any technologies that can result in a meaningful shift in the broader balance of power. And the solution is not to preserve second-strike capabilities, but to preserve prevailing power balances more broadly. When it comes to new technology, this means that the United States should seek to maintain an innovation edge. Washington should also work with other states, including its nuclear-armed rivals, to develop a new set of arms control and nonproliferation agreements and export controls to deny these newer and potentially destabilizing technologies to potentially hostile states. These are no easy tasks, but the consequences of Washington losing the race for technological superiority to its autocratic challengers just might mean nuclear Armageddon.