# SDI Starter Packet --- Cyber Info Sharing Aff

## 1AC

### Contention 1: Resilience

#### Contention 1 is Resilience:

#### First --- NATO lacks sophisticated cyber threat information (CTI) sharing – this undermines cyber resilience

--- relies too much on technical data

--- excludes classified data

Daniel & Kenway 21 --- Michael Daniel President & CEO Cyber Threat Alliance & Joshua Kenway Cybersecurity Associate Cyber Threat Alliance, “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”, 12 Jan 2021, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE (CCDOE) https://kclpure.kcl.ac.uk/portal/en/publications/cyber-threats-and-nato-2030-horizon-scanning-and-analysis(3724c535-e782-45cf-9272-046670e7100f).html

Information sharing has become such an overused but under-performing concept that the term tends to provoke eye rolls within the cyber security community. Yet, most practitioners and policymakers agree that better information sharing would improve defences against rapidly evolving cyber threats. Virtually every relevant panel, study, or review over the last 20 years has recommended increased information sharing as a key step in improving cyber security. The logical question is why information sharing has not increased. Its lack remains a barrier to better cyber security, whether within NATO or the broader digital ecosystem.

This chapter will identify three faulty assumptions that have prevented cyber threat information sharing from living up to its promise that cyber threat information consists primarily of technical data, that every organisation should consume this technical data, and that information sharing is easy. It then establishes a framework for updating the current approach to information sharing by distinguishing the characteristics and value of different threat information types, using relevance and comparative advantage as the basis for producing and consuming threat intelligence, addressing key barriers to information sharing, and identifying trust as a necessary component of effective information sharing. Finally, the chapter explores the implications of these changed assumptions for more effective information sharing, including within NATO’s information sharing ecosystem.

A. Technical Level Cyber Threat Information Sharing in NATO NATO adopted technical cyber threat information sharing early on through an instance of the open-source Malware Information Sharing Platform (MISP) (NATO, 2013; MISP, 2020a), which the Alliance leverages to privately share information with member states, industry partners, and national Computer Emergency Response Teams (CERT) (Schrooyen, 2017). NATO uses MISP for the exchange of classified technical information with tactical and operational value and information sharing with participating partners is filtered according to its classification level (Schrooyen, 2017). Using MISP only for classified technical information sharing limits its value because it restricts the number of potential partners and excludes other valuable types of strategic and operational information. Over-classification impedes information sharing, something which NATO has acknowledged (NATO, 2012).

NATO also maintains a best practice and threat information sharing relationship with EU-CERT (NATO, 2016) and is building an Industry Cyber Partnership (NICP) (NATO, 2020). These two programmes provide NATO with the foundation needed to meet the challenges of information sharing explored in this chapter. Key industry partners include Oracle (NATO, 2019a), RSA Security (NATO, 2017), FireEye (Fireye, 2016), Cisco (NATO, 2016), CY4GATE, Thales, Vodafone (NATO, 2018), BT, Minded Security, Lockheed-Martin, Fortinet, and Symantec (Schrooyen, 2017). The NICP has broad goals, including improvements to the sharing of best practices, expertise, experience, and information ‘including […] on threats and vulnerabilities’ (NATO, 2020).

In parallel, the Alliance’s efforts to operationalise a Cyber Security Collaboration Hub by 2023 (NATO, 2019b), which will allow member states ‘to quickly and securely share information with each other, and with the [Alliance]’ (NATO, 2019c), could address some of the challenges raised in this chapter. However, this chapter argues that NATO should shift its approach to information sharing to assume a leadership position in this area.

2. FAULTY ASSUMPTIONS: OVERPROMISING AND UNDERACHIEVING

Underlying the slow progress on information sharing are three faulty underlying assumptions: (1) cyber threat information consists primarily of technical data; (2) every organisation should be producing and consuming technical cyber information; and (3) sharing cyber threat information is easy.1 These fallacies are implicit, rather than explicit, and so have largely avoided critical review or academic assessment. Further, they have resulted in counter-productive policy, misaligned incentives, and ineffective cyber security. To address these shortcomings, different foundational assumptions are needed. In turn, using better assumptions can make information sharing a more effective tool against cyber threats.

A. Cyber Threat Information Consists Primarily of Technical Data

Within the cyber security community, the term ‘information sharing’ primarily refers to the exchange of technical data that identifies malicious activity such as malware and malicious domain names. While several scholars (Friedman et al., 2015; Chismon & Ruks, 2015) acknowledge that such exchanges should also include other types of information, the emphasis is on technical data in practice. For example, the main use cases or core functionalities associated, respectively, with the two commonly used cyber information sharing standards, Structured Threat Intelligence eXchange (STIX) and the Malware Information Sharing Platform (MISP), focus on technical information (MITRE, 2012; MISP, 2020b). Cyber threat information sharing ‘primarily focus[es] on sharing of indicators of compromise’ (Sauerwein et al., 2017: p. 838), leading to a situation in which the activities of almost every established sharing platform are ‘comparable to data warehousing’ (ibid: p. 849). Many US government programmes and existing statutes either explicitly or implicitly focus on this type of information sharing; meanwhile, companies are investing billions of dollars in an effort to consume and analyse technical cyber threat information (Verified Market Research, 2020).2

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. 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).

3. REBUILDING INFORMATION SHARING: NEW IMPERATIVES

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.

#### Second --- Cyber attacks are inevitable --- lack of resilience ensures they are successful --- killing millions and collapsing society --- increased situational awareness is key to mitigate harms

Conklin et al 17 --- William Arthur Conklin, Associate Professor and Director of the Center for Information Security Research and Education in the College of Technology at the University of Houston, & Dan Shoemaker, Professor and Director of the Masters of Science in Cyber Security Program at the Center for Cyber Security and Intelligence Studies, a NSA Center of Academic Excellence, at the University of Detroit (313) Mercy, & Anne Kohnke, College of Management, Lawrence Technological University, “Cyber Resilience: Rethinking Cybersecurity Strategy to Build a Cyber Resilient Architecture”, International Conference on Cyber Warfare and Security, 2017, https://www.proquest.com/docview/1897660614/fulltextPDF/FE6EBF8A132A40C1PQ/1?accountid=12598

Von Clausewitz might have lived through the Napoleonic wars, but he could just as well have been writing about the present state of affairs in cyberspace. The fact is that the multitude of threats that populate the virtual eco-system is so all-embracing that it is impossible to defend against every form of attack (Symantec, 2015). The unfortunate reality is that every system can eventually be compromised and no computer is safe. Furthermore, America's electronic infrastructure is so riddled with vulnerabilities and there are so many adversaries out there, that "cybersecurity" is a relative term indeed (Brasso, 2016).

Adversaries in cyberspace range from state-sponsored hackers to the professional perpetrators of cybercrime, to any person with a grudge and an internet link. Moreover, because of the proliferation of adversaries and the inescapable vulnerability of the U.S. critical infrastructure, cyberattacks on its various elements are a daily fact of life. For instance, the Industrial Control Systems-Computer Emergency Response Team (ICS-CERT) reports that the U.S. industrial control systems were attacked at least 245 times over a 12-month period (OAS, 2015). In other parts of the world, a 2015 attack on Ukraine's power grid left 700,000 people without electricity for several hours [Brasso, 2016). And the perpetrators of the Ukrainian attack were observed conducting similar attacks against the U.S. energy sector (Brasso, 2016). Though there was never any actual disruption, many experts believe that those exploits were a reconnaissance for future moves on the U.S. infrastructure (Brasso, 2016). So they are still out there.

The reason why this topic is so worrisome is that a successful digital Pearl Harbor type cyberattack on the electrical infrastructure would leave the U.S. cloaked in darkness, with its people unable to communicate with each other and without any form of twenty-first century transport. It would likely kill many thousands of citizens, perhaps millions, either through civil unrest, failure of public systems, or mass starvation (Brasso, 2016). This could be the foreseeable situation if hackers successfully shut down the U.S. power grid. Consequently, in the larger sense, the key question is, "Could a catastrophic cyberattack in the U.S. infrastructure ever occur? The National Security Agency's former Director, Mike Rodgers, made his own evaluation of the possibility of a successful attack against critical infrastructure when he said; "It's a matter of, when, not if" (Smith, 2014).

To illustrate the reason why something as unthinkable as a digital Pearl Harbor could happen, the non-profit Privacy Rights Clearinghouse reports that we have lost over one BILLION records over the past decade and these are just the losses that were REPORTED. Since most companies do not like to publicize their security failures that number could be, and probably is, much higher. The running average of 100 million records lost per year has been subject to some variation overtime and the source of breaches has changed in common-sense ways as the technology has evolved. Nonetheless, the number of reported incidents rose annually from 108 in 2005, to 607 in 2013 (PRC, 2015). The important point to note is that while losses have increased at a rate of fifty-percent per year over the same period corporate budgets for security have increased at the rate of fifty-one percent (Symantec, 2014).

Consequently, it is probably safe to say that cyberattacks are going to happen, no matter how much money we throw at the problem. At the same time, notwithstanding the clear recognition of the disastrous nature of a successful cyberattack, none of the industries in our current national infrastructure have developed an effective standard strategy to protect themselves (Brasso, 2016). This includes the Chemical Sector; Commercial Facilities: Communications; Dams; the Defense Industrial Base; Emergency Services; Energy: Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation; and Water and Wastewater Systems (PPD-21, 2013, p.2).

So, what we are suggesting here is that the paradigm we adopted long before the internet needs to be seriously rethought. Right now, we secure systems at the logical points of access. Even defense-in-depth, which is the modern doctrine for doing that, simply involves several increasingly rigorous perimeters. Instead of throwing our resources into defending the system at all points of attack, perhaps we should devise ways to ensure that the system assets that we cannot afford to lose are unconditionally protected. In concept, this strategy would narrow the attack surface to the point where absolute assurance within available resources could be guaranteed, while reducing the impact and recovery time of non-essential assets. This selective versus universal approach to security is what sums up the difference between a cyberresilient strategy, and one that is based on cybersecurity.

2. Cyber resilience versus cybersecurity

It is important to make a distinction between present ideas about cybersecurity and the approach we are suggesting. Cyber resilience is a much narrower strategic vision than the more diffuse activities that fall under the generic heading of "cybersecurity." At its heart, cybersecurity ensures against unknown, or unwanted penetrations of protected space. In that respect, a cybersecurity solution deploys a comprehensive set of defenses to ensure against unauthorized access to protected objects, either from external or internal sources. To accomplish its mission, cybersecurity deploys a targeted set of protection measures at all viable points of entry, along with the appropriate detection mechanisms to respond to known forms of unauthorized access. Whereas, cyber resilience attempts to create a security architecture that will ensure the continuous effective functioning of just the organization's core functionality.

Thus, cybersecurity focuses on access control, while cyber-resilience focuses on identifying and securing just those assets that the organization can't live without. In many respects, the cyber-resilience concept is comparable to locking up just those critical resources that an organization needs to survive. Those critical resources are then put into a safe within the building. This is in direct contrast with a strategy that attempts to protect every asset of value within the entire building. It should be evident that these are two entirely different approaches, especially from a resource utilization standpoint.

Ideally these two approaches work in tandem to create a secure organization. Both are important and neither works as effectively as it should if the other is missing. Cyber resilience is an emerging concept and there are already several institutionally sponsored approaches to creating a cyber resilient organization. These methods develop comprehensive enterprise architectures with the aim of building in greater resiliency. The methodology centers on and is driven by assessment and metrics. The assessment characterizes and then seeks to improve the resiliency of the enterprise's existing architecture. The goal is to understand the organization's practical ability of uninterrupted functionality, as well as the ability to recover within an acceptable period. The metrics of this entire process are meant to ensure continuous improvement. The approach itself, is deliberate and incremental and is a broad-scale strategic development process in the sense that the requisite capabilities are phased into existing enterprise processes in a planned and rational fashion.

3. Creating a cyber resilient architecture

Cyber resilience is not just a matter of building higher and thicker walls. Cyber resilience involves the creation of a set of well-defined processes, which are designed to react to successful penetrations of the organizational perimeter, affecting secure space. Cyber resilient processes prevent the attacker from ever reaching and harming the organization's most critical assets and they do not fortify every access point beyond basic access control countermeasures.

Cyber resilience is founded on classification, prioritization, and comprehensive strategic policy-based deployment of a rigorous set of real-world security controls. The security controls strictly ensure the achievement of just the organizational purpose. Therefore, less resources are required. These controls are both electronic and behavioral and they are designed to protect key assets, as well as ensure optimum recovery of the overall system in the event of successful attack. Figure 1 below shows the cyber resiliency process. The process is embodied in seven generic principles and are as follows:

1. Classify: You can't protect things that you don't know exist. Therefore, all the organization's assets must be identified, labeled, and arrayed in a coherent baseline of "things." This baseline describes all potential protection targets and it is maintained under strict configuration management. This is comparable to the "Classification" phase of the NIST Risk Management Framework (NIST, 2014).

2. Risk: Resiliency requires appropriate situational awareness. Therefore, a broad-spectrum risk assessment must be performed that characterizes all known threat scenarios as they apply to the identified asset base. This is a risk assessment process comparable to the "Security Assessment" phase of NIST SP 800-53a (NIST SP 800-53A Rev.4, 2014).

3. Rank - the assets that the organization absolutely can't afford to lose are selected, evaluated and a provably effective countermeasure response is deployed for each of the chosen assets. Organizational resources are focused on only assuring those critical things. The resources that are left over are then allocated to ensuring the protection and recovery of the rest of the organization's functionality. This is comparable to the "Select" phase of the NIST Risk Management Framework (NIST, 2014).

4. Design/Deplov: Resilience must be baked-into the architecture so that critical functions are assured given a generally successful attack. This is a design/control deployment exercise comparable to the "Implement" phase of the NIST Risk Management Framework (NIST, 2014).

5. Test: Architectural resilience needs to be assured. This is a planning and oversight function that characterizes critical control performance against stated mission goals. Methods like penetration testing apply here. This is an assessment process comparable to the "Assess" phase of the NIST Risk Management Framework (NIST, 2014).

6. Recover: Well-defined processes need to be documented and established to ensure that all enterprise functions are fully restored within requisite parameters. This is comparable to the "Plan-Purpose-Scope-Relationship" recommendations embodied in NIST SP 800-34 Rev. 1 (NIST, 2010).

7. Evolve: the organization dynamically adjusts its cyber-resilient architecture based on lessons learned. This is comparable to the implementation of the NIST Cyber Security Framework process (NIST-CSF, 2014).

4. Principle 1: Classify

In some respects, cyber resilience is nothing more than an ultimate defense-in-depth and continuity management solution rolled into a highly-limited protection mission. The core aim of cyber-resilience is to maintain critical business functionality at all costs. Thus, the decisions that come out of the cyber-resilience design process will determine how the business will invest its precious time and resources and build its architecture. The key to cyber resilience is understanding what constitutes core functionality. Cyber resilience assumes that all systems will eventually be compromised. Given this assumption, the cyber resilience function ensures a robust array of specifically targeted controls to ensure that only the subset of functions essential to the continuing operation of the business are completely protected, even if all other system activities are compromised. In conjunction with the goal of ensuring the survival of core functionality, the cyber resilience process also defines clear, straightforward and practical paths to restore any lower priority functions that might have been lost in the actual compromise. The seven stages of cyber resilience are designed to achieve those two specific goals.

All computerized systems are complex and highly interdependent so, the essence of success lies in the identification of just those fundamental processes and relationships that deliver a given desired outcome. The identification process is perhaps the most important step in creating a cyber-resilient organization because the outcome of the classification process will drive every subsequent protection action. In practical terms, if an organization does not understand what assets they have, it is almost impossible to intelligently protect them. Only eighteen percent of organizations reported being effective in classifying mission critical information assets (EY, 2014). The majority of surveyed organizations reported that they were minimally effective or did not know how effective they were (EY, 2014). Thus, a deliberate, formally executed and documented classification activity is the key starting point. This is an organization-wide exercise whose aim is to understand the criticality, sensitivity, and priority of all items in the asset base. It involves all stakeholders because buy-in is an essential condition for embedding changes in the organization.

5. Principle 2: Risk

Risk assessment provides timely and accurate understanding of the threat status of all components of the asset base and is essentially a situational awareness function. The Risk stage employs situational awareness practices to drive the decisions about the best way to ensure critical assets and services will continue to function as desired. The aim is to fully understand every conceivable hazard in the threat environment that might affect a critical asset. The term "hazard" denotes a threat or an incident, natural or manmade, that warrants action to protect against harm and to minimize disruptions of the mission. This includes natural disasters, cyber incidents, acts of terrorism, sabotage, and destructive criminal activity targeting critical components of the enterprise infrastructure (PDD-21, 2014).

The outcome of this phase is a detailed map of the threat environment sufficient to support decision making with respect to organizational priorities. No decisions are made until the entire threat assessment is mapped. There is obviously a potential that meaningful threats might be missed, or that a new threat might appear after the original risk assessment is completed. Therefore, there also should be a comprehensive plan to ensure subsequent systematic risk assessments against any potential attack that might occur against assets viewed as critical. Since the architecture will be altered to respond to those threats it is also crucial that a process exists to rapidly respond to those risks. The outcome is reasonable confidence that all conceivable risks to a given asset and its dependencies have been identified, characterized and ranked for likelihood and impact.

6. Principle 3: Rank

This is the second most important aspect of the cyber-resilience process. Once the organization's assets have been identified and baselined and the threat environment characterized, the criticality of all assets in the asset baseline is ranked. This is an organization-wide ranking process involving all stakeholders. "Assets" comprise all of the people, processes, technologies, and facilities required to achieve the organizational purpose. However, some assets are more critical than others. The ranking process identifies, documents, and assures only those assets ranked as "critical" to the organization's mission, vision, values and purposes (PDD-21, 2014).

Unfortunately, ranking can often turn into a political free-for-all where various stakeholders attempt to enforce their own agendas. Obviously, this can't be allowed to happen, if the eventual architectural solution is going to be truly resilient. Therefore, criticality must be understood based on a clear map of functions and dependencies, which are referenced in an objective and rational way to the mission and goals of the organization. Therefore, an asset can only be labeled "critical" if it provably underwrites some aspect of the organization's core functionality.

A rigorous set of protection requirements are specified for just those assets that directly enable the organizational mission. Rigor is defined as the ability to resist any known or conceivable method of attack (PDD-21, 2014). Relevant stakeholders are assigned to supervise and maintain each asset. Effective communications linkages are established between those stakeholders and documented. Then the protection requirements, access links, and the requisite permissions are enabled as a coherent set of electronic and behavioral controls.

7. Principle 4: Design/deploy

Design deploys the controls required to ensure a critical asset. This is a strategic governance process. Design creates an infrastructure of substantive controls to effectively satisfy its stated mission, goals and objectives. Thus, this phase identifies the explicit control objectives for each critical asset. It prioritizes those objectives and implements targeted control actions to most effectively achieve priority objectives. Then it analyzes and assesses the deployed control set to ensure that the resultant infrastructure satisfies the critical purpose. If documented control objectives are not satisfied, then the Design process undertakes the necessary analysis to modify controls, or plug gaps.

8. Principle 6: Recover

Organizations need to understand how resilient its critical services are. This is essentially the continuity management principle. The goal of recovery planning is to ease the impact of disruptive events by using well-established plans to ensure predictable and consistent continuity of the critical services (PDD-21, 2014). To do this, the critical service's operating environment is studied to identify all potential failure modes and then a proper strategy to recover from all possible breakdowns, or disruptions is devised.

The goal is to create a complete and consistent recovery process that will address all conceivable types of system compromise. The plan for incident recovery must be explicit for every asset and lessons learned are compiled to develop improvement strategies. This requires an operational plan capable of identifying, analyzing, responding to, escalating and learning from all adverse incidents. A well-defined process for assigning roles and responsibilities and managing and tracking resolutions.

9. Principle 7: Evolve

The Evolve stage serves as the formal basis for identifying and deploying process and technology responses and improvements across the organization. This evolution is required to meet the organization's cyber resilience goals as the threat picture changes. In this stage, measurable improvements that could increase the resilience of critical assets are identified, analyzed, and systematically deployed. The effects of currently deployed processes and technology improvements are measured and the effectiveness of the selected process improvement is characterized. The five functions that must be executed mirror those of the NIST Cyber Security Framework (NIST-CSF, 2014).

Evolution is driven by the collection and analysis of data from lessons learned about the operation of the day-to-day execution of the resilience process. Improvement recommendations are supported by data obtained from the deployment of prior process and technology controls. Nevertheless, because this is essentially a "maintenance," activity this type of analysis involves ongoing testing and risk estimation. Lessons-learned typically involve objectively evaluating the performance of deployed processes against plans, objectives, standards, and procedures; as well as the outcomes of organizational innovation and deployment process.

10. Conclusion

We understand that systems will never be 100% secure and there are simply too many threats to ever make that declaration. Organizations are far more exposed to a wider range of unknown, or even unknowable, attacks (EY, 2014). Given the existence of a myriad of unknowable elements in the cyber-threat environment, organizations must be able to detect and respond creatively to threats to their basic operation. The response encompasses all forms of attack; electronic, behavioral, and physical. Thus, the concept of cyber-resilience goes far beyond the classic boundaries of better hardware and software access controls (EY, 2014). Instead, organizations need to establish a "cyber resilience strategy" that gives them ability to withstand and recover rapidly from disruptive events (EY, 2014).

Practically speaking, organizations have to start rethinking strategically and given the large number of threats and the limited resources available to counter them, concentrate their resources where they will make the most difference. This means that businesses should stop viewing security as an access control and incident response problem. Instead they should approach the problem as a comprehensive, fully integrated, strategic management commitment; aimed at ensuring survival and easing recovery. This goal requires that a robust set of concrete controls are embedded in the enterprise architecture. The umbrella term for this approach is, "cyber resilience"

Cyber resilience recognizes that adversaries will succeed. There are too many advanced hacking tools to prevent sophisticated attackers from finding the cracks in even the most robust cyber-security system (Lois, 2015).

Accordingly, cyber resilience must be an organizational condition rather than a deployed set of explicit countermeasures. Cyber resilience should be integrated into the "bones" of the organization and requires the organization to spend whatever it takes to develop a well-defined, explicit architecture of controls to ensure cyber resiliency. The controls must assure provable protection of core functionality and its various interdependencies to include every form of electronic, human and physical threat inside and outside the enterprise's eco-system (EY, 2014).

Cyber resilience is not a traditional defensive stance focused on detecting network intrusions or fixing malware. Instead, the resilience concept emphasizes practical survival and recovery of the system in the face of all conceivable forms of attack. Effective implementation of a cyber-resilient enterprise architecture requires strategic vision. It also requires day-to-day engagement across the enterprise to assure and optimize that vision. Unfortunately, this perspective is new, and it will require a change in culture to accomplish.

In general, our belief is that the only way organizations are going to effectively prevent the inevitable digital Pearl Harbor is to amalgamate cyber security and cyber resilience concepts into a single strategy. The increased presence of advanced cyber threats makes it inevitable that all targeted organizations will ultimately be compromised (Trend Micro, 2015). Nevertheless, at its fundamental root the organization needs to survive and every organization's critical systems must be assured safe, assuming any realistic set of conditions. Lost data or ancillary functionality can be restored after the attack, but the key functions of the organization must be protected. Cyber resilient organizations can "tough-out" cyber-attacks and continue to accomplish the fundamental mission. Therefore, it is incumbent on decision makers to redesign or update their essential systems for resilience. This condition should make attacks less likely to succeed, minimize the consequences when they do succeed, increase the work-factor cost and uncertainty for the adversary, and possibly act as a deterrent against future attacks. Consequently, investment in building cyber resilience is strategic investment in organizational survival.

#### Scenario 1 – Smart Grids --- they’re uniquely vulnerable to cyber-attacks in ways neg defense doesn’t assume --- resilience through information sharing is critical to counter threats

Ghiasi et al 20 --- Mohammad Ghiasi et al, a Research Assistant at the Shiraz University of Technology, M.S.in electrical power engineering, “Investigating Overall Structure of Cyber-Attacks on Smart-Grid Control Systems to Improve Cyber Resilience in Power System”, IEEE Smart Grid Newsletter, March 2020, https://www.researchgate.net/profile/Mohammad-Ghiasi-2/publication/339912094\_Investigating\_Overall\_Structure\_of\_Cyber-Attacks\_on\_Smart-Grid\_Control\_Systems\_to\_Improve\_Cyber\_Resilience\_in\_Power\_System/links/5e6b9024a6fdccf321d99889/Investigating-Overall-Structure-of-Cyber-Attacks-on-Smart-Grid-Control-Systems-to-Improve-Cyber-Resilience-in-Power-System.pdf

The use of information and communication technologies and computer-based software to enhance the quality, efficiency, and reliability of smart grids (SGs) have brought unwanted threats in these systems; one of the most important of such threats is cyber-attack. Understanding the ways to detect and deal with cyber threats in SGs will increase the resilience of power systems. In this paper, conceptual models of SG vulnerabilities are presented to address the issue of the vulnerability of SG control systems against cyber-attacks. Different scenarios of cyber-attacks are then dealt with in SG control systems to enhance their resilience.

1. INTRODUCTION

The main security issues of SG control systems against cyberattacks are given in Figure 1. These issues are divided into four categories:

 Identifying different vulnerabilities and scenarios for attacking SG control systems and trying to prevent it

 Providing strategies to detect and identify the attack

 Recombining and using control tools to reduce the effects of the attack and increase the system's selfhealing properties

 Improving cyber security management in SG control systems

2. CONCEPTUAL MODEL OF CONTROL SYSTEMS VULNERABILITIES IN SMART GRID

Controlling of SG in energy systems has the task of directing and controlling physical processes. They usually consist of a set of multiple components including sensors, operators, data processing units such as programmable logic controllers (PLCs), communication networks, and central computers. There are several general models for elucidating the structure of smart control systems [1, 2]. A conceptual model of SG control system vulnerabilities is presented in Figure 2. As can be seen from the Figure 2, the vulnerabilities of the SG control system are divided into six categories:

1- Field equipment vulnerabilities

2- Field equipment communication network vulnerabilities

3- Local controller vulnerabilities such as remote terminal units (RTUs) and PLCs

4- Vulnerabilities of control network communication protocols

5- Local area network (LAN) control vulnerabilities

6- Vulnerabilities of cooperative and financial-commercial networks

The layered structure of this conceptual model emphasizes that the types of vulnerabilities of each layer of SG control system are different, and therefore each layer requires different security measures.

3. IDENTIFY DIFFERENT VULNERABILITIES AND SCENARIOS OF CYBER-ATTACK IN SMART GRID CONTROL SYSTEMS

With the advancement of control and protection systems in SGs as well as their use of the same software, hardware and network platforms and having the same standards, it is possible for unauthorized persons to access the internal layers of these systems. In general, an attacker who intends to attack a cyber-attack and damage an intelligent control system faces two major challenges:

 Identifying, penetrating and accessing the system

 Taking full or partial control of the process and damage it

So the first step in securing smart grid control systems is to identify vulnerabilities and access points. It can be divided into two major areas of communication equipment and protocols. The devices used in smart grid control systems also fall into two categories:

1- Equipment used solely for control systems, such as sensors, actuators, RTUs, and PLCs

2- IT equipment used in other systems and networks such as switches and computers

In this section, we first discuss a number of articles addressing the vulnerabilities of communication protocols of the SG control system and their solutions. Then, considering the extent of equipment vulnerabilities and articles in this field, first class equipment vulnerabilities are discussed. Finally, four categories of scenarios for attack on control systems in SGs are investigated.

3-1- Communication vulnerabilities and attempts to prevent intrusive influence

Nowadays, many protocols are used in intelligent control systems. Most of these protocols are designed to increase efficiency, reliability in real-time operations, and support for economic and operational requirements. Unfortunately, most of these protocols have ignored any unnecessary security features such as authentication and cryptography to enhance performance. Many have been developed by others to use the Ethernet protocol and connect to the Internet. Therefore, the communication protocols of industrial control systems are very vulnerable and exposed many attacks [3]. According to the American Gas Association reports, there are about 150 to 200 supervisory control and data acquisition (SCADA) protocols. The integration of these protocols in recent years has resulted in the attackers obtaining very accurate information on their function and structure. In this way, attackers can identify and modify data packets by identifying vulnerabilities in these protocols [4]; like the attack on Queensland's Australian Water and Wastewater Control System in 2000 when an attacker was able to infiltrate the field's communications network and bring 800,000 liters of sewage into the city's safe water cycle by having complete information about the attacking protocol. The vulnerabilities of these protocols have been investigated in several sources. References [3, 5] discuss a variety of industrial protocols, their vulnerabilities and security solutions. One of the issues discussed in this source is the Modbus protocol that lacks authentication, encryption, and encryption integrity.

One of the most useful and also dangerous features of Modbus is its ability to program controllers that many SG protocols share with Modbus. Due to this dangerous feature, attacker can use it to inject malware into PLCs and RTUs. One of the methods of intrusion detection in Modbus protocols is the use of model-based intrusion detection systems. Reference [6] introduces three model-based methods for monitoring and detecting Modbus TCP protocol attack. These methods provide a protection mechanism with respect to the topology and communication structure of the SCADA network. In order to prevent unauthorized access to the protected system, firewalls have been suggested as a security solution in many sources. One of its tasks is to block messages that are not structured in accordance with the protected area communication protocol [7].

Another common way to increase the security of communication protocols is to use cryptography. There are various traditional methods of encryption, but most are not usable in smart grid control systems. The reason is the limited computing power and low data transmission speed of these components, which must also meet the real-time performance requirements. These limitations make it difficult to implement sophisticated encryption. Reference [8] has explored various encryption methods to ensure data confidentiality and integrity.

3-2- Control equipment vulnerabilities

Many cyberattacks on industrial control systems have been exploited to exploit vulnerabilities in control equipment, one of which is the Stuxnet attack. Therefore, identification of these vulnerabilities is one of the issues of interest to researchers in this field [9]. In recent years, in addition to software vulnerabilities, various types of hardware have also been heavily favored by security experts. These are widespread in processors and electronic components and are found even on telecommunication surfaces [10].

3-3- Investigation and identification of different scenarios of attacks on SG control systems

Overall, there are five types of scenarios for attack on control systems of SGs:

3-3-1- Static false data injection attack

In static false data injection attack, the attacker changes the sensor output to such a way that the control system does not cheat and fails to send the wrong data to the controller. This scenario was first put forward in 2009 for an attack on the power system and its faulty detection system, assuming the attacker had full knowledge of the system [11]. In the references [12, 13], authors have proved that an attacker can even launch a successful attack even with partial awareness. In an effort to counteract this attack, the source proposes two security measures for the power grid state estimator, which is actually a measure of the minimum amount of attacker effort required to successfully execute an attack. These scales depend on the physical topology of the power grid and the degree of availability of the sensor outputs. Reference [14] stated that complete encryption and out-of-the-box protection of all equipment is not cost-effective and enforceable, and that the success of the injection attack can be prevented by protecting a limited number of measurements and their output. The number of these measurements is equal to the number of system state variables. In reference [15], two algorithms offer protection for a limited number of devices in such a way as to provide maximum security against injection attacks. Reference [16] first described an optimal attack strategy that can cause maximum damage to the system, and then by formulating the defense problem, it has been able to develop an optimal defense strategy and minimize the amount of damage. The economic effects of the data injection attack on the electricity grid market performance were formulated in paper [17].

3-3-2- Attack on power grid state estimator and wrong data injection

The purpose of the power grid state estimator is to estimate the state variables of that system based on the measured data. In reference [18], the control center of the state system matrix of the variables was described. Inappropriate estimates can be due to various reasons, such as measurement failures or malicious attacks. In this scenario, it is assumed that the attacker knows the state matrix variables of the target power system and makes subversive measurements with knowledge of this matrix. It then injects these erroneous measurements into the control system to disrupt the state estimation process. Figure 3 provides a schematic overview of the data injection attack on power grid control system.

3-3-3- Invalid dynamic data injection attack

The attack attempts to inject the wrong data dynamically and create an unstable and invisible fashion in the system. Reference [19] assumed that the attacker's purpose is to inject the wrong data, destabilize the system, and remain secret. The author used the Kalman filter and the linear–quadratic– Gaussian (LQG) controller to monitor and control the discontinuous linear system over time, as well as to detect the attack of a false dynamic data injection. Finally, this article described the requirements for a successful attack and proposes a method to counter attack based on the use of plugin sensors.

3-3-4- Information recovery attack

One of the most dangerous attacks is the information recovery attack. As observed in the "data injection" attacks, if the attacker can access the sensor or operator output data, he can enter the wrong data in an intelligent and purposeful manner, or accidentally, and control Error making the receiver [20]. In an information recovery attack, the attacker records the sensor or operator information under normal system conditions and sends it to the control network at the time of the attack and sabotage [21]. As such, the control system is cleverly deceived and, in addition to the loop control, the system goes into danger. One way to counter this attack is to add a Gaussian random input with a mean of zero to the system input [22]. Random input is an authentication signal and it is attempted to be optimally designed to minimize impact on system performance.

3-3-5- Stealth attack

The attack is actually a closed-loop information reconstruction attack. In other words, the attack output is reconstructed as a closed loop to eliminate the effect on the sensor output and keep the attack hidden. In these kinds of attacks, attacker should have a thorough understanding of the physical model of the system under control in order to simulate a model similar to it. As shown in Figure 4, the attacker puts the simulated model and its controller between the system and the master controller; and by sending arbitrary signals to the main controller input, it hides the attack and replaces the arbitrary work point.

4. IMPROVING CYBER SECURITY MANAGEMENT IN SG CONTROL SYSTEMS TO ENHANCE RESILIENCE OF POWER CONTROL SYSTEMS

In order to achieve optimal security, in addition to using appropriate security strategies there must be good security management. Appropriate security management tools include security policies, strategies, and programs that are based on accurate threat and risk analysis. In other words, given the wide range of cyber threats that industrial control systems are exposed to, it is essential to identify and analyze these threats to provide an optimal and cost-effective safeguard strategy. In general, the field of study of the articles in this section can be categorized as follows:

1- Providing methods for identifying cyber threats and assessing their risks in industrial control systems

2- Considering such analysis and evaluations to extract and select the optimal and cost-effective defense strategy and formulate a security plan Much effort has been made to provide methods for identifying threats and risks as well as analyzing them in industrial control systems. In reference [23], it is attempted to estimate the security threats of cyber-physical systems using the game theory method.

5. CONCLUSION

In addition to exploiting unknown vulnerabilities, cyber attackers are developing more sophisticated methods to attack smart grid control systems. Thus, after going through IT-based security strategies, they are virtually confronted with a control system without security protections. On the other hand, the ultimate goal of attackers is to damage and disrupt the optimal functioning of the physical system under control, which is ignored in IT-based security strategies. It can only be stated that IT-based security strategies alone cannot provide a depth defense strategy (the in-depth defense strategy allows the attacker to pass through each layer again to a security layer that eliminates Designed to reduce the attack (or reduce its impact) to control systems. Therefore, this article identified various vulnerabilities and scenarios of cyber-attack in smart grid control systems so as to increase system resilience of power system and to reduce the effects of such attacks.

#### Smart grids are particularly vulnerable to FDI attacks --- detection is key

Khazaei & Amini 21 --- Javad Khazaei, assistant professor in the electrical and computer engineering department at Lehigh University, and M. Hadi Amini, ssistant Professor at the Knight Foundation School of Computing and Information Sciences at Florida International University, “Protection of large-scale smart grids against false data injection cyberattacks leading to blackouts”, International Journal of Critical Infrastructure Protection Volume 35, December 2021, https://www.sciencedirect.com/science/article/pii/S1874548221000482?casa\_token=CJmndO91NGAAAAAA:hzNjEiWdnv10bAu7JnYgtcX86s\_r21wmcKPMTE\_mZNQK-8PEWxoJFMjNkexx3DXP-E5oTHW9

Power systems are the most important cyber–physical systems that guarantee reliability of other critical infrastructures including water networks, transportation, or health systems [1]. While the application of advanced monitoring system and supervisory control and data acquisition (SCADA) systems enhanced the monitoring, protection, and security of smart grids, they have made the energy system vulnerable to cyber threats, which can jeopardize the security of power systems [2], [3].

A cyberattacker can therefore inject computer viruses or anomalies to endanger the security and resilience of the smart grid system [4], [5], [6]. Examples of such attacks include software bugs on Israel’s utility grid in 2016 [7], or Russian’s cyberattack on obtaining detailed data on nuclear power plants and water facilities in the U.S. in 2018 [8]. Another real-world example is the successful cyberattack by Russian hackers in December 2015 on the Ukraine power grid. In this cyberattack, 30 substations were switched off by hackers which resulted in a power outage of 1–6 h for almost 230,000 people [9].

Transmission lines are the most important assets in power delivery in smart grids, and if failed, can cause serious cascading problems leading to blackouts. One example of such cascading failure was a blackout in Italy that happened in 2004 [10]. Cyberattacks on transmission lines are normally designed to overflow a line or series of lines with the aim of cascading failures. Such transmission line congestion can be achieved if an attacker injects any false data on measurements without being detected by bad data detection algorithms during the state-estimation process. Recent studies show that these FDIs can be deliberately designed in order to bypass state-estimation methods without being detected [11], [12], [13], [14], [15], [16]. Therefore, targeted cyberattacks on multiple transmission lines can potentially cause cascading failures resulting in blackouts.

#### FDI attacks on smart grids cause generator damage --- guarantees PROLONGED blackouts

Yan et al 21 --- Weili Yan et al, Research Scientist at Advanced Digital Sciences Center, established by the University of Illinois at Urbana Champaign (UIUC) in Singapore, “A Stealthier False Data Injection Attack against the Power Grid”, 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, IEEE 2021, https://ieeexplore.ieee.org/abstract/document/9632337

False data injection (FDI) is a broad class of cyberattacks that target the digital communications and control of a cyberphysical system (CPS). Well-known real-world incidents such as Stuxnet [1] and Dragonfly [2], [3] demonstrate the effectiveness of FDI attacks. For example, a malware-infected PLC in the power grid may send falsified sensor measurements that bypass standard methods of bad data detection (BDD) [4], thus compromising the grid’s state estimation. FDI attacks against the grid’s automatic generation control (AGC) [5] are especially dangerous. AGC adapts generators’ output to dynamic system conditions in real time [6], to regulate the grid’s frequency within a safe range. Breach of this range constitutes a frequency excursion that may damage generators if they are not quickly disconnected from the grid; both disconnection and damage can cause widespread and prolonged blackouts.

#### Extinction

Monarch 20 --- Benjamin Monarch, University of Kentucky College of Law, J.D. May 2015, LLM in Energy, Natural Resources, and Environmental Law and Policy from the University of Denver Sturm College of Law, Deputy District Attorney at Colorado Judicial Branch, and Term Member at the Council on Foreign Relations, “Black Start: The Risk of Grid Failure from a Cyber Attack and the Policies Needed to Prepare for It,” Journal of Energy & Natural Resources Law, vol. 38, no. 2, https://www.tandfonline.com/doi/abs/10.1080/02646811.2020.1744368?journalCode=rnrl20

In the industrial world, when a switch is flipped, we take for granted that it will produce light, boot a computer, illuminate a stadium or activate a power plant. We know, of course, that power losses can and do occur. Many of us have lit candles during a thunderstorm or brought out extra blankets when a blizzard takes down transmission lines. As of this writing, the most populated state in the United States, California, is experiencing rolling blackouts.1 Yet even in prolonged power outages, we expect that electricity will be restored and, consequently, life will return to normal. Perhaps we need ask, however, what if power cannot be restored in a timely manner? Concern is growing that in the not-too-distant future our electricity supply could be irreparably compromised by a cyber attack. The issue when considering a systemic grid failure of this nature is twofold: how did we reach a point where something so critical to routine life now presents an existential threat, and what can we do to mitigate the risk of a catastrophic grid attack?

This article posits that the emergence of cyber attacks on industrial control systems, as a means of war or criminal menace, have reached a level of sophistication capable of ~~crippling~~ [destroying] those systems. This article argues that a new grid security policy paradigm is required to thwart catastrophic grid failure – a paradigm that recognises the inextricable link between commercial power generation and national security. In section 5, seven policy recommendations are outlined that may, in part, mitigate a future where grid attacks pose existential risk to nations and their citizenry. Those recommendations are: first, develop a comprehensive insurance programme to minimise the financial risk of grid disruption; second, train more cybersecurity professionals with particular expertise in industrial control systems; third, institute a federally mandated information-sharing programme that is centralised under United States Cyber Command; fourth, subsidise and/or incentivise cybersecurity protections for small to mid-size utilities; fifth, provide university grants for grid security research; sixth, integrate new technologies with an eye towards securing the grid; and, lastly, formulate clear rules of engagement for a military response to grid disruption.

The purpose of this article is to provide the reader with an introduction to this complex topic. It is the aim of the author to give orientation to this issue and its many branches in the hope that better understanding will animate further curiosity and, ultimately, positive action on the part of the reader. Although many skilled and earnest people work tirelessly to prevent a grid failure scenario, it is essential that more be added to their ranks each day. Advisors, engineers, regulators, private counsel to power generators, and many others who play roles in electric power production are crucial to this subject. So, while this article provides entrée to the topic of grid security, its long-term objective is to spur action by the entire energy-related community. In the end, no one is immune to consequences of grid failure and, therefore, everyone is responsible, in part, for promoting grid integrity.2 In this regard, lawyers who represent various actors in the energy sector are going to be faced with questions and potential legal risks of a magnitude that they have never experienced before.

1.2. Turning the power back on in a powerless world

‘Black start’, not to be confused with the term ‘blackout’, is the name given to the process of restoring an electric grid to operation without relying on the external electric power transmission network to recover from a total or partial shutdown.3 At first glance, this description is unremarkable, but it implies a disturbing catch-22 – how might one restore power if the entire external transmission network is compromised?

If an electric disruption occurs at a household level, some homes may be equipped with a modest gasoline generator to temporarily restore power. If a hospital loses power, it will almost invariably be resupplied by automatic, industrial-scale generators. These micro considerations hardly give anyone pause; they are hiccups on a stormy night or a snowy day. In other words, their ‘black start’ is a quick and effective process for restoring power. But what happens, at a macro level, when an electric grid supplying power to large portions of the United States goes black, or worse, what happens if all of the United States’ electric grids go down simultaneously?4 In that scenario, how might enough non-grid power be harnessed and transmitted to turn the United States’ lights back on? Moreover, how might such a catastrophe occur in the first place? Perhaps the more ominous question is not how, but whether or not we can survive such circumstances if they persist in the long term.

The United States electric grid (‘the grid’) is the ‘largest interconnected machine’ in the world.5 It consists of more than 7000 power plants, 55,000 substations, 160,000 miles of high-voltage transmission lines and millions of low-voltage distribution lines.6 The scale and complexity of the grid in the context of the modern digital world are beyond comprehension because within it are innumerable industrial control systems; incalculable connections to digital networks; millions, if not billions, of analogue or digital sensors; many thousands of human actors; and trillions of lines of programming code.7 Further complexifying the grid is that it is comprised of generations of technologies, stitched together in ways that are not inherently secure in a world of cyber threats.8 The vastness of the grid makes security of it challenging. Likewise, the vastness of the grid makes the opportunities for intrusion seemingly infinite.

By any measure, grid failure will unleash a parade of horrors. Stores would close, food scarcity would follow, communication would cease, garbage would pile up, planes would be grounded, clean water would become a luxury, service stations would yield no fuel, hospitals would eventually go dark, financial transactions would stop, and this is only the tip of the iceberg – in a prolonged grid failure social chaos would reign, once-eradicated diseases would re-emerge and, increasingly, hope of returning to a normal life would fade.9 The notion of complete grid failure, once relegated to science fiction comics or James Bond movies, is now not only possible but also one of the most pressing national security threats today.10

#### Scenario 2 – Shipping --- the industry is especially vulnerable to inevitable cyber attacks

Ben Farah et al 22 --- Mohamed Amine Ben Farah et al, Department of Networks and Cyber Security, Birmingham City University, “Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends”, Information 2022, 13, 22, https://www.mdpi.com/2078-2489/13/1/22/pdf

Maritime transportation is central to the economic sustainability of many regions throughout the world. The growth in global population, improvements in living standards and investment and elimination of trade barriers all contribute to driving an ever-increasing reliance on the industry. In geographies with navigable rivers or comprising a cluster of islands, maritime transportation is the spine to both domestic and international trading. Moreover, in markets that demand sustainable development, low cost, efficiency and, recently of growing importance, ecofriendly operations, the maritime sector is responsible for 90% of the transportation of all goods [1,2]. Recent developments in the Internet of Things (IoT), Big Data and Artificial Intelligence have enabled the migration to more digitalised maritime infrastructures and, consequently, have necessitated a renewed assessment of the cyber-security provision [3]. Furthermore, connectivity and reliance on intelligent devices play a pivotal role in motivating cyber criminality such as social engineering, identity theft and spam emails. The protection of the integrity of next generation maritime infrastructures is a pressing need [4–7].

Connectivity through navigation systems such as Automatic Identification System (AIS, see Abbreviations), Global Navigation Satellite System (GNSS) and Radio Detection and Ranging (RADAR) impacts negatively on the security level of infrastructures. Moreover, shipping companies have been subjected to highly complex and new classes of cyber attacks targeting in-port information systems and inflicting damage on on-vessel core equipment [8,9]. The reliance on the Internet, operating with unprotected computers, and the fact that crews do not receive appropriate security training increase further the probability of a successful cyber breach. There is clear evidence that the absence of structured security awareness training for employees across the supply chain is a major source of vulnerabilities; as a result, hackers can use classical approaches such as spam emails or Denial-of-Service (DoS) attacks to achieve successful breaches [10,11]. A security plan providing recommendations to protect the maritime supply chain and a co-coordinated strategy with international marine organizations is a near-term necessity [12]. The update of software through removable media increases the risk of stealing identities and in-port data and the sharing of information in real time using new technologies—such as IoT—exacerbates the risk due to insecure network services or weak authentication.

#### European ports are particularly vulnerable

Muncaster 22 --- Phil Muncaster UK / EMEA News Reporter, Infosecurity Magazine, “Cyber-Attacks Hobble Some of Europe's Largest Ports”, Feb 4th 2022, https://www.infosecurity-magazine.com/news/cyberattacks-hobble-europe-ports/

Oil terminals in some of Europe’s biggest ports appear to have been disrupted by ransomware, according to reports.

A broker in the region told AFP that the attacks are disrupting the oil supply chain.

“There was a cyber-attack at various terminals, quite some terminals are disrupted,” Jelle Vreeman, senior broker at Riverlake in Rotterdam, told the newswire.

“Their software is being hijacked, and they can’t process barges. Basically, the operational system is down.”

The Amsterdam-Rotterdam-Antwerp oil hub, which spans ports across the Netherlands and Belgium, is believed to have borne the brunt of the attacks. AFP cited local Belgian reports that logistics and storage firm SEA-Tank Terminal is one of those impacted in Antwerp.

According to a separate report from The Associated Press, at least two energy companies in the Belgian ports of Antwerp and Ghent were hit by cyber-attacks, with the government’s Federal Computer Crime Unit opening an investigation.

This follows reports earlier this week that two German oil logistics firms were struck by ransomware: Oiltanking GmbH Group and Mabanaft Group.

Both companies were forced to declare force majeure, a legal clause used in emergencies when companies cannot fulfill their contractual obligations.

However, the head of Germany’s federal office for information security, Arne Schönbohm, is quoted as saying the incident is serious but “not grave.”

Anglo-Dutch oil giant Shell has already admitted it has been forced to reroute supplies due to the incident.

The news has uncomfortable echoes of the Colonial Pipeline attack in May 2021, which crippled oil supplies up and down the US east coast for days, leading to queues at gas stations.

This time the culprit, at least in the attacks in Germany, appears to be BlackCat (aka “alphv”), a relatively new ransomware-as-a-service variant.

#### Kills billions and causes LNG city attacks on par with nukes

Sincai 21 --- Avital co-founded and heads as the COO in Cydome, Maritime Cyber Attacks Are Among the Greatest Unknown Threats to the Global Economy, June 28, https://www.cpomagazine.com/cyber-security/maritime-cyber-attacks-are-among-the-greatest-unknown-threats-to-the-global-economy/

The fact is, if the maritime industry suddenly disappeared without a trace, the economic, social, and political impacts would be devastating. Billions of tons of vital products like food, medicine and oil are shipped around the world every year, and if these goods stopped flowing, billions of people would suffer the consequences. We saw a taste of this devastation early this year, when a ship lodged itself in the Suez Canal, blocking other ships from getting through. The incident cost the world nearly $10 billion in trade each day it was stuck.

This is only a fraction of the damage that could be caused by cyber attacks in the maritime industry.

There are various vectors for hackers to attack which could result in taking full control over a vessel or fleet, creating damage to critical systems on board or it could just be ransomware or a malicious virus attempting to take control. In one of the cases, we have seen that hackers took control of the pipeline and essentially held it hostage until they were transferred a certain amount of money they requested. In the end, faced with no other option, the pipeline company paid $4.4 million in ransom to the foreign hackers, according to the Colonial Pipeline CEO.

The hackers then reopened the pipeline, but the damage had already been done. The Colonial pipeline transferred huge amounts of oil across the country, and the shutdown caused massive shortages and panic buying. Gas prices went up across the country as a result of just a few hackers managing to exploit a vulnerability in the pipeline’s system. It’s easy to see from this one incident, how cyber attacks can affect much more than your personal computer.

Now, it is evident that the greatest cyber threat lies in the maritime industry. The COVID-19 pandemic sped up the already occurring digitization of the world, as a result of guidelines that required people to work from home over the internet. As such, the maritime industry also had to rely more heavily on the internet than ever before. You may not think of vessels and fleets as deeply connected with technology, but vessels are constantly connected to the internet.

Here’s where the real problem lies: some of the systems and computers on these vessels often use incredibly complicated and old systems. This makes it much harder to protect them from cyber attacks. The systems that these ships use are so complexly intertwined that there are many blind spots that are virtually unknowable.

Since the maritime industry is shifting into the digital age, and since the pandemic has forced it to rely even more heavily on the internet, there have verifiably been more cyber attacks on vessels recently. In only the first few months of the pandemic alone, attempted cyber attacks on maritime vessels shot up by 400%. This dramatic increase has truly sent a shockwave through the maritime community. The industry is one of the oldest industries in the world, and so it was surprising to some, how much they could be affected by just a few hackers.

Imagine if a hacker took control of a ship that was carrying something truly vital, like COVID vaccines. At this point, the internet is so deeply integrated with maritime systems, it would be impossible to switch to a manual system, so hackers would have full control.The hacker could shut down the ship for as long they wanted to, and as in the case of the Colonial pipeline, there is nothing the owner of the vessel could do but give them whatever it is they were asking for. Significant delays could cause millions, even billion dollars in economic damage, and have even more social and political effects.

Imagine if a hacker with malevolent intent took control of an oil tanker, containing millions of gallons of flammable liquid, and decided to do something terrible with it? We’ve seen oil spills before, but LNG tankers are so dangerous that even a small amount of damage could cause an explosion on the scale of a nuclear bomb. So what can we do?

#### Great power war

Liu 18 --- Qian Liu is an economist based in China, The next economic crisis could cause a global conflict. Here's why, https://www.weforum.org/agenda/2018/11/the-next-economic-crisis-could-cause-a-global-conflict-heres-why/

The response to the 2008 economic crisis has relied far too much on monetary stimulus, in the form of quantitative easing and near-zero (or even negative) interest rates, and included far too little structural reform. This means that the next crisis could come soon – and pave the way for a large-scale military conflict.

The next economic crisis is closer than you think. But what you should really worry about is what comes after: in the current social, political, and technological landscape, a prolonged economic crisis, combined with rising income inequality, could well escalate into a major global military conflict.

The 2008-09 global financial crisis almost bankrupted governments and caused systemic collapse. Policymakers managed to pull the global economy back from the brink, using massive monetary stimulus, including quantitative easing and near-zero (or even negative) interest rates.

But monetary stimulus is like an adrenaline shot to jump-start an arrested heart; it can revive the patient, but it does nothing to cure the disease. Treating a sick economy requires structural reforms, which can cover everything from financial and labor markets to tax systems, fertility patterns, and education policies.

Policymakers have utterly failed to pursue such reforms, despite promising to do so. Instead, they have remained preoccupied with politics. From Italy to Germany, forming and sustaining governments now seems to take more time than actual governing. And Greece, for example, has relied on money from international creditors to keep its head (barely) above water, rather than genuinely reforming its pension system or improving its business environment.

The lack of structural reform has meant that the unprecedented excess liquidity that central banks injected into their economies was not allocated to its most efficient uses. Instead, it raised global asset prices to levels even higher than those prevailing before 2008.

In the United States, housing prices are now 8% higher than they were at the peak of the property bubble in 2006, according to the property website Zillow. The price-to-earnings (CAPE) ratio, which measures whether stock-market prices are within a reasonable range, is now higher than it was both in 2008 and at the start of the Great Depression in 1929.

As monetary tightening reveals the vulnerabilities in the real economy, the collapse of asset-price bubbles will trigger another economic crisis – one that could be even more severe than the last, because we have built up a tolerance to our strongest macroeconomic medications. A decade of regular adrenaline shots, in the form of ultra-low interest rates and unconventional monetary policies, has severely depleted their power to stabilize and stimulate the economy.

If history is any guide, the consequences of this mistake could extend far beyond the economy. According to Harvard’s Benjamin Friedman, prolonged periods of economic distress have been characterized also by public antipathy toward minority groups or foreign countries – attitudes that can help to fuel unrest, terrorism, or even war.

For example, during the Great Depression, US President Herbert Hoover signed the 1930 Smoot-Hawley Tariff Act, intended to protect American workers and farmers from foreign competition. In the subsequent five years, global trade shrank by two-thirds. Within a decade, World War II had begun.

To be sure, WWII, like World War I, was caused by a multitude of factors; there is no standard path to war. But there is reason to believe that high levels of inequality can play a significant role in stoking conflict.

According to research by the economist Thomas Piketty, a spike in income inequality is often followed by a great crisis. Income inequality then declines for a while, before rising again, until a new peak – and a new disaster. Though causality has yet to be proven, given the limited number of data points, this correlation should not be taken lightly, especially with wealth and income inequality at historically high levels.

This is all the more worrying in view of the numerous other factors stoking social unrest and diplomatic tension, including technological disruption, a record-breaking migration crisis, anxiety over globalization, political polarization, and rising nationalism. All are symptoms of failed policies that could turn out to be trigger points for a future crisis.

Voters have good reason to be frustrated, but the emotionally appealing populists to whom they are increasingly giving their support are offering ill-advised solutions that will only make matters worse. For example, despite the world’s unprecedented interconnectedness, multilateralism is increasingly being eschewed, as countries – most notably, Donald Trump’s US – pursue unilateral, isolationist policies. Meanwhile, proxy wars are raging in Syria and Yemen.

Against this background, we must take seriously the possibility that the next economic crisis could lead to a large-scale military confrontation. By the logic of the political scientist Samuel Huntington , considering such a scenario could help us avoid it, because it would force us to take action. In this case, the key will be for policymakers to pursue the structural reforms that they have long promised, while replacing finger-pointing and antagonism with a sensible and respectful global dialogue. The alternative may well be global conflagration.

#### Effective information sharing solves every cyber impact --- builds resilience --- but all types of data are key

Balson 20 --- David Balson et al, Director of Intelligence, Ripjar Technologies, Lead author of “Cyber Information Sharing: Building Collective Security”, World Economic Forum, INSIGHT REPORT OCTOBER 2020, https://www3.weforum.org/docs/WEF\_Cyber\_Information\_Sharing\_2020.pdf

Knowledge is power. Intelligence, carefully curated from the collection, evaluation and assessment of data from many sources is fundamental to understanding the complex and dynamic threats that exist in the information age. Once only the preserve of government departments and military agencies, intelligence now helps businesses and global institutions make better, data‑driven decisions. It gives them the edge in formulating new plans and strategies to manage risk, and to perform efficiently and effectively.

Such is the scale and complexity of the challenge, cyberthreats and risks must be understood in detail if organizations want to prevent breaches and prosper in the age Fourth Industrial revolution. Cybersecurity is defined by its multistakeholder ecosystem and needs to be seen from a holistic viewpoint. All participants in that ecosystem need to be able to participate in building the systemic resilience of the collective infrastructure on which those stakeholders rely.

The scale of the cybersecurity challenge facing global institutions requires a mindset shift from traditional models for managing business and security risks. It is no longer feasible to rely on one’s own capabilities; instead a step change will be essential to the future of business resilience. No single organization has visibility over the entire problem space, making collaboration and information sharing essential.

Information sharing and having the ability to use it helps build resilience and drives collective action. It is one of the most fundamental tools that an enterprise or organization has to protect itself. This, however, must be the right type of information sharing to solve the complex problems. Each security community is different and must define the fundamental insights required to protect itself, be this technical information or insights into strategic behaviours or trends. The ability to share the right insights at the right time in a systematic way with the right stakeholders will allow for the effective protection of assets, intellectual property and business processes.

Cyber information sharing as a platform for collective resilience

Cyber information sharing is the ability of an ecosystem to be able to share at scale intelligence with many different stakeholders to generate the right level of situational awareness for organizations to defend themselves. By doing this the ecosystem can answer what has been, and what can be done about malicious activity. Organizations need to be able to do this in three key domains:

1. Strategic: Information that can help enterprises understand the type of threat they are defending against, the motivation and capability of the threat and the potential consequences and risks of attacks.

2. Operational: Information that can help enterprises’ decision‑making, resource allocation and task prioritization. It includes trend analysis showing the technical direction of threat actors and an understanding of malicious tactics, techniques and procedures.

3. Technical: Information from technical data, sources and systems that provide insights that can influence tactical decisions. This data is typically derived from near real‑time monitoring and sharing of network information required for adjusting an organizations security.3

### Contention 2: Attribution

#### Contention 2 is Attribution:

#### First --- Lack of intel sharing undermines trust in attribution --- crushes NATO cohesion

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”, Lawfare, February 14, 2019 https://www.lawfareblog.com/dont-let-cyber-attribution-debates-tear-apart-nato-alliance

The United States still struggles to find effective policies for deterring cyberattacks. Suggestions run the gamut from more widespread use of indictments and economic sanctions, despite their lackluster record of success, to less traditional but more risky policies that emphasize the asymmetric advantage America has in conventional military power.

Most of the discussion of cyber deterrence focuses on preventing a single catastrophic or cascading cyberattack that would threaten lives (like disruptions to electricity transmission or clean water)—or our way of life—altering election outcomes or grinding global finance to a halt. Yet the reality is that in the event of such an attack, the response would likely not come from the U.S. alone but from the NATO alliance in concert.

NATO’s cyber-defense mandate has evolved over time to update its collective defense commitment under Article V of the North Atlantic Treaty for the era of cyberattacks. In the latest effort to collectively impose costs on adversaries, the 2018 NATO Summit saw a commitment from heads of state and government “to integrate sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions, in the framework of strong political oversight.” The newly updated White House National Cyber Strategy likewise envisions working together with a “coalition of like-minded states” to “ensure adversaries understand the consequences of their malicious cyber behavior.”

Therein lies the rub. Both formal alliances, such as NATO, and more ad hoc arrangements, such as what the Cyber Deterrence Initiative imagines, will require members to share intelligence and eventually, to the best of their ability and perhaps in different domains, contribute to joint action against a presumably well-armed foreign aggressor. States including the United States, the United Kingdom, the Netherlands, Estonia, and Denmark have publicly declared their willingness to lend sovereign offensive cyber effects to deter, defend against and counter the full spectrum of threats.

Sharing intelligence and information is a key element of NATO’s core decision-making process enshrined in Article 4 of the Washington Treaty. Political consultations are part of the preventive diplomacy between member states, but they are also an avenue to discuss concerns related to the security threats member states face. These consultations can be a catalyst for reaching a consensus on policies to be adopted or actions to be taken—including those on the use of sovereign cyber effects to support a NATO operation.

The alliance has a track record of collective action and cooperative security measures. For example, Operation Active Endeavour helped to deter, disrupt and protect against terrorist activity in the Mediterranean in the aftermath of the 9/11 terrorist attacks, in solidarity with the United States. For the seventh time, the Atlantic Council’s Cyber Statecraft Initiative will be among the organizations privileged to organize an event on the sidelines of the Feb. 15–17 Munich Security Conference. This year in particular, the Atlantic Council’s event, “Defending Human Dignity: Limiting Malicious Cyber Activity Through Diplomacy,” will complement the topics high on the agenda of the main conference, such as transatlantic collaboration, the consequences of a resurgence of great power competition and the future of arms control.

In the United States, the greatest failures of response and deterrence to foreign aggression in cyberspace have not been caused by a lack of intelligence, capability or imagination. Rather, U.S. policy has been serviceable in theory but impotent in practice because of an inability to translate technical findings and intelligence into public support for sufficiently tough responses ordered by elected political leaders. North Korea’s repeated operations targeting U.S. companies and critical infrastructure have been met with public skepticism over their culpability, limiting the strength of retaliatory options needed to deter further events. Chinese cyber economic espionage continued for years despite widespread knowledge of China’s activities because political leaders found it difficult to confront Beijing without undermining U.S. companies in return. Russian information operations did not sow enough doubt to mislead experts, but they succeeded in exacerbating the partisan polarization of an already-divided electorate and its leaders.

That inability to translate the findings of cyber experts into public sentiment and therefore political action has sidelined America’s cyberwarriors, by far the most technologically advanced and well-resourced in the world. Imagine the political response of an ally that is asked to burden-share in response to cyber aggression but is probably much closer to any resulting kinetic fight than the United States.

Now imagine the response of that ally when it’s being asked to take causus belli on faith: The United States is presenting attribution for a cyberattack elsewhere in the world, but perhaps is depending on the ally lacking critical details due to classification, and is presenting that information alongside a request for help that might well put the ally in the crosshairs of its own cyberattack or lethal action. How can allies with different capabilities to collect, analyze and understand intelligence be part of a consensus on using sovereign cyber effects to support a NATO operation? How can a commander achieve a common operational picture to authorize the use of sovereign effects in a NATO operation if all the allies are not on the same page with respect to critical attribution and other technical information needed for a use of effect in an operation? We all know what a tank looks like on a shared satellite image, but if you ask three cyber experts to interpret the attribution for a set of indicators, you are likely to get at least four answers.

For most U.S. allies in Europe and elsewhere, there is simply a dearth of technical know-how within the government when it comes to cyber attribution and operations. This is already a challenge for the United States, with a massive defense budget, Silicon Valley innovation and an educated workforce to pull into government service. But for many U.S. allies, tech-savvy public servants will have long fled for the private sector, nongovernmental organizations (NGOs) and academia before reaching ministerial positions.

To its credit, the U.S. National Cyber Strategy does propose capacity-building measures to support allies. This means building up law enforcement, intelligence, and military operational and investigative capability. But even with successful capacity-building programs, many nations could, in a crisis, end up in the same place the United States is—with good options stuck on the shelf while political leaders and their electorates lack a critical mass of informed voters to trust, understand and act on expert findings.

For countries weighing whether to risk their own blood and treasure in support of an ally’s cyber attribution findings, this hurdle could well prove insurmountable if not addressed well before a crisis emerges. Many such countries will no doubt recall being burned when placing too much confidence in U.S. technical and human sources without an ability to evaluate the evidence for themselves, as with the Iraq weapons of mass destruction findings.

The private sector will probably play a crucial role in providing intelligence to support alliance responses to cyberattacks, especially as a stopgap over the next few years. FireEye and its peer competitors and partners regularly produce analyses of major world cyber events—many that fly below the radar of Western leadership, in fact—sometimes at a near-government quality and often covering much of the same “classified” evidence.

More important, private-sector analysts are accustomed to writing for impact with both their technical counterparts, like chief information security officers (CISOs) and threat hunters, and nontechnical stakeholders such as boards of directors, CEOs and other persons controlling the purse strings. In this sense, unclassified, private-sector and NGO-driven cyber threat intelligence can become the lingua franca of discussions. Relying on commercial reporting generated by international teams, rather than declassified government-generated reports, both broadens the audience enough to make alliance discussions feasible and mitigates against disparities in terminology across national lines—the tendency of even closely integrated allies to describe cyber “attack,” “information operations,” and attribution findings with different implicit assumptions or implications.

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.

#### Second --- Hostile actors will use ambiguity to undermine NATO cohesion --- attribution through intelligence sharing is essential to collective response and deterrence

Christian 20 --- Joshua D. Christian, M.A. in Strategic Studies from Naval Postgraduate School, “RUSSIAN CYBER OPERATIONS TO DESTABILIZE NATO”, Thesis Paper, June 2020, https://apps.dtic.mil/sti/pdfs/AD1114628.pdf

Russia’s apparent interest in destabilizing NATO at the strategic level likely entails degrading relationships not only within the Alliance but also within individual states of the Alliance. Karlsen notes that promoting division within the Alliance is what Western security institutions believe to be a key goal of Russian cyber operations.323 Due to this, cyber attribution is a critical aspect of responding to a cyber operation and NATO needs to denounce and openly attribute blame to the provocateur of a cyber operation. Open attribution places the aggressor state in the international spotlight which works to deter that state from future operations. It is the recommendation of this author that NATO adjust its posture and demonstrate a willingness to denounce any cyber activity that experts believe is from Russia. The case studies demonstrate the significant challenge to investigate and accurately attribute responsibility for cyberattacks. It is the recommendation for policy makers to conduct ongoing research and analyze findings to guide countermeasures and training.

Currently, not all NATO states are as willing as the United States to attribute blame for a cyber operation. The French presidential election provided documented evidence that resulted in the U.S. government’s willingness to blame Russia; in contrast, the French government refrained from directly attributing the cyber operation to Russia.324 In order to strengthen the Alliance and its position as a leading institution, NATO leaders are encouraged to evaluate future events and require collective recognition and responses to Russian cyber operations. A collective response and agreement from all of the NATO states, in response to a cyber operation against one member, displays a unity within the Alliance that further strengthens NATO. A unified NATO response demonstrates a strong Alliance that will minimize Russia’s ability to create division within the states and an Alliance that is prepared to respond to any threat.

2. Determine NATO Threshold for Response and Retaliation

The NATO Alliance is centered around the Article 5 commitment to collective defense from a conventional attack. In 2019, NATO Secretary General Jens Stoltenberg affirmed that “a serious cyberattack could trigger Article 5.”325 This is an evolving stance on cyberattacks that the Alliance did not demonstrate during previous incidents of Russian cyber operations analyzed in this thesis. Russia was able to carry out those cyber operations with minimal repercussions due to the issue of attribution. Following a systematic intelligence gathering and review, the NATO Alliance will be better equipped to determine the threshold for an Article 5 response. Creating and implementing NATO guidelines and strategies to evaluate, identify, and respond to cyber threats, allows NATO the ability to compare and contrast previous attacks against present threats to determine thresholds in each case. NATO should then publish a statement that all NATO member states have come together to determine the threshold for a cyber Article 5 response and are committed as an Alliance to respond to such an attack. Determining a threshold and then reaffirming commitment to retaliating to an Article 5 attack extends the longstanding strength of the Alliance, which in turns solidifies its legitimacy as an institution.

Not every cyber threat or cyberattack will warrant an Article 5 response, but in order to display the strength and commitment of the Alliance, a measured response is a critical tactic from the Alliance. For Russian attempts to interfere with the domestic electoral proceedings of a NATO member the Alliance could invoke Article 4 which states “The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened.”326 This allows the Alliance to come up with a unified response to a threat to a member state. Cyber operations involving influence operations or critical infrastructure threats warrant individual evaluation. NATO needs to develop guidelines for responding to cyber operations against member states that handle operations on a case by case basis. Not all operations are undertaken for the same purpose and therefore require strategic responses. NATO has exercised responses to issues below the threshold of Article 5 for conventional matters; implementing guidelines and strategies in response to a cyber threat below this threshold would strengthen the legitimacy of NATO in cyber while deterring future adversaries.

3. Strengthen Intelligence Sharing Cooperation

Intelligence sharing is a key element of any alliance, and NATO member states are obligated to continually improve and strengthen intelligence cooperation. Greater cooperation between NATO states strengthens the Alliance as well as prepares states to defend against cyber operations while creating a deterrent. Greater intelligence cooperation will lead to further strengthening NATO resiliency and defense as specified in Article 3 which states “In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.”327 Cooperation and collaboration between partner states makes it more difficult for an adversary, such as Russia, to carry out a cyber operation against a NATO state. In the French presidential election, the U.S. government was able to communicate with the French government to alert it to Russian cyber activity meant to interfere in the election.328 Continual intelligence sharing between NATO members enables them to design and implement cyber defenses resulting in a stronger Alliance.

Cooperation between NATO states is crucial to strengthening cyber defenses; additionally, it is critical that policies identify cooperation between state and private entities. Private cybersecurity firms as well as areas of critical infrastructure of a state need to work closely with government agencies to create a stronger defense network. Dragonfly wasfirst discovered by cybersecurity firm Symantec, a discovery which led to governments being able to track the cyber operation back to the Russian government.329 Private entities may discover suspicious cyber activity and through close cooperation with government agencies could deter, defend, and even attribute cyber operations before an attack or effective information operation could take place. Intelligence sharing and cooperation within a NATO state can then be taken to the Alliance to be shared with other states and private entities. Close collaboration and intelligence sharing benefits the Alliance and further strengthens its commitment to the defense of NATO states.

#### Unity solves nuclear war

The Economist 22 --- “In Ukraine, Biden must relearn Truman’s lessons from the cold war”, March 26th 2022, <https://www.economist.com/united-states/2022/03/26/in-ukraine-biden-must-relearn-trumans-lessons-from-the-cold-war>

America once again seeks to curb Russia and China without blowing up the world

Joe biden entered the White House last year styling himself on Franklin Roosevelt. The better model today might be Harry Truman. His words to Congress 75 years ago this month—“It must be the policy of the United States to support free peoples who are resisting attempted subjugation by armed minorities or by outside pressures”—girded America for the cold war. Those words have a new resonance as Ukraine, helped by the West, battles to resist Russia’s month-old invasion.

As in the 1940s and 50s, the world is separating into distinct blocs. The Eurasian giants, Russia and China, are again making common cause. America is seeking to counter them by mustering allies around their periphery, from Europe to Japan. Truman’s America was engaged in a fight against communism; Mr Biden sees a global contest against autocracy. The cold-war strategy of “containment” is being studied for the current age.

This arouses dread, but also hope. Dread, because of the return of war in Europe, renewed big-power confrontation and the increased risk of nuclear conflict. Hope, because Russia’s military incompetence, Ukraine’s valour and the West’s newfound unity raise confidence that the American-led liberal order can prevail. Writing in American Purpose, an online magazine, Francis Fukuyama of Stanford University, who in an earlier bout of optimism coined the notion of the “end of history” about the demise of the Soviet Union, goes so far as to predict that Ukraine will inflict “outright defeat” on Russia and make possible a “new birth of freedom”.

Mr Biden’s strategy will become clearer in the coming days. On March 24th he was due to take part in a trio of summits in Brussels with the leaders of nato, the European Union and the g7. The signs are he will steel the allies for a long struggle. “This war will not end easily or rapidly,” said Jake Sullivan, his national security adviser, on March 22nd. The West would stand by Ukraine “for as long as it takes”.

Another signal will be the president’s request for more defence spending in the coming financial year, expected to be sent to Congress next week. A succession of formal strategy documents—for national security, defence and nuclear posture—will follow after hurried redrafting. For Robert Gates, a former American defence secretary, the war “has ended Americans’ 30-year holiday from history”. Ahead lies a two-front contest, against both Russia and China. “A new American strategy must recognise that we face a global struggle of indeterminate duration against two great powers that share authoritarianism at home and hostility to the United States,” he wrote in the Washington Post.

Strategists are reaching for the annals of the cold war. Is Vladimir Putin’s invasion akin to the Soviet Union’s blockade of Berlin in 1948, the start of the Korean war in 1950 or the Cuban missile crisis of 1962? Some are re-reading George Kennan, the American diplomat whose “long telegram” from Moscow in 1946 set the intellectual foundation for containment. American “unalterable counterforce”, Kennan argued in a later essay, could hasten “either the break-up or the gradual mellowing of Soviet power”. In practice containment involved more than the high-minded means Kennan imagined, such as the Marshall plan to rebuild Europe. It also involved coercive instruments: military alliances and build-ups, nuclear standoffs, proxy wars and much else short of a direct conflict.

Dean Acheson, Truman’s secretary of state, wrote that America’s task after 1945 was “just a bit less formidable than that described in the first chapter of Genesis. That was to create a world out of chaos; ours, to create half a world, a free half, out of the same material without blowing the whole to pieces in the process.”

Mr Biden’s burden is to prevent the world from reverting to chaos, and to preserve as much of the free portion as possible. Russia today may be a lesser foe than the Soviet Union, “a wounded empire” rather than a superpower with a global ideology and a semi-autarkic economic hinterland, as Eliot Cohen of Johns Hopkins University notes. Yet China is a greater challenger, not least in economic terms. Its navy is already larger than America’s, and it is fast expanding its nuclear arsenal.

To judge Mr Biden, then, consider three measures: first, how he deals with Russia; in the longer term, how he confronts China; and, throughout, how he carries his profoundly polarised country.

Vladimir the terrible

Team Biden had no illusions about Russia. Its early warning about the invasion of Ukraine, and its release of intelligence about the Kremlin’s plans, were innovative and prescient. It denied Mr Putin a pretext, and primed allies to respond forcefully, both by arming Ukraine and by imposing severe sanctions on Russia. Like Mr Putin, however, Mr Biden may have underestimated Ukraine. On the eve of war America seemed to think that, at best, Ukraine might become another Iraq or Afghanistan, easy to invade but hard to control. Instead Russia has found it surprisingly arduous to take Ukraine’s cities, even as it pulverises them. The longer the horrors go on, the greater the cries for the world to stop them.

At their summits in Europe, the Western allies will resolve to strengthen nato’s defences, provide more weapons to Ukraine and increase economic pressure on Russia. Above all, American officials say, they will stiffen their sinews for a long contest as economic pain spreads.

How far dare the allies go in waging a proxy war against a nuclear power? The answer keeps shifting. In 2014, when Russia took a first chunk of Ukraine, America declined to provide weapons. It later began to deliver anti-tank missiles. Now it is shipping small anti-aircraft weapons and drones. Soon it may facilitate the supply of longer-range air-defence missiles.

Yet there are limits. When Mr Biden vows that America will defend “every inch” of nato’s territory he declares, in effect, that American forces will not defend any inch of Ukraine’s. To get involved directly, says Mr Biden, would be “World War III”. He has refused calls to impose a no-fly zone over Ukraine, act as the intermediary for Polish mig-29 jets or even supply American-made Patriot anti-aircraft batteries.

The point at which America becomes a “co-combatant” will not be decided by lawyers but, ultimately, by Russia. The Kremlin has given notice that arms convoys to Ukraine would be legitimate targets. It has bombed sites close to Poland.

History suggests the boundaries of proxy conflicts can be dangerously fuzzy. Chinese “volunteer” forces fought against American troops in the Korean war of 1950-53, when America considered using atom bombs against them. Russians manned anti-aircraft batteries and, perhaps, flew missions against American aircraft in the Vietnam war of 1955-75.

“During the cold war the United States and the Soviet Union were at daggers drawn but usually did not stab each other directly,” explains Richard Fontaine of the Centre for a New American Security, a think-tank in Washington. Mr Putin has rattled his nuclear sabre, but American officials say they have detected no change in Russia’s nuclear posture, nor have they changed theirs.

Mr Biden’s caution in Ukraine contrasts with his almost careless talk about defending Taiwan against China. Last year Mr Biden said America had a “commitment” to defend the island. America’s “strategic ambiguity”, whereby it promises to help Taiwan defend itself but will not say whether it would intervene directly, has become less ambiguous.

Nobody can say quite why America seems readier to risk “World War III” for Taiwan than for Ukraine. Perhaps the danger in Ukraine is concentrating minds. Some note that America has no alliance with Ukraine, a non-nato country, whereas it has a semi-obligation to Taiwan. The island’s important semiconductor industry is a consideration. The main reason is that America considers China, not Russia, to be the greatest danger.

“Russia is the acute threat. But China is the pacing challenge, the only country able to challenge the United States systemically,” says a senior American official. “Nothing about the crisis in Ukraine has changed that.” Or, as one diplomat puts it, “Ukraine is the tsunami; China is climate change.” America’s response in Europe contributes to alliance-building, says the envoy; it will expect Europeans to help in Asia.

The fact that Australia, Japan and other Asian countries have imposed sanctions on Russia is a sign of their fears about the war’s wider repercussions. American military chiefs have warned that a Chinese invasion of Taiwan could happen before the end of the decade. A successful Russian attack on Ukraine might have emboldened China. Now that Russia is bogged down, the danger may have receded.

Russia and China have declared that their friendship has “no limits”. America is hoping that Xi Jinping, China’s leader, will now have second thoughts. In a video summit on March 18th Mr Biden issued a threat to impose sanctions on China if it came to Russia’s aid. One aim of Mr Biden’s trip this week is to push Europeans to deliver the same message at the eu-China summit on April 1st. China maintains the fiction that it is neutral, so could in theory distance itself from Russia. Few in Washington think Mr Xi is prepared to let Mr Putin fail. But America now sees “an opportunity to deal a strategic blow to Russia, and an opportunity to make Russia increasingly a strategic burden for China,” the official says.

#### Independently --- Attribution through information sharing allows NATO to counter hybrid war --- the alternative is an ineffective response

Underwood et al 22 --- Andrew Underwood et al, Major Underwood is Executive Assistant to the Deputy Director for Strategy, Plans, and Policy (J5), Europe, NATO, Russia, “All Quiet on the Eastern Front: NATO Civil-Military Deterrence of Russian Hybrid Warfare” April 14, 2022, National Defense university Press, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2999367/all-quiet-on-the-eastern-front-nato-civil-military-deterrence-of-russian-hybrid/

Information Operations. Another critical aspect of imposing costs and limiting options available through Russia’s hybrid warfare approach is effective IO attribution and response. IO is substantive enough a factor in Russian hybrid warfare to be considered beyond comprehensive defense. Staying abreast of Russian hybrid objectives, methods, and tools prevents Allies and partners from being caught [unprepared] ~~flat-footed~~. It also enables a better understanding of Russian intent and options for hybrid activity, both in traditional spheres and within the gaps and seams of 21st-century technology as an information platform. This analysis focuses on the intelligence- and information-gathering and strategic communication aspects of IO. Intelligence- and information-gathering are critical to identify Russia’s hybrid options and intent and to mobilize NATO member states toward the activity. Conversely, strategic communication is a proactive, comprehensive defense measure to specifically limit Russian hybrid options and to broadcast the costs Russia would incur if it moved forward with them.

For intelligence-gathering to be effective in today’s operating environment, countries must be willing to break down stovepipes and widely share information within their own government structures as well as with Allies and partners. The coordinated actions of hybrid warfare allow Russia to exploit regional, national, and international seams. Building intelligence-sharing apparatuses both within and without ministries among and across countries helps to close those seams. Effective intelligence-sharing could occur at levels ranging from joint/multinational collection teams to finished intelligence analysis at ministerial or national levels. In other words, information-sharing does not always have to be top-down driven; sometimes bottom-up is effective.

One goal of shared intelligence is to reduce the time required for NATO to consult and respond in part or as a whole. This effort could be facilitated by a common intelligence picture shared by all parties. Partial, inconsistent, or stovepiped intelligence might slow NATO’s response process by creating doubt or failing to correctly attribute malign activity to the Russian government. In addition, whether internal to a state or between allied states, stovepiping challenges coordinated action against hybrid warfare. Better intelligence-sharing would allow states to deny Russia the benefit of using IO techniques in hybrid warfare to isolate specific states or populations. A common intelligence picture also makes it more likely, for example, that a Russian intelligence operative or team preparing to assassinate a dissident would be identified and detained, and have the network and messaging compromised. An example of intelligence-sharing success within NATO nations against hybrid activity is the Baltic Special Operations Forces Intelligence Fusion Cell, a budding Estonian, Latvian, Lithuanian, and Polish initiative that operates with assistance from the United States.20 If implemented properly, such intelligence fusion cells might provide key indications and warnings of Russian hybrid warfare operations across the spectrum of IO, denying Russia the benefit of being able to claim noninvolvement/noninterference and could serve as a template for future initiatives among other Allies and partners. Furthermore, such fusion cells provide a path for connecting information across the Alliance’s multiple stovepipes, that is, the intra- and inter-bureaucratic inertia and the multilingual nature of the information environment. This enables a common intelligence picture and, consequently, the ability of the Allies to collectively deny Russian IO to access seams unfettered and without attribution.

Once Russian hybrid warfare IO activity is recognized and NATO agrees a response is appropriate, strategic communication would likely be employed as the principal countermeasure and vanguard to prevent Russian activity. The situational awareness derived from the shared information and intelligence discussed in the previous section would be critical to crafting targeted messages. Strategic communication would likely be split between two audiences: external actors and an audience internal to the conflict (that is, the targeted population). Internal strategic communication efforts should focus on countering the information aspect of hybrid warfare. Prior to a campaign, successful strategic communication might limit the vulnerability to target audiences, such as the Russian-speaking minorities of the Baltic states, or a Russian hybrid campaign. This is achieved by negating Russia’s plausible deniability concerning the sponsorship of the conflict’s version of “little green men” (or whatever the aggressor looks like in that campaign). Internal strategic messaging campaigns must be swiftly organized and executed because they are most effective if they prevent Russia from gaining a tactical advantage during the initial “fog of war” period. Once a hybrid warfare campaign has begun, the focus of external strategic communication should be to expose Russian activities to NATO (and the rest of the world). This might undermine Russian public support for such activities, would inform decisionmakers during NATO deliberations, and should unite the international community against the malign actor.

#### Failure to share information makes Russia hybrid attacks successful

Beaulieu & Salvo 18 --- Brittany Beaulieu, fellow and program officer for GMF's Alliance for Securing Democracy, and David Salvo, deputy director of the Alliance for Securing Democracy (ASD) and a senior fellow at the German Marshall Fund, German Marshall Fund of the United States (2018), “NATO and Asymmetric Threats:: A Blueprint for Defense and Deterrence”, https://www.jstor.org/stable/pdf/resrep18856.pdf

While NATO and the EU have pledged to improve their information sharing and coordination of responses across the asymmetric toolkit, these efforts are under-funded and lack high-level coordination. Moreover, the absence of a mechanism to share NATO classified information with the EU, an old problem, prevents both organizations from more systematic cooperation in responding jointly to the hybrid challenge. The lack of information sharing among allies at NATO is another challenge. For example, the United States did not share much information about the Russian operation against the 2016 presidential election as it unfolded and only a meager amount afterward. In the lead up to the French and German elections, information was shared on a bilateral basis, rather than through the NAC. The reservations of some allies to discuss their own vulnerabilities to interference operations only exacerbate NATO’s organizational impediments to addressing hybrid threats in a timely and coordinated manner. A formalized information sharing or early warning mechanism could help to rectify this problem, as would decisions in allied capitals to elevate discussion on hybrid threats at the NAC and share more threat information and intelligence.

#### Successful hybrid tactics crush democratic models and ensure global backsliding --- attribution and intelligence are key to deter

Wigell 21 --- Mikael Wigell, Research Director at the Finnish Institute of International Affairs, “Democratic Deterrence: How to Dissuade Hybrid Interference”, The Washington Quarterly Volume 44, 2021 - Issue 1, https://www.tandfonline.com/doi/full/10.1080/0163660X.2021.1893027

Much of the debate on new “hybrid” threats has revolved around “little green men” and other grey zone military tactics, or hybrid warfare, essentially a military approach to conducting “indirect war” under special circumstances.4 The more pressing challenges from a Western perspective are the more subtle, non-military activities deployed by authoritarian regimes to penetrate democratic society. “Hybrid interference” is a concept developed to capture non-military practices for the mostly covert manipulation of other states’ strategic interests.5 As such, it bears resemblance to what was referred to as “active measures” during the Cold War and, more recently, in Russian strategic debate as gibridnaya voyna.

The idea of gibridnaya voyna is to avoid the traditional battlefield with the aim of destroying “the political cohesion of an adversary from the inside by employing a carefully crafted hybrid of non-military means and methods that amplify political, ideological, economic and other social polarisations within an adversary’s society, thus leading to its internal collapse.”6 While keeping diplomatic relations intact, and thus not breaking any official threshold of war, the aggressor mobilizes oppositionists and radicals within the target state through a host of means ranging from disinformation campaigns to corrupting political actors and financing subversive movements, carefully synchronized to compound the effect.

Hybrid interference avoids the use of overt kinetic means in order to maintain plausible deniability. Yet, it may include the use of targeted violence, through proxies, to inject fear and exploit emotional pressure points in the target society. In 2014, for example, pro-democracy protesters in Taiwan were attacked by some with links to the Chinese Communist Party to incite political tensions and undermine democratic governability.7 In Montenegro, Moscow instigated a coup attempt before the 2016 elections. The attempt involved harnessing its close relations to the Orthodox Church and the Serb minority population to foment distrust in the democratic process and, in the final phase, using Russian intelligence operatives disguising as police officers to create disruption by shooting protesters and blaming the Montenegrin government for killing innocents.8

Central to hybrid interference is subversion. Subversion refers to an aggressor state’s purposeful attempt to destabilize and undermine the authority of a target state by using local proxy actors.9 It specifically involves the use of disinformation and economic inducements to recruit and assist these actors inside the target country, detach their loyalties from the target government, and use them as interlocutors to transform the established social order and its structures of authority and norms. The aim is to weaken democratic governance and norms as a means of enhancing their own authoritarian standing. Not only are weakened democracies less able to directly confront these authoritarian aggressors, but they will also look less appealing as models of success and partners for others. By portraying Western democracies as corrupt and ungovernable, authoritarian regimes such as China, Iran, Russia, and Turkey are less at risk of being overthrown by their own populations.

As such, hybrid interference is designed as a flexible approach in which the tools and tactics can vary but will always be tailored to manipulate existing cleavages and sow internal dissension in target countries and alliances. Hybrid interference does not adopt a one-size-fits-all approach but exploits specific vulnerabilities depending on the context in the target country. The hybrid aggressor interferes in domestic politics by seeking to amplify divisions and hatred, undermining the “civic culture” that has been found to be so important for democratic governability by tempering the intensity of political conflicts and cleavages.10

The migrant crisis in Europe offered an excellent opportunity for authoritarian aggressors. By exposing rifts between “liberals” and “anti-liberals,” it allowed Russia and Turkey to leverage refugees as a disruptive force, fanning the already simmering political tensions in Europe. Following the outbreak of the Syrian civil war, Russia and Turkey began actively pushing migrants over the borders to Europe, while simultaneously engaging in disinformation campaigns by playing up rumored (or actual) misdeeds by immigrants and portraying European governments as unwilling or unable to manage the influx of people.11 To compound the polarizing effect, Russia also began channeling money to anti-immigrant and anti-EU political parties and movements such as France’s National Front.12 In this way, particularly Russia has contributed to Europe’s surge in anti-immigrant sentiments and populist support, as well as rising democratic dissatisfaction.13

Democratic Deterrence as a Novel Strategy

Western democracies urgently need to find counter measures against hybrid interference, recognizing that traditional military deterrence only works against predominantly military threats. By reducing clarity about who is doing what, or even whether somebody is actually doing anything, hybrid interference complicates traditional deterrence.14 Yet, the attribution problem is not insurmountable. The responsibility for interfering in US elections, for example, was traced and attributed to Russia, though only after a painstaking process involving much controversy and resources.15 But the question, then, even after the attribution problem is solved, becomes what to do about it? Any prudent deterrence posture needs to avoid unnecessary escalation, and a military response to political interference does not seem proportional.

The strategic concept of democratic deterrence suggests a novel way of thinking about deterrence to dissuade these hybrid interference activities by authoritarian states. Table 1 summarizes the differences between traditional military deterrence and democratic deterrence.

<Table Omitted>

First, in contrast to traditional deterrence that is state-based, democratic deterrence rests on a whole-of-society approach, albeit one in which the state retains a coordinating role. It harnesses market- and society-based actors in an effort to pull together resources and take full advantage of democracy’s societal strengths and cultural capital. This difference is important because in this new era of subversive politics, where the classical Westphalian dichotomy between internal and external state affairs has been blurred, deterrence is harder to achieve by state action alone. Deterring hybrid interference requires a whole-of-society response whereby various societal actors build resilience capacities, support the state in maintaining preparedness, and ensure the continuity of vital societal functions and supply lines. For instance, private actors often own full or partial stakes in critical infrastructure such as energy pipelines, undersea cables, railways, banking and finance, health services, and food supply. Ensuring that they live up to their responsibilities with regard to safety measures must form an essential part of any modern defense. The whole-of-society approach is thus an inclusive model of cooperation and joint preparedness that aims to bring all relevant actors together into a comprehensive system of deterrence. It involves an effort to diversify and devolve responsibilities for security production to market- and societal-based actors, while maintaining a strong coordinating role for the state.

#### Democracy solves great power war.

Larry Diamond 19. PhD in Sociology, professor of Sociology and Political Science at Stanford University. “Ill Winds: Saving Democracy from Russian Rage, Chinese Ambition and American Complacency,” Kindle Edition

In such a near future, my fellow experts would no longer talk of “democratic erosion.” We would be spiraling downward into a time of democratic despair, recalling Daniel Patrick Moynihan’s grim observation from the 1970s that liberal democracy “is where the world was, not where it is going.” 5 The world pulled out of that downward spiral—but it took new, more purposeful American leadership. The planet was not so lucky in the 1930s, when the global implosion of democracy led to a catastrophic world war, between a rising axis of emboldened dictatorships and a shaken and economically depressed collection of selfdoubting democracies. These are the stakes. Expanding democracy—with its liberal norms and constitutional commitments—is a crucial foundation for world peace and security. Knock that away, and our most basic hopes and assumptions will be imperiled. The problem is not just that the ground is slipping. It is that we are perched on a global precipice. That ledge has been gradually giving way for a decade. If the erosion continues, we may well reach a tipping point where democracy goes bankrupt suddenly—plunging the world into depths of oppression and aggression that we have not seen since the end of World War II. As a political scientist, I know that our theories and tools are not nearly good enough to tell us just how close we are getting to that point—until it happens.

### Plan(s)

#### \*\*Plan 1\*\*:

#### The United States federal government should substantially increase cyber threat information sharing with the North Atlantic Treaty Organization

#### Plan 2:

#### The United States federal government should substantially increase cyber threat information sharing, particularly increasing tactical, operational, and strategic information, with the North Atlantic Treaty Organization

#### Plan 3:

#### The United States federal government should substantially increase cyber threat information sharing and cyber incident management with the North Atlantic Treaty Organization

### Solvency

#### Increasing cyber information sharing reduces threats, builds resilience, and allows for effective attribution --- US first-mover key to other countries saying yes

Daniel & Kenway 21 --- Michael Daniel President & CEO Cyber Threat Alliance & Joshua Kenway Cybersecurity Associate Cyber Threat Alliance, “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”, 12 Jan 2021, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE (CCDOE) https://kclpure.kcl.ac.uk/portal/en/publications/cyber-threats-and-nato-2030-horizon-scanning-and-analysis(3724c535-e782-45cf-9272-046670e7100f).html

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.

4. IMPLICATIONS OF INFORMATION SHARING IMPERATIVES

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 barriers, 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, organisations can concentrate on the information types most relevant to them. Information sharing architectures, policies, and systems should assist organisations 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 organisations will share every type of cyber threat information. Most organisations should focus on the types of information most relevant to their business model. For example, under this paradigm, only organisations 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 organisations would primarily consume information about best practices and defensive measures.

The focus of information sharing programmes should change. Since most organisations do not need to produce or consume technical cyber threat information, government cyber security initiatives should reflect this. These programmes should instead encourage most organisations 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 prioritising patches. Most organisations would primarily consume updates to best practice and strategic or tactical warnings. This change would make information sharing programmes more relevant and cost-effective.

Information sharing programmes 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.

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 organisations expected to share technical information would make achieving speed and scale easier. Abandoning the idea that all organisations everywhere should engage in technical cyber threat information sharing makes overcoming the barriers to technical sharing easier. Under this assumption, the number of organisations 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 organisations 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 organisations voluntarily participate in such activities. By focusing sharing activities on the most relevant information types, the time and monetary investment for most organisations would decrease. At the same time, the connection between shared information and the organisation’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 organisations 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 organisations 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 endeavour; organisations must incorporate regular review and implementation into their business processes. Absent a long-term commitment from organisational 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 organisations budget for and sustain over the long-term.

5. CONCLUSION

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 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.

#### Information sharing builds resilience and attribution --- reduces vulnerabilities to attack

Housen-Couriel 22 --- Deborah Housen-Couriel, Chief Legal Officer and Vice-President Regulation for Konfidas Digital Ltd., a cyber and data protection consulting firm, She currently serves on the Advisory Board of the Hebrew University Law School’s Cyber Security Research Center and as a research fellow with the Reichman University’s Interdisciplinary Center Herzliya’s Institute for CounterTerrorism, Chapter 3 “Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace” in “Cyber Peace Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace”, edited by Scott J Schakelford et al, published in 2022 by Cambridge Univ Press, Pages 39-41

The concept of cyber peace brings a much-needed, innovative perspective to discussions of the governance of cyberspace. The ambiguity, conflicting terminology, and lack of transparency with respect to activities by state and nonstate actors have characterized efforts to conceptualize and analyze this new area of human endeavor at least since John Perry Barlow’s 1996 Declaration of the Independence of Cyberspace. Barlow’s (1996) proclamation that claimed cyberspace as a home for the “civilization of the Mind” and a “global social space” that must be kept free of governments, state sovereignty, and legal constructs – in effect, exempt from any type of governance – marked early on in the life of online activities the challenges and tensions that remain today for the global collective action problem of cyberspace governance. Thus, the distinctive perspective of cyber peace has the potential to set our analytical sights anew and to provide a framework for moving ahead with the normative projects connected to the aspects of cyberspace governance, including the ongoing elucidation of binding rules of international and domestic law that are applicable to cyberspace activities of state and nonstate actors.

Building on previous chapters that treat the concept of cyber peace in depth, the following definition focuses on four specific elements:

Cyber peace is […] not […] the absence of conflict […]. Rather it is the construction of a network of multilevel regimes that promote global, just and sustainable cybersecurity by clarifying the rules of the road for companies and countries alike to help reduce the threats of cyber conflict, crime and espionage to levels comparable to other business and national security risks. To achieve this goal, a new approach to cybersecurity is needed that seeks out best practices from the public and private sectors to build robust, secure systems and couches cybersecurity within the larger debate on internet governance (Shackelford, 2014, pp. xxv–xxvi).

The four elements emphasized in the above definition describe the fundamental connection between the goals of cyber peace and information sharing (IS), the subject of this chapter (Johnson et al., 2016, p. iii).1 Clarification of “rules of the road,” whether these are binding or voluntary; threat reduction, risk assessment, and best practices for carrying out these three tasks are precisely the substantive contribution that IS makes to the cybersecurity postures and strategies of stakeholders participating in any given IS platform. As detailed herein, such a platform optimally defines threshold norms of permissible and nonpermissible online behavior on the part of all actors, establishing the criteria for determining whether an individual, private organization, country, group of hackers, or even another autonomously acting computer has violated a rule (Deljoo et al., 2018, p. 1508). It also reduces vulnerability to cyber threats by lessening the informational asymmetries that characterize hostile cyber activities to the advantage of the attacker, and contributes to organizational risk assessment by integrating the information shared by other participants in the IS community into heightened “cyber situational awareness” for all sharers. Fourth, IS is readily framed and understood by a multiplicity of actors at the domestic level – private, governmental, and individual – as a best practice and, at the international level, as a confidence-building measure (CBM) for building trust among state and nonstate actors.2 These two characterizations of IS in the domestic and international jurisdictional arenas, respectively, are evidenced by the inclusion of IS modalities in many instances of national law and policy, as well as tens of multilateral and bilateral instruments for governing cyberspace at the international level (Housen-Couriel, 2017, pp. 46–84). Five examples of the latter are the 2015 Shanghai Cooperation Organization’s International Code of Conduct for Information Security, the UN GGE Report of July 2015, the OSCE’s Confidence-Building Measures for Cyberspace of 2016, the EU’s Network and Information Security Directive that entered into force in August 2016; and the 2018 Paris Call for Trust and Security in Cyberspace.

When IS implemented as a voluntary or recommended best practice or CBM in the context of these regulatory arrangements – rather than as a mandated regulatory requirement – it has the advantage of bypassing the legal challenges of achieving formal and substantive multistakeholder agreement on cyber norms. The difficulties of such normative barriers are often observed as characteristic of the contemporary cyber lay of the land. Either as a best practice (at the domestic level) or a CBM at the international level, IS has the advantage of bypassing the present challenges of achieving formal and substantive multistakeholder agreement on cyber norms that are inherent elements of national and multilateral legal regimes for the governance of cyberspace (Macak, 2016; Ruhl et al., 2020).

We propose in this chapter that, as IS platforms provide increasingly relevant, timely, and actionable data on vulnerabilities, including zero-day vulnerabilities (Ablon & Bogart, 2017); adversaries’ tactics, techniques, and procedures; malware tool configurations; and other tactical and strategic threat indicators, stakeholders will become more incentivized to increasingly trust IS platforms and to utilize them for both real-time response to hostile cyber activities and for building longterm cybersecurity strategies. Technological advances are easing this process, as platforms adopt new techniques for the automation of alerts and communications among sharers (Wagner et al., 2019). Thus, in instances when sharing communities are substantively and technologically optimized for cybersecurity, participants benefit from expertise and insights which may otherwise be unavailable to them with respect to developing threat vectors, mitigation of specific cyber risks, and real-time coordinated responses to hostile cyber events.

#### The US is key --- Our intelligence is critical and sharing it guarantees other countries model

Arts 18 --- Sophie Arts, master's degree in American studies with a concentration in U.S. foreign policy and political communication from Humboldt University in Berlin, “Offense as the New Defense: New Life for NATO’s Cyber Policy”, German Marshall Fund, 2018 | No. 039, https://www.gmfus.org/sites/default/files/Offense%2520-%2520Arts.pdf

Related to this challenge, NATO’s constraints on information sharing could hurt strategic decisionmaking processes and cyber operations. While most experts acknowledge that intelligence capabilities within NATO are significant, these remain isolated and well-guarded by national intelligence communities.31 More advanced information sharing, among allies and with other partners such as the EU, is critical for situational awareness and NATO’s preparedness. Yet, due mostly to a lack of trust between allies, this process is far from being at an optimal level.32

When it comes to intelligence sharing, some allies fear that infiltration and attacks against countries with lower resilience could potentially compromise information shared by other member states. Pushback against greater transparency is especially strong on the part of the United States, which owns a large share of NATO’s intelligence capabilities, making it a critical player in alliance intelligence operations from a tactical as well as strategic perspective.33 Due to the country’s outsized role in this field, NATO’s intelligence adaptation is largely dependent on U.S. inclinations to share capabilities and information with other allies.34 Although efforts to protect intelligence by minimizing sharing may be justified, elevating the role of the United States in NATO’s cyber policy without increasing transparency could potentially limit tactical effectiveness.

#### Information sharing and management are critical to NATO cyber resilience and attribution capabilities --- countries will follow-on the US model

Brown 19 --- Sarah Brown et al, Senior Scientist at the NATO Communications and Information (NCI) Agency where she works on cyber security capability development for NATO, with a particular interest in cyber threat intelligence, “Towards Mature Federated Cyber Incident Management and Information Sharing Capabilities in NATO and NATO Nations”, MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM), https://ieeexplore.ieee.org/document/9020814

For the past decade, cyber security teams around the world have recognized the growing importance of sharing cyber security information. Data regarding recently discovered vulnerabilities, cyber threats, and even cyber incident information has been recognized as vital for cyber security teams to stay resilient in the face of the ever-changing threat landscape.

Nations and the North Atlantic Treaty Organization (NATO) need to share information with each other and to work collaboratively in order to investigate potential cyber security incidents. Particularly in the course of joint missions, it is recognized as a key requirement to allow mission commanders to build situational awareness and to make more informed decisions in response to threats or vulnerabilities.

The Federated Mission Network (FMN) framework aims to enable the rapid deployment of mission networks by federating NATO, NATO Nations, and Mission Partner capabilities. Federated cyber information sharing and incident management are included as key cyber security requirements.

The focus of this paper is to discuss incident management and information sharing challenges, and to highlight the value added by the Cyber Information and Incident Coordination System (CIICS) system to support these capabilities.

SECTION II.Federated Cyber Incident Management

Cyber incident management (IM) can be defined as the ability to plan and control activities that ensure detected attacks and faults are addressed. Incidents need to be managed from start to finish to ensure that systems and services can be returned to a normal state, any undesired effects are addressed, and future reoccurrences are prevented. The results from these activities is a key information source for improving effectiveness and efficiency of cybersecurity.

Cyber information sharing (IS) refers to sharing of reference information about systems, networks, and interdependencies, as well as threat intelligence to include indicators of attacks as they progress, to support partners in their own defence activities.

In a federated mission context, establishing these capabilities supports collective defence, which is essential in support of mission objectives. However, in a federated design these capabilities require very high levels of interoperability to support quality interaction between participants. In a federated environment closely connected networks of teams operate as a decentralized, multi-team system.

It may be difficult to execute relatively simple tasks such as checking a range of systems for signs of an intrusion. While each federation participant organizes collaboration between its own team members, the success of the federated cyber IM function hinges on the interaction between component teams (across the different FMN participants) that make up the capability.

SECTION III.Federated Cyber IM Best Practices

Previous NCI Agency work [1] on best practices for achieving successful IM&IS in a multi-team system provided recommendations that apply across the Doctrine, Organization, Training, Material, Leadership, Personnel, Facility, and Interoperability (DOTMLPFI) spectrum.

Two key recommendations address roles and responsibilities and technical interoperability.

Defined roles and responsibilities, as well as communication channels, are required for the federated cyber IM&IS capability to achieve interoperability between teams. Ideally, all individuals with a role in the IM capability will have the details of all the other individuals, including contact information, role, and position in the overall hierarchy.

Technical interoperability is also an essential and inseparable element in capability development and system implementation for FMN. Cyber IM&IS systems operating in an FMN environment may need to transmit data to and receive data from a variety of other systems, units or forces of any service or Nation, and use the exchanged data to operate effectively together. Without it, it is not possible to work together effectively collaborating in a multi-vendor, multi-network, multi-service environment [5].

SECTION IV.Capability Development with Ciics

It is this shared challenge (and requirement), among Nations and within NATO, for federated cyber IM&IS, that formed the basis of development of the CIICS project in 2014.

The CIICS project was initiated by three (3) Nations: Canada, The Netherlands, and Romania, as part of the Multinational Cyber Defence Capability Development (MN CD2) smart defence program1, in which a group of Nations, supported by the NATO Communications and Information Agency (NCIA) pooled resources to develop solutions to common challenges.

CIICS is a tool to support cyber IM&IS, both within and beyond organizational boundaries.

CIICS is built around four (4) key functional requirements required in NATO and by the MN CD2 CIICS Nations.

A. Federated Design

CIICS is designed with a federated architecture to support multi-team collaboration, such as in an FMN scenario, as illustrated in Fig. 1. CIICS nodes are able to exchange data with other CIICS nodes by directly establishing a communication channel to each other (peer-to-peer mode). A dedicated public key infrastructure (PKI) allows strong certificate-based authentication between CIICS nodes. CIICS nodes manage the data and provide a web application to front-end to users.

B. Ability to Work Collaboratively on Cyber Securiy Incidents and to Share Key Cyber Information

From an information sharing perspective, Nations can directly feed threat intelligence, email alerts, and other relevant cyber defence information directly into their CIICS instance. This information will be stored in a knowledge base and is automatically replicated to all other Nation's CIICS nodes. The reference library is indexed with Elastic Search to enable efficient searching of large amounts of data.

From an IM perspective, CIICS contains a ticketing system designed specifically to track cyber defence incidents. Tickets can be handled locally on the CIICS node, or can be shared with one or more participants (e.g., in a federated mission environment), facilitating both local cyber incident handling, and joint coordination of incidents as necessary.

C. High Degree of Customization

CIICS is highly customizable. It support custom configuration of workflows, permissions, notifications, presentation language, structure and fields. Incident information is stored in an incident ticketing system component with many “facet” templates which can be added to support different incident types, as required. General knowledge (in human or machine readable formats)can be stored in a wiki-based knowledge repository, with configurable Communities of Interest with varying privacy / sharing levels.

D. Standards-Based Design

CIICS is standards-based, with the ability to import and export data in standard formats as well as enabling other systems to exchange data with CIICS nodes via its API.

SECTION V.The Incentive to Share

CIICS was designed with a number of target user groups in mind. These include National military Computer Emergency Response Teams (CERTs), other National defence organizations, the NATO Computer Incident Response Capability Technical Center (NCIRC TC), and FMN teams.

As with all organizations with a defence or security focus, the need to know tends to dominate. That is, information is limited to only those who are believed to have good business reasons to access the information. Sharing sensitive security outside of the organization is considered not worth the risk.

Usually, sharing will only start to happen when an organization is not able to solve an incident or needs extra information to be able to solve it. A tipping point it reached when the need to share exceeds the need to know. That is when incident sharing becomes clear and precise, and supplied and / or requested information will be handled and addressed properly.

This need to share will also occur when an infrastructure or application is shared, meaning there is a chance of being impacted by the same incident.

In most other circumstances common needs for incident information will be unclear, and requesting or supplying actionable information is really a challenge. This will either result in the sharing of massive amounts of incident information, since we are not sure what to share, so might as well share everything, or very risk-averse sharing of only very few pieces which we feel do not expose our own systems or vulnerabilities. As a result this shared information will be not directly actionable by the receiving party thus hard to address and filter.

So trust and sharing incident information only really becomes viable when there is a common goal that is collectively well understood and articulated.

SECTION VI.Federated Incident Management and Information Sharing in Action

Following its successful development and release, the CIICS sponsoring nations deployed a federation between themselves and the NCIRC TC which operates across the Internet at UNCLASSIFIED. A number of other nations have since joined this federation, and a community continues to grow. It has been interfaced to the open source Malware Information Sharing Platform (MISP) to draw in various pieces of structured cyber threat information which can then be linked to incidents within CIICS, and allows the users to explore overall links (for example, if certain indicators of compromise (IOCs) have been seen associated with multiple incidents, these incidents may infact also be linked).

As described above, however, in peacetime, and with the limitation of the classification, only very limited information sharing is viable through this system. The federation nations and NCIRC TC continue to work together to define the information sharing parameters for such a system.

In the meantime, the NATO Headquarters Consultation, Command and Control Staff (NHQC3S) recognize the overwhelming requirement for cyber information sharing platforms, and indeed the requirement for potentially more classified information sharing, as they are in the process of implementing a MISP for access by NATO Nations and partners via BICES. Similarly, they are working on the development of the precise information exchange requirements for such circumstances.

On the domestic level, the Netherlands and Romania have found great use in the CIICS system for cyber information sharing and incident handling between government departments.

In the Netherlands, a national UNCLASSIFIED CIICS federation allows the various military domains to share relevant (nationally sensitive) cyber incidents, as they recognize the commonality between their different network infrastructures, and the potential benefits from this collaboration. More sensitive incidents can be escalated up to, and be handled on, their highly classified CIICS federation, while they can transfer nonsensitive elements back to the international CIICS as deemed appropriate. More details are provided in Section VII.

Romania's National Cyberint Center (CNC) implemented a CIICS federation between 55 central government agencies, again recognizing that the institutions have a shared goal to identify and analyze cyber threats. An interface to the UNCLASSIFIED international CIICS system allows them to selectively share non-sensitive details, as described in more detail in Section VIII.

To further explore use cases on classified systems, the sponsoring nations also provided the CIICS system for trial in a number of NATO exercises, which are discussed in Section IX.

SECTION VII.NLD National Experience

In The Netherlands Ministry of Defence (NL MOD) each military branch as well as the Military police (Royal Netherlands Air Force (RNLAF), Royal Netherlands Navy (RNLN), Royal Netherlands Military Police (RNLMP), Royal Netherlands Army (RNLA)) has their own cyber security challenges within their own specific working area.

While the different forces use different hardware - tanks, airplanes, ships, armored cars - they do all use a shared communications infrastructure. Here there is a common interest and an implicit need to share incident information about that infrastructure as well as the technical details that can threaten it.

Within the NL MOD, multiple infrastructures are being used, which are not necessarily interconnected - for example, as a result of different classifications. But these are built upon the same building blocks, probably suffering from the same vulnerabilities.

While information that relates to a specific operational command may not need to be shared to other organizations, there will always be information that is important to share.

Being interconnected and being able to share incident information when needed is key here and CIICS is used to meet this requirement. Each operational command determines from its own authority whether to share or escalate an incident to the other organizations.

Furthermore, at the national level, NL MOD has identified multiple requirements for CIICS instances - at the “National Restricted” level, at the “National Secret” level, and also requirements to pass across the unclassified international federation, as well as potential classified (mission) federations. In trying to balance this plethora of business requirements, NL MOD has come up with an interesting solution, as illustrated in Fig. 2.

From this perspective all operational commands will run their own unclassified CIICS instances “National Restricted area” in Fig. 2), and these will be federated to one another.

To be able to handle and share classified incident information a federated national classified CIICS environment is also set up “National Secret area” in Fig. 2). This classified

CIICS system will be able to receive information from NATO partners and the unclassified CIICS system through data-diodes. This highly classified CIICS-system-high environment will contain the most relevant and complete actionable and historical incident information for each operational command and for the NL MOD CERT in an incident escalation role.

The NL MOD CERT's CIICS systems play an additional role in that they have additional interconnections with other CIICS federations (illustrated in Fig. 2 by the diodes), so that they can get or share incident information with other organizations, (e.g., governmental or peers). Sharing declassified incident information from the higher classifications downwards is done via air-gapped processes, following policies.

SECTION VIII.ROU National Experience

In Romania, following its designation as a national authority in the field of cyber intelligence, the Romanian Intelligence Service, through a specific unit, the National Cyberint Center (CNC), has endeavored to identify, prevent and counter the vulnerabilities, risks and threats to Romania's cyber security.

The team from Cyberint Center's objective is to collect, identify and understand cyber events from Cyber Infrastructures of National Interest (CII). Hence in2015, CNC implemented a project to build a National security system for the protection of Communications and Information Systems (CIS) critical infrastructures against cyber security threats. The project was implemented across 55 public infrastructures used by 55 institutions across Romania, bringing them together for a shared goal to identify and analyze cyber threats.

CIICS was implemented in a federated architecture, supporting joint incident handling, coordination and collaboration between the CNC organization and any of the 55 CIIs. When there is a common interest, CNC has the ability to share related aspects of cyber incidents with all organizations, helping them to have a proactive defence against specific threats.

The federated network between all the CIIs is a dedicated and isolated network between the 55 institutions and associated CIICS instances, together with a MISP instance, which is the main CNC tool used for sharing of indicators of compromise (see Fig. 3).

As with the Dutch, the Romanians have implemented a slightly bespoke CIICS deployment to best suit their national requirements. In this case, all instances are hosted and managed by the CNC, as a national authority for cyber defence. The federated system model allows the institutions to manage local incidents on their own system, and only share information that they believe might be of interest to other parties. The CNC acts as an escalation / central control hub to facilitate appropriate decision-making for sharing.

CIICS was also used during the last 3 editions of the main Romanian cyber defence exercise, CyDEx. The ability to conduct federated cyber defence information sharing as well as cyber incident artefacts, were the most appreciated aspects from the participating teams.

SECTION IX.Exercising Mission-Based Federated Incident Management and Information Sharing

The CIICS system has also been provided to NATO for use by National CERT teams during the Cyber Coalition (CC) Exercise (2014–2018), the Cyber Focus Area of the Cyber Warrior Interoperability eXercise (CWIX)(2014–2017), and NATO Response Force (NRF) in Steadfast Cobalt Exercise (2019). As described previously, a joint mission environment is the perfect scenario to necessitate joint cyber incident handling and information sharing.

Lessons learned during these exercises have been valuable to further refine what is needed by NATO and Nations across all DOTMLPFI aspects for federated incident management and federated information sharing.

Through use in Cyber Coalition exercises, users demonstrated a far richer appetite for joint IM&IS than is usually demonstrated during daily operations on fixed national networks. The tool proved a success in that teams progressed though the storylines faster than expected due to the rich collaboration. Lessons were learned in terms of the need for guidance on what information should, and should not, be shared [7].

At CWIX, the Cyber Focus Area is a test-bed by nations for new cyber capabilities. A federated network is formed, and proof of concepts are trialled, for example honeynets and honeytokens. A red team is then allowed to attack the federated blue teams, and they can exercise protecting themselves - and working together - for mutual defence. The red team attacks give the blue team participants good reason to share incident information, and the new capabilities help exercise the CIICS tool, to make sure it can support all types of cyber information sharing.

Steadfast Cobalt 2019 provided an opportunity to address a Cyber Defense (CD) IM&IS shortfall identified during the evaluation of the security domains NRF2020 and Joint Command and Control Capability (JC2C). NATO CIS Group (NCISG)Cyber Directorate, in coordination with NCI Agency Test Directorate, set up a feasibility test for existing CD IM&IS processes to determine if it meets operational network requirements.

These processes were complimented by a single CIICS instance, managed by NATO, deployed at the Mission Secret level, as a tool to facilitate the FMN teams in the absence of other tooling designed for this purpose. While this isn't the ideal implementation for CIICS - which would be for each mission network partner to have its own locally managed system, federated to the equivalent systems of the other partners such that information can be exchanged between them when required - this simple deployment enabled selective sharing via “visibility groups” and further helped the community to establish escalation processes, and to further determine agreements on when and what to share. Indeed, the requirement to have national ownership and privacy over a nationally-controlled, federated system, was highlighted by some partners, and this deterred them from using the system to handle nation-level incidents.

Fourteen (14) National deployed units from 10+ countries in Bucharest Romania along with several static entities (NCISG, JFC Brunssum, JFC Naples) tested their processes and ability to coordinate and work together on cyber security incidents that may affect a joint mission they are in together [3] [4].

The CD IM&IS process was assessed as capable for management and information sharing in future NRF-/FMN-networks and it was recommended that these requirements be endorsed as operational requirements for future NRF-rotations [6]

At a national and multinational level, cyber defence teams from NATO, NATO Nations, and Partners increasingly have a requirement to share cyber defence information and to coordinate on cyber incidents, particularly when they are engaged as coalition partners (e.g., the FMN Spiral 3 requirement for Nations to be able to conduct joint incident coordination and cyber security information sharing in a federated environment [2]).

SECTION X.Conclusion

Therefore, NATO and Nations must find ways to work seamlessly as a closely connected network of decentralized teams, as reflected in the FMN concept.

Collaborative work to date has made significant steps in establishing joint information sharing requirements, national and joint incident handling processes and procedures - and the definition of the interfaces between them, and requirements for the definition of escalation processes.

Three Nations, NLD, ROU, and CAN have developed a valuable tool in CIICS to support NATO and Nations in addressing requirements.

NATO and Nations must continue to invest in maturing existing capabilities (e.g., roles and responsibilities, what to share, workflows, interoperable tools and systems, training, etc.), to achieve mature federated incident coordination and information sharing capabilities.

NATO is also encouraged to use common funding to further the development of these capabilities, because of the federated aspect to the capability requirement.

#### Only increased information sharing can build resilience capabilities and reduce harms of attack

Skopik et al 16 --- Florian Skopik Senior Scientist of the research program “IT Security”., Giuseppe Settanni joined AIT in 2013 as scientist and is currently working on national and European applied research projects regarding security in communication and information systems, Roman Fiedler is Scientist at the AIT Austrian Insititute of Technology and runs projects in the areas of telehealth and ICT security, “A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing”, Computers & Security Volume 60, July 2016, Pages 154-176, <https://www.sciencedirect.com/science/article/pii/S0167404816300347>

International collaboration is of the utmost importance for effective response mechanisms. Indeed, digital boundaries are not clearly defined and do not correspond to national frontiers. Moreover, recent publications show that threats such as malware (and botnets, in particular) are no longer an issue that people should deal with individually, but are increasingly a social and civic responsibility that affects all sectors of the digital society (Anonymous, 2012, ENISA, 2013b).

According to Helmbrecht et al. (2013), response mechanisms, containing numerous established policy initiatives, have been in place from the early days of ICT development. However, the deployment of ICT solutions used by citizens in their day-to-day lives is threatened by cyber attacks, targeting areas such as online payment, e-government services, and in general every critical infrastructure relying on computer networks. Finally, ICT is increasingly used in vandalism, terrorism, hacktivism, war and fraud that reduce the level of confidence citizens have in trustfully adopting such technology and exposes them to higher and higher danger.

Securing ICT systems within a confederation of countries needs to be coherent across geographical borders and consistently pursued over time.

The European Network and Information Security Agency (ENISA) is the main European body aiming at improving the convergence of efforts from the different Member States by encouraging the exchange of information, methods and results, and avoiding duplication of work. To this end, one of ENISA's tasks is to support European institutions and Member States by facilitating a coordinated approach to respond to network and information security threats.

The NIST supports the coordination of existing Computer Security Incident Response Teams (CSIRTs), when responding to computer security incidents, by identifying technical standards, methodologies, procedures, and processes related to Computer Security Incident Coordination (CSIC). NIST provides guidance on how multiple CSIRTs should cooperate while handling computer security incidents, and how CSIRTs should establish synergies with other organizations within a broader information sharing community.

4.2. The threat landscape

The cyber threat landscape evolves rapidly. Innovative methods to achieve malicious objectives are constantly taking shape in cyber space. Cyber-criminals and certain nation-states are aggressively pursuing valuable data assets, such as financial transaction information, product design blueprints, user credentials to sensitive systems, and other intellectual property. Attackers are armed with the latest zero-day vulnerabilities, high-quality toolkits, and social engineering techniques to perpetrate advanced targeted attacks. These threats use several stages and vectors to duck traditional defenses and find vulnerable systems and sensitive data (FireEye, 2013).

Attacks have changed in form, function, and sophistication from just a few years ago. The new generation of threats utilize both mass-market malware designed to infect multiple systems as well as sophisticated, zero-day malware to infect targeted systems. They leverage multiple attack vectors cutting across Web, email, and application-based attacks. Today's attacks are aimed at getting valuable data assets, sensitive financial information, intellectual property, authentication credentials, insider information, and each attack is often a multi-staged effort to infiltrate networks, spread, and ultimately exfiltrate the valuable data (FireEye, 2013).

Modern cyber attackers are not only motivated by economic reasons, but also their actions are more and more driven by impulses of social and political nature. International groups of associated activists and hacktivists, such as Anonymous, are nowadays well known for attacks on government, religious and corporate websites (Olson, 2012). In April 2007, Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, following the country's spat with Russia over the removal of a war memorial. Some government online services were temporarily disrupted and online banking was halted. The attacks were more like cyber riots than crippling attacks and provoked outages lasting several hours or days (Herzog, 2011). In October 2010, Stuxnet, a complex piece of malware designed to interfere with Siemens Industrial Control Systems (ICS), was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear program (Farwell and Rohozinski, 2011). On November 24, 2014, data belonging to Sony Pictures Entertainment including personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of unreleased Sony films, and other information were released by hackers who called themselves the “Guardians of Peace” or “GOP” (State of California Department of Justice Office of the Attorney General, 2014). They demanded the cancellation of the planned release of the film The Interview, a comedy about a plot to assassinate North Korean leader.

In order to develop effective defense strategies, it is necessary to understand the cyber threats and the methodologies put in place to deploy them. The components of the evolving cyber threat landscape are becoming increasingly complex. A comprehensive analysis of the reported cyber incidents needs to be performed to characterize the multitude of aspects a cyber threat involves. Priority lists of cyber threats, threat agents, attack methods and threat trends are all elements that need to be taken into consideration. This information is useful for cyber security experts assessing risks to various systems and developing cyber security policies for defending valuable information. Nevertheless, care should always be taken when analyzing such data – the fact that an event has happened frequently in the past does not guarantee that it will continue to happen.

Given that the cyber threat landscape develops very dynamically, the main challenge is to capture the trends as early as possible (cf. ENISA report, Helmbrecht et al., 2013).

In 2014, for Drive-by-exploits there is a shift from botnets to malicious URLs as the preferred means to distribute malware, because URLs are a more difficult target for law enforcement take-downs. Regarding Code Injection, a notable issue is attacks against popular content management systems (CMSs). Due to their wide use, popular CMSs make up a considerable attack surface that has drawn the attention of cyber criminals. An interesting aspect is the increased use of peer-to-peer (P2P) botnets – more difficult to locate and take down. Also, the use of botnet infrastructures to mine the “virtual currency” bitcoins is an emerging trend.

After the 2013 Spamhaus attack (Arstechnica, 2013), Domain Name System (DNS) reflection attacks have gained popularity within the Denial of Service attacks. Further, there is an increase in rogueware/scareware reported. One reason for the growth is the expansion of ransomware and fake antivirus distribution to mobile platforms such as Android. Cyber espionage attacks reached a dimension that went far beyond expectations (ENISA, 2013c). Several mass surveillance campaigns run by nation states have been recently uncovered (see Clarke, 2011 and Hudson, 2014), generating the indignation of the population. Identity theft led to some of the most successful attacks by abusing SMS-forwarders to commit significant financial fraud. These attacks were based on known financial Trojans (e.g. Zeus, SpyEye, Citadel) that have been implemented on mobile platforms and attack two-factor authentication. Search Engine Poisoning has also moved to mobile devices. These developments led to the conclusion that attackers remain one step ahead; quite often it suffices to exploit simple and well known weaknesses to cause havoc.

Although information sharing might seem in contrast with the attitude of some nation states performing espionage on other countries, this should not void information sharing efforts among organizations (especially those with similar infrastructures, and thus suffering from similar vulnerabilities or being potentially similarly attractive to attackers) from these countries on another layer. The key message of ENISA is to transfer knowledge from the cyber security community to the user groups for the purpose of strengthening cyber defense. To this end, effective information sharing, not only between security professionals, but also between all stakeholders dealing with critical ICT systems, needs to be enabled.

## Aff Extensions / A2s --- Resilience

### Ext --- Info Sharing Insufficient Now

#### Information sharing is insufficient now

Faesen 22 --- Louk Faesen et al, Senior Strategic Analyst at the Cyber Policy and Resilience Program of the Hague Centre for Strategic Studies, “The Promises and Perils of a Minimum Cyber Deterrence Posture Considerations for Small and Middle Powers”, April 2022, https://hcss.nl/wp-content/uploads/2022/04/Promises-and-Perils-of-Minumum-Cyber-Deterrence-Posture-HCSS-2022.pdf

At an international level, the challenges are compounded even when the interdependence of cyberspace and a commonality of threats and interests makes the imperative to cooperate highly salient. The transatlantic alliance, broadly construed, has oftentimes struggled to arrive at a consensus around what constitutes acceptable behavior and appropriate responses in cyberspace. More directly pertinent from a deterrence perspective, there are operational limitations to meaningful cooperation between allies about intelligence-sharing around cyber threats and coordinating responses to malicious cyber behavior. The nexus between cyber and intelligence operations, and the deep ties between the cyber and signals intelligence worlds, creates significant impediments to sharing intelligence even among close allies that would enable timely and effective attribution, defense, and other responses. For offensive cyber operations in particular, the challenge is most delicate. Allies vary in terms of the level of maturity of offensive cyber programs (if at all); perspectives on the application of sovereignty to cyberspace and, by extension, how other states should approach maneuvering in others’ networks; and potential sources of mistrust about allies’ cyber activities. The latter is evident in debates about how new US cyber concepts, such as persistent engagement and defend forward, which were debuted in Cyber Command’s 2018 Command Vision and the 2018 Department of Defense Cyber Strategy, might affect US allies.181 Issues about the extent to which US cyber forces may be maneuvering in allied owned and operated networks, doctrinally defined as “gray space” by the US military, and appropriate mechanisms and timelines for notification about these operations, remain unresolved.182

### A2: Resilience Now

#### Cyberattacks inevitable and evolving --- resilience through information sharing is the only way to ensure sustained resilience prevents escalation

Conklin & Shoemaker 17 --- William Arthur Conklin, Associate Professor and Director of the Center for Information Security Research and Education in the College of Technology at the University of Houston, & Dan Shoemaker, Professor and Director of the Masters of Science in Cyber Security Program at the Center for Cyber Security and Intelligence Studies, a NSA Center of Academic Excellence, at the University of Detroit (313) Mercy, “Cyber-Resilience: Seven Steps for Institutional Survival”, EDPACS The EDP Audit, Control, and Security Newsletter Volume 55, 2017 - Issue 2, https://www.tandfonline.com/doi/full/10.1080/07366981.2017.1289026?casa\_token=YkLN2jNKIq4AAAAA%3AcCFCFoQdc7m6VLRsQUiXbuJ1GOnstIh5Tv2fiuAZwIDgWL4DCMehSsX\_FX8t0z-nxVXENYjLorw

The point of this article is that the enterprise will never be 100% secure. There are simply too many threats to ensure that. Consequently, organizations should stop viewing security in access control enforcement terms and start treating it as a comprehensive, fully integrated, strategic management responsibility that is rooted in enterprise architecture. Thus, organizations need to approach the problem as a preparation, detection, response, and recovery challenge instead of viewing security in terms of classic walls and access control. That will require a change in culture to accomplish.

Cyber-resilience recognizes that people are the weakest link. It acknowledges that workers will make mistakes, and that intruders using advanced hacking tools will find cracks in even the most robust cybersecurity system (Lois, 2015). Accordingly, cyber-resilience needs to be integrated into the “bones” of the organization. That requires the organization to create a well-defined architecture and implement explicit control over the interdependencies among processes, including those that apply to every electronic, human and physical asset in the enterprise’s infrastructure.

Cyber-resilience is not a defensive stance, which is focused on detecting network intrusions, or fixing malware. Instead, the resilience concept enables practical survival in the face of attack. Nevertheless, effective implementation of a cyber-resilient enterprise requires strategic vision. It also requires day-to-day engagement across the enterprise. This is rooted in the specialized actions and collaborations with the classic cybersecurity function, which implies an effective amalgamation of cybersecurity and cyber-resilience strategies. Although the role of the latter focuses more on identification, authentication, authorization, and enforcement, a cyber-resilient mindset is also essential when cyber-defenses fail.

Fundamentally, the organization needs to survive. The increased presence of advanced cyberthreats makes it inevitable that a targeted organization will ultimately be compromised. Therefore, every organization’s critical systems must be assured safe under any realistic set of conditions. Lost data or ancillary functionality can be restored afterward. But the basic things that the organization needs to endure must be maintained safe. Cyber-resilient organizations are able to “tough-out” cyber-attacks and continue to accomplish their critical mission and satisfy their business goals, Redesigning or updating systems for resilience will make attacks less likely to succeed; minimize the consequences when they do succeed; increase cost and uncertainty for the adversary; and possibly act as a deterrent against future attacks. Consequently, investment in building cyber-resilience is investment in organizational survival.

### Ext- Sharing Solves Resilience

#### Resilience solves impacts

Abraham & Daultrey 20 --- Chon Abraham Associate Professor of Management Information Systems William & Mary Sally Daultrey Chief Intelligence Analyst Adenium Group, “Considerations for NATO in Reconciling Challenges to Shared Cyber Threat Intelligence: A study of Japan, the US and the UK”, in “Cyber Threats and NATO 2030: Horizon Scanning and Analysis”, Dec 2020, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE (CCDOE), https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030\_Horizon-Scanning-and-Analysis.pdf

Cyber threats are fundamentally changing the nature of warfare and the digital economy with implications for international collaboration and security cooperation (NATO, 2019). Governments and the leadership of multinational companies must understand threat vectors and threat actors to activate their collective response, both in peacetime and during targeted cyber operations. Efforts for developing approaches to exchange information on security incidents, known as Cyber Threat Intelligence (CTI) sharing, is an international imperative (Menges et al., 2019) and governments can no longer rely on voluntary compliance across business ecosystems and supply chains to operationalise international cyber defence. Cyber operations are increasingly understood as linked to strategic campaigns, particularly when initiated by adversarial countries seeking to shift the relative balance of power amongst targeted countries with rippling global effects (Harknett and Smeets, 2020; NATO CCDCOE, 2017). CTI sharing is therefore essential for all directly and indirectly targeted societies and countries to build a collective understanding of these cyber operations and strategic campaigns in terms of: (1) their true nature; (2) the global reach of effects; (3) the duration; and (4) the extent of data exfiltration and aggregation compromising national security. The sophistication and proliferation of cyber threats are outpacing the capacities of countries to respond using conventional decision structures, to be replaced by dynamic bilateral and regional collaboration architectures. CTI sharing is vital to protecting the global business ecosystem and shared security interests, yet not all nations have comparable capabilities to effectively share and act on threat information.

### Ext --- Grid Attack Impacts --- Blackouts

**Blackouts threaten critical supply chains --- triggers multiple existential scenarios**

**Pry 21** --- Dr. Peter Vincent Pry is executive director of the Task Force on National and Homeland Security, “When will America protect itself against EMP, cyber and ransomware attacks?”, The Hill, 05/21/21, https://thehill.com/opinion/national-security/554503-when-will-america-protect-itself-against-emp-cyber-and-ransomware

“A long-term outage owing to EMP could **disable most critical supply chains**, leaving the U.S. population living in conditions similar to centuries past, prior to the advent of electric power. In the 1800s, the U.S. population was less than 60 million, and those people had many skills and assets necessary for survival without today’s infrastructure. An extended blackout today could result in the death of a **large fraction of the American people** through the effects of **societal collapse, disease and starvation**. While national planning and preparation for such events could help mitigate the damage, few such actions are currently under way or even being contemplated.” — Congressional EMP Commission (2017)

The people of Rangely, Colo., are not waiting for Washington to protect them from a Great American Blackout caused by a solar superstorm or cyber warfare or electromagnetic pulse (EMP) attack. Like several other Western municipalities, Rangely, a town of 2,300 in northwest Colorado, home to a community college, has rolled up its sleeves and, in the best traditions of Western pioneering spirit, independence and self-sufficiency, is building redundant microgrids so they can survive anything.

Texas state Sen. Bob Hall and his colleagues aren’t waiting for Washington to “provide for the common defense,” either. Hall’s bill to protect the Texas electric grid from all hazards — including EMP, cyber warfare and sabotage — recently passed the state Senate.

Texans had a small taste of “electronic apocalypse” in February when an ice storm caused statewide rolling blackouts, resulting in property damage totaling billions of dollars, fuel shortages including a reduction in the national fuel supply, industrial accidents, including a major explosion and fire in a chemical plant, and 100 deaths. Experts have cautioned the same could happen during hot, summer weather.

Sen. Hall, a former Air Force officer and an EMP expert, has been warning Texas for years that electric grid vulnerability to EMP and cyber attack could have catastrophic consequences. The Electric Reliability Council Of Texas (ERCOT), which manages the state’s electricity infrastructure, proved in February **that they and the utilities are not even prepared to cope with a severe ice storm,** let alone existential threats from EMP and cyber warfare.

#### Blackouts cause extinction

Morris 17 --- Craig Morris, co-author of Energy Democracy, the first history of Germany’s Energiewende, “After two weeks without power, civilization collapses”, Energy Transition, Oct 2nd 2017, https://energytransition.org/2017/10/after-two-weeks-without-power-civilization-collapses/

Elsberg started work on the book in 2008. Just before he finished, Germany’s Office of Technology Assessment (TAB) published its own scientific study on what an extended blackout would look like (PDF in German). Entitled “The vulnerability of modern societies: a case study of a large-scale blackout,” the study revealed lots of scary things.

For instance, people would not only be without drinking water, but the piping itself would become “irreparably” contaminated within weeks. Chaos would quickly break out because all forms of communication – cell phones, radio, television, internet, etc. – would stop working, and people would lack power for batteries in their devices anyway (how many of you have a hand-crank flashlight or radio?). Those with backup generators would run out of fuel because the authorities would confiscate the available supply (fuel pumps require power) for emergency services.

Elsberg took account of some findings from the study in his novel, but he says he basically already had the situation described well. For the first few days, people deal with the inconvenience well. Everyone has a little food and water at home, and grocery stores contain a few days of supplies as well. But without power, you can’t withdraw money from the bank. There is a run on the stores, and prices quickly stretch out of control. Things not needed for survival become worthless, while food and water become unaffordable.

After the first few days, people begin to starve. The strong start to force their will on others; the rule of law collapses. Those with guns use them (Germans have lots of guns). Citizens ~~are reduced to barbarians~~ as they fight to survive.

**Loss of critical infrastructure causes extinction**

**Friedemann 16** (Alice Friedemann, transportation expert, founder of EnergySkeptic.com and author of “When Trucks Stop Running, Energy and the Future of Transportation,” worked at American Presidential Lines for 22 years, where she developed computer systems to coordinate the transit of cargo between ships, rail, trucks, and consumers, citing Dr. Peter Vincent Pry. Pry is executive director of the Task Force on National and Homeland Security, a Congressional advisory board dedicated to achieving protection of the United States from electromagnetic pulse and other threats. Dr. Pry is also the director of the United States Nuclear Strategy Forum, an advisory body to Congress on policies to counter weapons of mass destruction. Dr. Pry has served on the staffs of the Congressional Commission on the Strategic Posture of the United States, the Commission to Assess the Threat to the U.S. from an EMP Attack, the House Armed Services Committee, as an intelligence officer with the CIA, and as a verification analyst at the U.S. Arms Control and Disarmament Agency. 1-24-16, accessed 1/1/19 “Electromagnetic pulse threat to infrastructure (U.S. House hearings)” <http://energyskeptic.com/2016/the-scariest-u-s-house-session-ever-electromagnetic-pulse-and-the-fall-of-civilization/>)

Modern civilization **cannot exist** for a protracted period without electricity. Within days of a blackout across the U.S., a blackout that could **encompass the entire planet**, emergency generators would run out of fuel, **telecom**munications would cease as would transportation due to **gridlock**, and eventually **no fuel**. Cities would have no running **water** and soon, within a few days, exhaust their **food** supplies. Police, Fire, Emergency Services and **hospitals cannot** long **operate in a blackout**. **Government and Industry** also need electricity in order to operate. The EMP Commission warns that a natural or nuclear EMP event, given current **unpreparedness**, would likely result in **societal collapse**. Terrorists, criminals, and even lone individuals can build a non-nuclear EMP weapon without great trouble or expense, working from Unclassified designs publicly available on the internet, and using parts available at any electronics store. In 2000, the Terrorism Panel of the House Armed Services Committee sponsored an experiment, recruiting a small team of amateur electronics enthusiasts to attempt constructing a radiofrequency weapon, relying only on unclassified design information and parts purchased from Radio Shack. The team, in 1 year, built two radiofrequency weapons of radically different designs. One was designed to fit inside the shipping crate for a Xerox machine, so it could be delivered to the Pentagon mail room where (in those more unguarded days before 9/11) it could slowly fry the Pentagon’s computers. The other radiofrequency weapon was designed to fit inside a small Volkswagon bus, so it could be driven down Wall Street and disrupt computers— and perhaps the National economy. Both designs were demonstrated and tested successfully during a special Congressional hearing for this purpose at the U.S. Army’s Aberdeen Proving Ground. Radiofrequency weapons are not merely a hypothetical threat. Terrorists, criminals, and disgruntled individuals have used home-made radiofrequency weapons. The U.S. military and foreign militaries have a wide variety of such weaponry. Moreover, non-nuclear EMP devices that could be used as radiofrequency weapons are publicly marketed for sale to anyone, usually advertised as ‘‘EMP simulators.’’ For example, one such simulator is advertised for public sale as an ‘‘EMP Suitcase.’’ This EMP simulator is designed to look like a suitcase, can be carried and operated by one person, and is purpose-built with a high energy radiofrequency output to destroy electronics. However, it has only a short radius of effect. Nonetheless, a terrorist or deranged individual who knows what he is doing, who has studied the electric grid for a major metropolitan area, could—armed with the ‘‘EMP Suitcase’’— black out a major city. A CLEAR AND PRESENT DANGER. An EMP weapon can be used by state actors who wish to level the battlefield by neutralizing the great technological advantage enjoyed by U.S. military forces. EMP is also the ideal means, the only means, whereby rogue states or terrorists could use a single nuclear weapon to destroy the United States and prevail in the War on Terrorism or some other conflict with a single blow. The EMP Commission also warned that states or terrorists could exploit U.S. vulnerability to EMP attack for coercion or blackmail: ‘‘Therefore, terrorists or state actors that possess relatively unsophisticated missiles armed with nuclear weapons may well calculate that, instead of destroying a city or military base, they may obtain the greatest political-military utility from one or a few such weapons by using them—or threatening their use—in an EMP attack.’’ The EMP Commission found that states such as Russia, China, North Korea, and Iran have incorporated EMP attack into their military doctrines, and openly describe making EMP attacks against the United States. Indeed, the EMP Commission was established by Congress partly in response to a Russian nuclear EMP threat made to an official Congressional Delegation on May 2, 1999, in the midst of the Balkans crisis. Vladimir Lukin, head of the Russian delegation and a former Ambassador to the United States, warned: ‘‘Hypothetically, if Russia really wanted to hurt the United States in retaliation for NATO’s bombing of Yugoslavia, Russia could fire an SLBM and detonate a single nuclear warhead at high altitude over the United States. The resulting EMP would massively disrupt U.S. communications and computer systems, shutting down everything.’’ China’s military doctrine also openly describes EMP attack as the ultimate asymmetric weapon, as it strikes at the very technology that is the basis of U.S. power. Where EMP is concerned, ‘‘The United States is more vulnerable to attacks than any other country in the world’’: ‘‘Some people might think that things similar to the ‘Pearl Harbor Incident’ are unlikely to take place during the information age. Yet it could be regarded as the ‘Pearl Harbor Incident’ of the 21st Century if a surprise attack is conducted against the enemy’s crucial information systems of command, control, and communications by such means as… electromagnetic pulse weapons… Even a superpower like the United States, which possesses nuclear missiles and powerful armed forces, cannot guarantee its immunity…In their own words, a highly computerized open society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems and from power plants to iron and steel works, relies entirely on computer networks… When a country grows increasingly powerful economically and technologically…it will become increasingly dependent on modern information systems… The United States is more vulnerable to attacks than any other country in the world.’’ Iran—the world’s leading sponsor of international terrorism—in military writings openly describes EMP as a terrorist weapon, and as the ultimate weapon for prevailing over the West: ‘‘If the world’s industrial countries fail to devise effective ways to defend themselves against dangerous electronic assaults, then they will disintegrate within a few years… American soldiers would not be able to find food to eat nor would they be able to fire a single shot.’’ The threats are not merely words. The EMP Commission assesses that Russia has, as it openly declares in military writings, probably developed what Russia describes as a ‘‘Super-EMP’’ nuclear weapon—specifically designed to generate extraordinarily high EMP fields in order to paralyze even the best protected U.S. strategic and military forces. China probably also has Super-EMP weapons. North Korea too may possess or be developing a Super-EMP nuclear weapon, as alleged by credible Russian sources to the EMP Commission, and by open-source reporting from South Korean military intelligence. But any nuclear weapon, even a low-yield first generation device, could suffice to make a catastrophic EMP attack on the United States. Iran, although it is assessed as not yet having the bomb, is actively testing missile delivery systems and has practiced launches of its best missile, the Shahab–III, fuzing for high- altitude detonations, in exercises that look suspiciously like training for making EMP attacks. As noted earlier, Iran has also practiced launching from a ship a Scud, the world’s most common missile—possessed by over 60 nations, terrorist groups, and private collectors. A Scud might be the ideal choice for a ship-launched EMP attack against the United States intended to be executed anonymously, to escape any last-gasp U.S. retaliation. Unlike a nuclear weapon detonated in a city, a high-altitude EMP attack leaves no bomb debris for forensic analysis, no perpetrator ‘‘fingerprints.’’ Under present levels of preparedness, communications would be severely limited, restricted mainly to those few military communications networks that are hardened against EMP. Today’s microelectronics are the foundation of our modern civilization, but are over 1 million times more vulnerable to EMP than the far more primitive and robust electronics of the 1960s, that proved vulnerable during nuclear EMP tests of that era. Tests conducted by the EMP Commission confirmed empirically the theory that, as modern microelectronics become ever smaller and more efficient, and operate ever faster on lower voltages, they also become ever more vulnerable, and can be destroyed or disrupted by much lower EMP field strengths. Microelectronics and electronic systems are everywhere, and run virtually everything in the modern world. All of the civilian critical infrastructures that sustain the economy of the United States, and the lives of 310 million Americans, depend, directly or indirectly, upon electricity and electronic systems. Of special concern is the vulnerability to EMP of the Extra-High-Voltage (EHV) transformers, that are indispensable to the operation of the electric grid. EHV transformers drive electric current over long distances, from the point of generation to consumers (from the Niagara Falls hydroelectric facility to New York City, for example). The electric grid cannot operate without EHV transformers—which could be destroyed by an EMP event. The United States no longer manufactures EHV transformers. They must be manufactured and imported from overseas, from Germany or South Korea, the only two nations in the world that manufacture such transformers for export. Each EHV transformer must be custom-made for its unique role in the grid. A single EHV transformer typically requires 18 months to manufacture. The loss of large numbers of EHV transformers to an EMP event would plunge the United States into a protracted blackout lasting years, with perhaps no hope of eventual recovery, as the society and population probably could not survive for even 1 year without electricity. Another key vulnerability to EMP are Supervisory Control And Data Acquisition systems (SCADAs). SCADAs essentially are small computers, numbering in the millions and ubiquitous everywhere in the critical infrastructures, that perform jobs previously performed by hundreds of thousands of human technicians during the 1960s and before, in the era prior to the microelectronics revolution. SCADAs do things like regulating the flow of electricity into a transformer, controlling the flow of gas through a pipeline, or running traffic control lights. SCADAs enable a few dozen people to run the critical infrastructures for an entire city, whereas previously hundreds or even thousands of technicians were necessary. Unfortunately, SCADAs are especially vulnerable to EMP. EHV transformers and SCADAs are the most important vulnerabilities to EMP, but are by no means the only vulnerabilities. Each of the critical infrastructures has their own unique vulnerabilities to EMP: The National electric grid, with its transformers and generators and electronic controls and thousands of miles of power lines, is a vast electronic machine—more vulnerable to EMP than any other critical infrastructure. Yet the electric grid is the **most important of all critical infrastructures**, and is in fact the **keystone supporting modern civilization**, as it powers **all the other critical infrastructures**. As of now it is our **technological Achilles Heel**. The EMP Commission found that, if the electric grid collapses, so too will collapse **all the other critical infrastructures**. But, if the electric grid can be protected and recovered, so too all the other critical infrastructures can also be restored. **Transportation** is a critical infrastructure because modern civilization cannot exist without the goods and services moved by road, rail, ship, and air. Cars, trucks, locomotives, ships, and aircraft all have electronic components, motors, and controls that are potentially vulnerable to EMP. Gas stations, fuel pipelines, and refineries that make petroleum products depend upon electronic components and cannot operate without electricity. Given our current state of unpreparedness, in the aftermath of a natural or nuclear EMP event, transportation systems would be paralyzed. **Traffic control systems** that avert traffic jams and collisions for road, rail, and air depend upon electronic systems, that the EMP Commission discovered are especially vulnerable to EMP. **Communications** is a critical infrastructure because modern economies and the cohesion and operation of modern societies depend to a degree unprecedented in history on the rapid movement of information—accomplished today mostly by electronic means. Telephones, cell phones, personal computers, television, and radio are all directly vulnerable to EMP, and cannot operate without electricity. Satellites that operate at Low-Earth-Orbit (LEO) for communications, weather, scientific, and military purposes are vulnerable to EMP and to collateral effects from an EMP attack. Within weeks of an EMP event, the LEO satellites, which comprise most satellites, would probably be inoperable. **Banking and finance** are the critical infrastructure that sustain modern economies. Whether it is the stock market, the financial records of a multinational corporation, or the ATM card of an individual—financial transactions and record keeping all depend now at the macro- and micro-level upon computers and electronic automated systems. Many of these are directly vulnerable to EMP, and none can operate without electricity. The EMP Commission found that an EMP event could transform the modern electronic economy into a **feudal economy based on barter**. **Food** has always been **vital to** every person and **every civilization**. The critical infrastructure for producing, delivering, and storing food depends upon a **complex web of technology**, including machines for planting and harvesting and packaging, refrigerated vehicles for long-haul transportation, and temperature-controlled warehouses. Modern technology enables over **98 percent of the U.S. National population** to be fed by less than 2 percent of the population. Huge regional warehouses that resupply supermarkets constitute the National food reserves, enough food to feed the Nation for 30–60 days at normal consumption rates, the warehoused food preserved by refrigeration and temperature control systems that typically have enough emergency electrical power (diesel or gas generators) to last only about an average of 3 days. Experience with storm-induced blackouts proves that when these big regional food warehouses lose electrical power, **most of the food supply will rapidly spoil**. Farmers, less than 2 percent of the population as noted above, **cannot feed 310 million Americans** if deprived of the means that currently makes possible this technological miracle. Water too has always been a basic necessity to every person and civilization, even more crucial than food. The critical infrastructure for purifying and delivering potable water, and for disposing of and treating waste water, is a vast networked machine powered by electricity that uses electrical pumps, screens, filters, paddles, and sprayers to purify and deliver drinkable water, and to remove and treat waste water. Much of the machinery in the water infrastructure is directly vulnerable to EMP. The system cannot operate without vast amounts of electricity supplied by the power grid. A natural or nuclear EMP event would immediately deprive most of the U.S. National population of running water. Many natural sources of water—lakes, streams, and rivers—would be dangerously polluted by toxic wastes from sewage, industry, and hospitals that would backflow from or bypass wastewater treatment plants, that could no longer intake and treat pollutants without electric power. Many natural water sources that would normally be safe to drink, after an EMP event, would be polluted with human wastes including feces, industrial wastes including arsenic and heavy metals, and hospital wastes including pathogens. Emergency services such as police, fire, and hospitals are the critical infrastructure that upholds the most basic functions of government and society—preserving law and order, protecting property and life. Experience from protracted storm-induced blackouts has shown, for example in the aftermath of Hurricanes Andrew and Katrina, that when the lights go out and communications systems fail and there is no gas for squad cars, fire trucks, and ambulances, the worst elements of society and the worst human instincts **rapidly takeover**. The EMP Commission found that, given our current state of unpreparedness, a natural or nuclear EMP event could create **anarchic conditions** that would **profoundly challenge the existence of social order**.

**Blackouts go nuclear.**

Richard **Andres and** Hanna **Breetz, 2011**. Professor of National Security Strategy at the National War College and a Senior Fellow and Energy and Environmental Security and Policy Chair in the Center for Strategic Research, Institute for National Strategic Studies, at the National Defense University, doctoral candidate in the Department of Political Science at The Massachusetts Institute of Technology. “Small Nuclear Reactors for Military Installations: Capabilities, Costs, and Technological Implications”, [www.ndu.edu/press/lib/pdf/StrForum/SF-262.pdf](http://www.ndu.edu/press/lib/pdf/StrForum/SF-262.pdf)

The DOD interest in small reactors derives largely from problems with base and logistics vulnerability. Over the last few years, the Services have begun to reexamine virtually every aspect of how they generate and use energy with an eye toward cutting costs, decreasing carbon emissions, and reducing energy-related vulnerabilities. These actions have resulted in programs that have significantly reduced DOD energy consumption and greenhouse gas emissions at domestic bases. Despite strong efforts, however, two critical security issues have thus far proven resistant to existing solutions: bases’ vulnerability to civilian power outages, and the need to transport large quantities of fuel via convoys through hostile territory to forward locations. Each of these is explored below. Grid Vulnerability. DOD is unable to provide its bases with electricity when the civilian electrical grid is offline for an extended period of time. Currently, domestic military installations receive 99 percent of their electricity from the civilian power grid. As explained in a recent study from the Defense Science Board: DOD’s key problem with electricity is that critical missions, such as national strategic awareness and national command authorities, are almost entirely dependent on the national transmission grid . . . [which] is fragile, vulnerable, near its capacity limit, and outside of DOD control. In most cases, neither the grid nor on-base backup power provides sufficient reliability to ensure continuity of critical national priority functions and oversight of strategic missions in the face of a long term (several months) outage.7 The grid’s fragility was demonstrated during the 2003 Northeast blackout in which 50 million people in the United States and Canada lost power, some for up to a week, when one Ohio utility failed to properly trim trees. The blackout created cascading disruptions in sewage systems, gas station pumping, cellular communications, border check systems, and so forth, and demonstrated the interdependence of modern infrastructural systems.8 More recently, awareness has been growing that the grid is also vulnerable to purposive attacks. A report sponsored by the Department of Homeland Security suggests that a coordinated cyberattack on the grid could result in a third of the country losing power for a period of weeks or months.9 Cyberattacks on critical infrastructure are not well understood. It is not clear, for instance, whether existing terrorist groups might be able to develop the capability to conduct this type of attack. It is likely, however, that some nation-states either have or are working on developing the ability to take down the U.S. grid. In the event of a war with one of these states, it is possible, if not likely, that parts of the civilian grid would cease to function, taking with them military bases located in affected regions. Government and private organizations are currently working to secure the grid against attacks; however, it is not clear that they will be successful. Most military bases currently have backup power that allows them to function for a period of hours or, at most, a few days on their own. If power were not restored after this amount of time, the results could be disastrous. First, military assets taken offline by the crisis would not be available to help with disaster relief. Second, during an extended blackout, global military operations could be seriously compromised; this disruption would be particularly serious if the blackout was induced during major combat operations. During the Cold War, this type of event was far less likely because the United States and Soviet Union shared the common understanding that blinding an opponent with a grid blackout could escalate to nuclear war. America’s current opponents, however, may not share this fear or be deterred by this possibility. In 2008, the Defense Science Board stressed that DOD should mitigate the electrical grid’s vulnerabilities by turning military installations into “islands” of energy self-sufficiency. The department has made efforts to do so by promoting efficiency programs that lower power consumption on bases and by constructing renewable power generation facilities on selected bases. Unfortunately, these programs will not come close to reaching the goal of islanding the vast majority of bases. Even with massive investment in efficiency and renewables, most bases would not be able to function for more than a few days after the civilian grid went offline Unlike other alternative sources of energy, small reactors have the potential to solve DOD’s vulnerability to grid outages. Most bases have relatively light power demands when compared to civilian towns or cities. Small reactors could easily support bases’ power demands separate from the civilian grid during crises. In some cases, the reactors could be designed to produce enough power not only to supply the base, but also to provide critical services in surrounding towns during long-term outages. Strategically, islanding bases with small reactors has another benefit. One of the main reasons an enemy might be willing to risk reprisals by taking down the U.S. grid during a period of military hostilities would be to affect ongoing military operations. Without the lifeline of intelligence, communication, and logistics provided by U.S. domestic bases, American military operations would be compromised in almost any conceivable contingency. Making bases more resilient to civilian power outages would reduce the incentive for an opponent to attack the grid. An opponent might still attempt to take down the grid for the sake of disrupting civilian systems, but the powerful incentive to do so in order to win an ongoing battle or war would be greatly reduced.

### Ext --- Grid Collapse Causes Nuclear Meltdowns

#### Grid collapse makes all conflict inevitable and causes nuclear meltdowns

Ahmed 19 --- Nafeez Ahmed, Vice, “U.S. Military Could Collapse Within 20 Years Due to Climate Change, Report Commissioned By Pentagon Says”, Oct 24th 2019, https://www.vice.com/en/article/mbmkz8/us-military-could-collapse-within-20-years-due-to-climate-change-report-commissioned-by-pentagon-says

The US Army report shows that California’s power outage could be a taste of things to come, laying out a truly dystopian scenario of what would happen if the national power grid was brought down by climate change. One particularly harrowing paragraph lists off the consequences bluntly:

“If the power grid infrastructure were to collapse, the United States would experience significant:

Loss of perishable foods and medications

Loss of water and wastewater distribution systems

Loss of heating/air conditioning and electrical lighting systems

Loss of computer, telephone, and communications systems (including airline flights, satellite networks and GPS services)

Loss of public transportation systems

Loss of fuel distribution systems and fuel pipelines

Loss of all electrical systems that do not have back-up power”

Although the report does not dwell on the implications, it acknowledges that a national power grid failure would lead to a perfect storm requiring emergency military responses that might eventually weaken the ability of the US Army to continue functioning at all: “Relief efforts aggravated by seasonal climatological effects would potentially accelerate the criticality of the developing situation. The cascading effects of power loss… would rapidly challenge the military’s ability to continue operations.”

Also at “high risk of temporary or permanent closure due to climate threats” are US nuclear power facilities.

There are currently 99 nuclear reactors operating in the US, supplying nearly 20 percent of the country’s utility-scale energy. But the majority of these, some 60 percent, are located in vulnerable regions which face “major risks” including sea level rise, severe storms, and water shortages.

**Extinction**

**Goldes 11** – MA @ Brandeis and San Francisco State

Mark Goldes Former Research Fellow at Brandeis University is Founder of the Aesop Institute. Formerly Senior Director of the Berlin Corridor control radar in Germanyfor US Air Force SOLAR MEGASTORMS can GENERATE a GLOBAL NUCLEAR NIGHTMARE <http://www.opednews.com/articles/SOLAR-MEGASTORMS-can-GENER-by-Mark-Goldes-111119-448.html>

We face a severe potential emergency. External threats serve to unite. The world faces an unrecognized nuclear peril! Uniting to confront it can generate the missing popular and government support to generate millions of jobs and revitalize the global economy.

A THREAT GREATER THAN ANY TERROR ATTACK!

A NASA funded study by the National Academy of Sciences was titled Severe Space Weather Events--Understanding Societal and Economic Impacts. The resulting Report detailed what might happen in the event of a solar megastorm launching a powerful Coronal Mass Ejection (CME) that strikes our geomagnetic field. The study predicts blackouts that may last for years. As the map above indicates, highly vulnerable areas include most of the Eastern and Northwestern parts of the nation.

The NOAA estimates each 11 year sunspot cycle is capable of launching 4 "extreme" (X class) CMEs and 100 "severe" CMEs at the earth. More X class events than were anticipated have occurred in the current cycle. The most dangerous period is the next 5 years. The peak peril is predicted by some to occur in May, 2013.

So far, neither NASA nor NOAA have publicly acknowledged the mortal threat these events may cause as the result of multiple meltdowns of nuclear plants worldwide. To date, there is no indication that the White House, Congress, Homeland Security, the Department of Defense and/or the **N**uclear **R**egulatory **C**ommission have adequately prepared to prevent the horrendous effects of such a solar megastorm.

The recent statement by a NASA scientist that human life would not end as the result of the direct effects of a solar storm during 2012 is misleading. A solar megastorm that causes widespread meltdowns of numerous nuclear power plants can **seriously end** millions, if not hundreds of millions, or even **billions, of lives** from radioactivity. This event could very well parallel the aftermath of a **nuclear weapons exchange** had there been war **between the USA and the USSR** -- **massive amounts of radioactivity** carried on prevailing winds all over the planet. The issue is not the specific year. This entire 11 year sunspot cycle should be of concern.

### Ext --- Grid Collapse Causes Food Shocks

**Blackouts cause extinction and mass crop failures**

**Hecht 11** – Editor in Chief @ 21st Century Magazine

Laurence, Solar Storm Threatening Power Grids – Yet no Action Taken to Implement Defences, <http://oilprice.com/Energy/Energy-General/Solar-Storm-Threatening-Power-Grids-%E2%80%93-Yet-no-Action-Taken-to-Implement-Defences.html> \*Language Modified

A prolonged lack of electricity in any of these areas would reduce the population to **Dark Age-like conditions**. Drinking **water supply** would break down for lack of pumping, and sewage service would cease shortly thereafter. For lack of refrigeration, the **food chain would collapse**, and medical supplies would be lost. Fuel could not be pumped, and thus transportation would break down. Heating and air conditioning systems would cease functioning. Communication would be [undermined] ~~crippled~~ by the lack of electricity as well as from the direct damage to satellites and sensitive electronics which a solar storm produces—perhaps no Internet and no cell phones. Modern **life would come to an end**, and a population and economic infrastructure unprepared for a return to pre-electricity conditions could **descend into chaos**.

### Ext --- Grid Collapse Turns Economy

#### A cyberattack on the grid collapses the economy and invites lethal terror attacks

Barletta 16(Lou Barletta, Congressman of Pennsylvania’s 11th Congressional District, 6/2/16, “Attack on electrical grid could collapse economy,” https://barletta.house.gov/media-center/opinion-editorials/attack-on-electrical-grid-could-collapse-economy)

It was like something from a Hollywood movie, but it was real. At about 3:30 p.m. on Dec. 23, a computer in an electricity distribution center in western Ukraine seemed to take on a life of its own. While a helpless worker watched, the cursor on the screen moved by itself and clicked on a box that opened a series of circuit breakers — a move that would take the entire power station offline. When a dialogue box appeared asking for confirmation of the command, the ghostly cursor moved again and completed the action. Reaching frantically for the mouse, the worker tried to abort what was happening, but the computer was being controlled from elsewhere. In all, about 30 substations were taken out of commission and 225,000 customers were suddenly cut off from the power supply. It marked what is believed to be the world’s first successful cyber-attack on a nation’s power grid. What happened is ominous because it reminded us that we should not believe ourselves immune to such an attack, even in the United States. A cyberattack on the power grid could leave millions of residents and key physical locations without power for an extended period of time. It is a discouraging fact that unlike every other hazard we are likely to face, from hurricanes to earthquakes and chemical attacks to space weather, there is no specific planning scenario to help state and local governments prepare for an extensive blackout. This prompts a blizzard of questions: How long will the power be out? How many people will be impacted? What backups need to be in place to protect our citizens? With this in mind, I hosted an April hearing on the consequences of a massive, coordinated attack on the electrical grid, in my role as chairman of the House Transportation and Infrastructure’s Subcommittee on Economic Development, Public Buildings and Emergency Management. We asked our witnesses from the Department of Energy, the Federal Emergency Management Agency and the Department of Homeland Security to provide the realistic timeframe for which we should be prepared for the power to be out. FEMA Administrator Craig Fugate was clear, saying, “Planning needs to be measured in weeks.” The other witnesses agreed. As a former mayor of my hometown of Hazleton, Pennsylvania, I know that localities will be on the front lines during a widespread, lengthy outage and will be tasked with handling much of the response. While our subcommittee witnesses tried to assure us that there were numerous efforts underway to help prepare state and local governments for the unthinkable, the mayors and local elected officials I frequently talk to feel they do not have all the information they need to prepare for such a catastrophe. We must be ready to deal with disruptions in telecommunications, water and waste treatment, healthcare delivery, financial services and transportation. There is no question that good communication is vital during the reaction to a disaster, but it is also critical when crafting a response strategy in advance. Since I believe that all disasters are local events, it is important that we tie in localities with states and the federal government so that the greatest coordination can be achieved. All levels of government must cooperate and anticipate all types of disasters. The FBI and the Homeland Security Department are hosting briefings for local governments, law enforcement, and energy companies to discuss and develop strategies for mitigating risk and providing better defense. In addition, I have been meeting with the North American Electric Reliability Corporation, the Edison Electric Institute, the American Public Power Association and the National Rural Electric Cooperative Association. These national organizations have committed to identify initiatives that cut across all levels of government and create plans we can put in the hands of officials at the state and local levels. Some pre-planning has already been undertaken, such as exercises conducted by NERC and PPL — one of the largest electric utilities in the nation. At our hearing, PPL President and CEO Bill Spence told of regular internal exercises and external drills with other utilities to practice their responses to various disaster scenarios. By extending this training by linking up state and local officials to the utilities, relationships will be formed, information will be shared, and efforts will be maximized. If the goal of terrorists is to collapse our economy, then shutting down our electrical grid is where they would start. Most troubling is the possibility that a cyberattack would be accompanied by a physical terrorist attack, a scenario that promises true havoc, panic and loss of life. The great challenge is that the threat continues to evolve, which only means that we are forced to evolve with it and be prepared for it.

#### **Cyberattack on electric grid hurts the economy, national security, and public health**

Kenderine and Jermain 18 (Melanie A. Kenderdine, nonresident senior fellow at the Atlantic Council’s Global Energy Center, served at the US Department of Energy (DOE) as the energy counselor to the secretary and director of the Office of Energy Policy and Systems Analysis, David Jermain, adjunct professor at Boston University, contributed to the DOE’s electricity system review, “US power grid needs defense against looming cyber attacks”, The Hill, published 3/23/18, accessed 7/3/18, <http://thehill.com/opinion/energy-environment/379980-us-power-grid-needs-defense-against-looming-cyber-attacks> )//EQ

A recent poll showed that more than 90 percent of Americans believe the government is not doing enough to protect the electric grid from cybersecurity attacks. Their fears appear to be justified. This month, the U.S. government revealed its concerns about Russian incursions into the operating systems of domestic electric power plants and noted that the efforts to disrupt date back to 2013. These attacks have the capability to bring down all or part of our electricity service. Such large-scale grid cyberattacks were foreseen. The Departments of Energy and Homeland Security identified the grid’s vulnerability to cyberattacks some time ago and called for new protective measures in the DOE-led January 2017 Quadrennial Energy Review. The study, which analyzed the entire U.S. electricity system, noted that that the key critical infrastructures underpinning the nation’s economy and national security — transportation, water, finance, natural gas, oil, communications/IT — depend upon a reliable electricity “uber-network.” A 2012 report by the National Research Council concluded that a cyberattack could black out a large region of the nation for weeks or even months. Public health and safety would be in jeopardy from an extended, widespread power outage, resulting in loss of life support systems in hospitals, nursing homes, and households, disruption of clean water supplies and sanitation, and a massive breakdown of the transportation system. The economic disruptions from an extended blackout would also be enormous. A 2015 Lloyds of London study found that a cyberattack on 50 generators in the Northeast could leave 93 million people without power and cost the economy over $234 billion. We’ve already seen previews of a successful cyberattack on the grid stemming from operational failures and extreme weather. The 2003 Northeast blackout left 50 million people without power for four days, causing economic losses between $4 billion and $10 billion. In Puerto Rico, 400,000 people are still without power six months after Hurricane Maria, with staggering impacts on the commonwealth’s economy and well-being. Russia, Iran, North Korea and others have large-scale, offensive cyberattack programs. The CIA has concluded with “high confidence” that Russian military attackers crippled computers in Ukraine’s financial system last year. This followed 2015 and 2016 cyberattacks that disabled part of Ukraine’s electric grid. Global security analysts say Russia is using Ukraine as a cyberwar testing ground. The U.S. also appears to be in their crosshairs as the overall U.S.-Russia relationship hits new lows, evidenced most dramatically by their interference in our 2016 elections. According to DHS and the FBI, Russia appears to be laying a foundation for a large scale cyberattack on U.S. infrastructure. The Dragonfly 2.0 hackers, identified by DHS as Russian government cyber actors, pursued a prolonged cyberattack (since 2015) on a U.S. power plant and computer networks controlling the grid. Industry and government have been trying to address cyber vulnerabilities. In 2015, Congress expanded DOE’s authority to take immediate measures in response to cyberattacks on the grid in the FAST Act. Congress has also proposed additional legislation to address grid-related cyber-defense deficiencies with resilience measures for electricity infrastructure. These bills — introduced but not passed — focus on state assistance, authority to address cybersecurity gaps for other energy infrastructures, and identification of cybersecure products for the grid. Energy Secretary Rick Perry should also be commended for setting up a new cybersecurity office at DOE. These actions are important but not enough. It is time for a comprehensive examination of how we anticipate, recover, and deter cyberattacks. We need to fund development and deployment of advanced designs and technologies to protect our grid and to provide states the tools they need to contribute to the defense of the nation’s electricity system. We need to incorporate mandatory reliability and resilience measures into every aspect of our electricity system and the internet. We must also address state-sponsored cyberattacks at the legal, regulatory, operational and diplomatic levels, including the development of international protocols. But the hardest part may be modernizing our jurisdictional system to ensure seamless federal authority to prepare for and respond to cyberattacks. The DOE study concluded that the electricity system is a national security asset. National security is inherently a federal responsibility and cybersecurity attacks do not respect jurisdictional boundaries. It is time to adopt a regulatory system that meets 21st century realities. Our economy and national security depend on it

### A2: Grid Resilient

#### Grid attacks likely

Stringer 21 --- David Stringer, Asia Energy Team Leader, and Heesu Lee. Bloomberg News, “Why Global Power Grids Are Still Vulnerable to Cyber Attacks” https://www.bloomberg.com/news/articles/2021-03-03/why-global-power-grids-are-still-so-vulnerable-to-cyber-attacks#xj4y7vzkg

More than five years after massive cyber attacks left a quarter of a million Ukrainians without electricity, the world’s power grids have become even more vulnerable to hackers.

As utilities turn to sources of renewable energy and add millions of other components like smart meters, they’re rapidly multiplying the number of connections and sensors along their networks, widening the potential for intrusions.

“Power grids are getting increasingly vulnerable because of digitalization and the use of more smart applications,” said Daine Loh, a Singapore-based power and renewables analyst at Fitch Solutions.

It’s a threat highlighted in an initial probe in India that found an October blackout in Mumbai may have been caused by cyber sabotage. That outage impacted stock markets, trains and thousands of households in the nation’s financial hub. The disruptive potential of grid failures -- as seen in Texas last month due to a sudden deep freeze -- makes the sector a key target, particularly for state-based hostile actors.

Over the past four decades, power plants and substations have been moving from manual to automatic controls, and are increasingly being connected to public and private networks for remote access, leaving them exposed to attacks. Producers and distributors have also often been reluctant to spend on protecting themselves against low-probability attacks.

“India’s power system is in urgent need of proper cybersecurity systems,” said Reji Kumar Pillai, president of India Smart Grid Forum, a think-tank backed by the federal power ministry and which advises governments, regulators and utilities. “Both the state and the central governments need to treat this with utmost urgency, without waiting for a disaster to happen.”

There’s been a sharp rise over the past two years in cyber attacks targeting critical infrastructure, including grids, and it’s also becoming easier for hackers to gain access to key equipment, according to Darktrace, a U.K.-headquartered security provider.

“There is now a path for attackers to run from spoof emails in an employee’s inbox right through to critical gas compressors and turbines,” said Sanjay Aurora, Darktrace’s managing director, Asia-Pacific.

The U.S. Department of Energy and its National Nuclear Security Administration said in December they were among targets in a suspected Russia-backed hack. Nuclear Power Corp. of India Ltd. said in 2019 that malware infected a computer network used for administrative functions.

Attacks aren’t confined to power grids. Recorded Future, a privately held cybersecurity firm based near Boston that tracks malicious activity by nation-state actors, said it noticed activity by a China-linked group against an Indian maritime port this week.

“Essential state infrastructures like power grids and nuclear reactors have been and will continue to be a target of cyber attacks because modernization allows internet connectivity, which makes them vulnerable,” said Kim Seungjoo, a professor at Korea University’s School of Cybersecurity. “It’s almost a natural instinct of hackers, especially the state-sponsored ones, to attack energy infrastructure because they can easily disrupt national security.”

### A2: No Grid Attacks

#### Actors have the means and motivations to strike critical infrastructure.

Wintch 21 --- Timothy M. Wintch, an active-duty Major in the United States Air Force. He is currently a graduate student at the Oettinger School of Science & Technology Intelligence, National Intelligence University, in Bethesda, Maryland. Mr. Wintch has over 11 years of experience in command-and-control operations as an Air Battle Manager. He holds a Bachelor of Arts in Politics from the University of California, Santa Cruz, and a Master of Arts in Military Studies from American Military University. (April 20th, 2021, “PERSPECTIVE: Cyber and Physical Threats to the U.S. Power Grid and Keeping the Lights on”, https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/)

Among critical infrastructure sectors in the U.S., energy is perhaps the most crucial of the 16 sectors defined by the Department of Homeland Security. This sector is so vital because it provides the energy necessary to run every other critical infrastructure sector. However, the U.S. power grid, the backbone of the energy sector, is built upon an aging skeleton that is becoming increasingly vulnerable every day. Whether from terrorists or nation-states like Russia and China, the power grid is susceptible to not just physical attacks, but also to cyber intrusion as well. However, much of this threat can be mitigated if the U.S. takes the appropriate steps to safeguard the power grid and avoid a potential catastrophe in the future.

Since Sept. 11, 2001, terrorism on U.S. soil has been at the forefront of American consciousness. Critical infrastructure provides an appealing target because of the disproportionally large impact even a small attack can have on the sectors. In particular, the power grid represents a particularly lucrative target, both in terms of the ease of access and the large impact it can make. The National Research Council stated that the U.S. power grid is “vulnerable to intelligent multi-site attacks by knowledgeable attackers intent on causing maximum physical damage to key components on a wide geographical scale.”[[1]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn1) Additionally, the physical security of transmission and distribution systems is difficult due to the dispersed nature of these key components, which in turn is advantageous to attackers as it reduces the likelihood of their capture.[[2]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn2) From 2002-2012, approximately 2,500 physical attacks occurred against transmission lines and towers worldwide and approximately 500 attacks against transformer substations.[[3]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn3) Terrorists have the motivation to attack the U.S. power grid but the very nature of the grid makes it highly vulnerable. The power grid is not only at risk from physical attacks, but also nation-state cyberattacks.

One nation that has shown both the capability and intent to use attacks against critical energy infrastructure is Russia, as demonstrated in their 2015 annexation of Crimea from Ukraine. A Russian cyber threat group known as Sandworm, which used its BlackEnergy malware, attacked Ukrainian computer systems that provide remote control of the Ukraine power grid.[[4]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn4) This attack, and another in 2016, each left the capital Kiev without power, prompting cyber experts to raise concern about the same malware already existing in NATO and the U.S. power grids.[[5]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn5) In any conflict between Russia and NATO, not only would similar cyberattacks pose a threat, but so would potential physical attacks severing fuel oil and natural gas lines to Western Europe. Russia has both the capability and intent to attack critical infrastructure, particularly power grids, during future conflicts in their “hybrid warfare” approach.

Another nation that has the capability to attack critical energy infrastructure is China, representing a threat to not just the U.S. energy infrastructure but also that of our allies whose support would be vital in a major conflict. A recent NATO report highlighted this threat from China’s Belt and Road Initiative, stating that “[China’s] foreign direct investment in strategic sectors [such as energy generation and distribution] …raises questions about whether access and control over such infrastructure can be maintained, particularly in crisis when it would be required to support the military.”[[6]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn6) Like Russia, China has been active with cyber intrusions in U.S. energy infrastructure. The Mission Support Center at Idaho National Laboratory characterized these as attacks as “multiple intrusions into US ICS/SCADA [Industrial Control Systems/Supervisory Control and Data Acquisition] and smart grid tools [that] may be aimed more at intellectual property theft and gathering intelligence to bolster their own infrastructure, but it is likely that they are also using these intrusions to develop capabilities to attack the [bulk electric system], as well.”[[7]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn7) China, therefore, has both the capability and intent to conduct cyber intrusions and attacks for myriad reasons.

Another arm of this threat is the reliance the U.S. energy industry has on imports from China, especially transformers. In early 2020, federal officials seized a transformer in the port of Houston that had been imported by the Jiangsu Huapeng Transformer Company before sending it to Sandia National Laboratory in Albuquerque. Sandia is contracted by the U.S. Department of Energy for mitigating national security threats.[[8]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn8) The Wall Street Journal reported that “Mike Howard, chief executive of the Electric Power Research Institute, a utility-funded technical organization, said that the diversion of a huge, expensive transformer is so unusual – in his experience, unprecedented – that it suggests officials had significant security concerns.”[[9]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn9) Previously destined for the Washington Area Power Administration’s Ault, Colo., substation, the transformer is believed to have been seized due to “backdoor” exploitable hardware emplaced by the Chinese prior to shipment.[[10]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn10) Shortly after these events, President Trump issued Executive Order 13920, “[Securing the United States Bulk-Power System](https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/),” essentially limiting the import of Chinese-built critical energy infrastructure components due to concerns about cybersecurity.[[11]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn11) Interestingly, Jiangsu Huapeng “boasted that it supported 10 percent of New York City’s electricity load.”[[12]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn12)

Franklin Kramer, the former Assistant Secretary of Defense for International Security Affairs, testified before a U.S. House of Representatives Energy and Commerce subcommittee during an energy and power hearing in 2011 and said that a “highly-coordinated and structured cyber, physical, or blended attack on the bulk power system, however, could result in long-term (irreparable) damage to key system components in multiple simultaneous or near-simultaneous strikes.” He added that “an outage could result with the potential to affect a wide geographic area and cause large population centers to lose power for extended periods.”[[13]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn13) Even the inclusion of features such as smart grids to the overall grid structure poses new vulnerabilities through their connectivity. Kramer stated that “such connectivity means that the distribution system could be a key vector for a national security attack on the grid.”[[14]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn14)

### Ext --- Resilience Solves Shipping

#### Resilience through info sharing key to shipping

Estay & Guerra 20 --- Daniel Sepulveda Estay and Pablo Guerra, Department of Technology Management and Economics, Technical University of Denmark, “The Wave Analogy of Cyber-Resilience as Applied to Shipping Operations” in “Cybersecurity and Resilience in the Arctic” 2020, page 266

It is therefore becoming increasingly clear that the abilities to avoid and detect cyber-attacks (cyber-security) and to react efficiently once cyber-attacks have been detected (cyber-resilience) have become critical for the success of smart shipping operations. loT enabled cyber-physical systems are regularly threatened by a broad range of potential cyber-attacks coming from criminals, terrorists, or hacktivists (He et al., 2016). Cyber-attackers use any available channel to exploit poorly secured systems for different purposes, giving way to threats like harassment, corporate espionage, extortion, stock market manipulation, or the planning and carrying out of terrorist activities. In parallel, there is the risk that failing to ensure continuous IT systems may also cause disruptions in operations (Jarvelainen, 2013), and consequent challenges for mission assurance of the enterprise (D. J. Bodeau, Graubart & Fabius-Greene, 2010). Rand has estimated that the global cost of cyber-crime can range from USS799 billion to over USS2 trillion (Dreyer et al., 2018) and, as recent examples like the Wannacry and Petya a viruses have shown, effects include not only disruption of industrial operations, but also lives put at risk.

The modem shipping industry thus faces cyber-risks associated with its own data and control systems, and also to its supply chains (He et al., 2016), as processes connected both with suppliers and customers through the internet form part of a shared network. As a result, cyber-attackers' access and impact actors sharing a common network, gaining access to IT systems through the weakest link in the supply network (He et al., 2016), (Khan & Sepulveda Estay, 2015). Considering their effects and the urgency of a problem that is continuing to unfold, it is sensible to ask how risks derived from the use of IT systems should be managed in shipping operations to increase detection and reaction to cyber-attacks.

### Ext --- Shipping Impact Dump

#### Major supply chain cyberattacks triggers great power conflict

Tung 8/3

Liam Tung (Liam Tung is an Australian business technology journalist living a few too many Swedish miles north of Stockholm for his liking. He gained a bachelors degree in economics and arts (cultural studies) at Sydney's Macquarie University, but hacked (without Norse or malicious code for that matter) his way into a career as an enterprise tech, security and telecommunications journalist with ZDNet Australia.), 8-3-2021, "Supply chain attacks are getting worse, and you are not ready for them", ZDNet, https://www.zdnet.com/article/supply-chain-attacks-are-getting-worse-and-you-are-not-ready-for-them/ jt

The European Union Agency for Cybersecurity (ENISA) has analyzed 24 recent software supply chain attacks and concluded that strong security protection is no longer enough. Recent supply chain attacks in its analysis include those through SolarWinds Orion software, CDN provider Mimecast, developer tool Codecov, and enterprise IT management firm Kaseya. ENISA focuses on Advanced Persistent Threat (APT) supply chain attacks and notes that while the code, exploits and malware was not considered "advanced", the planning, staging, and execution were complex tasks. It notes 11 of the supply chain attacks were conducted by known APT groups. Cybersecurity certifications can help you enter an industry with a high demand for skilled staff. "These distinctions are crucial to understand that an organization could be vulnerable to a supply chain attack even when its own defences are quite good and therefore the attackers are trying to explore new potential highways to infiltrate them by moving to their suppliers and making a target out of them," ENISA notes in the report. SEE: Network security policy (TechRepublic Premium) The agency expects supply chain attacks to get a lot worse: "This is why novel protective measures to prevent and respond to potential supply chain attacks in the future while mitigating their impact need to be introduced urgently," it said. ENISA's analysis found that attackers focused on the suppliers' code in about 66% of reported incidents. The same proportion of vendors were not aware of the attack before it was disclosed. "This shows that organisations should focus their efforts on validating third-party code and software before using them to ensure these were not tampered with or manipulated," ENISA said, although this is something easier said than done. As the Linux Foundation highlighted in the wake of the SolarWinds disclosure, even reviewing source code – for both open source and unaudited proprietary software – probably wouldn't have prevented that attack. ENISA is calling for coordinated action at an EU level and has outlined nine recommendations that customers and vendors should take. Recommendations for customers include: identifying and documenting suppliers and service providers; defining risk criteria for different types of suppliers and services such as supplier and customer dependencies, critical software dependencies, single points of failure; monitoring of supply chain risks and threats; managing suppliers over the whole lifecycle of a product or service, including procedures to handle end-of-life products or components; classifying of assets and information shared with or accessible to suppliers, and defining relevant procedures for accessing and handling them. ENISA recommends suppliers: ensure that the infrastructure used to design, develop, manufacture, and deliver products, components and services follows cybersecurity practices; implement a product development, maintenance and support process that is consistent with commonly accepted product development processes; monitor security vulnerabilities reported by internal and external sources, including third-party components; maintain an inventory of assets that includes patch-relevant information. The SolarWinds attack for example rattled Microsoft whose president Brad Smith said it was the "largest and most sophisticated attack the world has ever seen" and that it probably took 1,000 engineers to pull off. Alleged Russian intelligence hackers compromised SolarWinds' software build system for Orion to plant a backdoor that was distributed as a software to several US cybersecurity firms and multiple federal agencies. SEE: The cybersecurity jobs crisis is getting worse, and companies are making basic mistakes with hiring The US Department of Justice (DoJ) revealed last week that 27 districts' Microsoft Office 365 email systems were compromised for at least six months beginning in May 2020. The rise of state-sponsored supply chain attacks and criminal ransomware attacks that combine supply chain attacks, such as the Kaseya incident, has shifted the focus of discussions between the US and Russia. US president Joe Biden last week said a major cyberattack would be the likely cause of the US entering a "real shooting war" with another superpower.

#### Supply chain cyber disruptions trigger grid disruption and environmental destruction

Edwards et al. 21

Frances L. Edwards, MUP, PhD, CEM, Joseph Szyliowicz, PhD, Dan Goodrich, MPA, CEM, William Medigovich, MS, Liz Lange, MPA, Autumn Anderton, MA, March 2021, “Surface Transportation Supply Chain Security: Creating a Blueprint for Future Research”, Mineta Transportation Institute, <https://transweb.sjsu.edu/sites/default/files/1937-Edwards-Transportation-Supply-Chain-Security-Blueprint.pdf> jt

Cybersecurity has a prominent role in the management of business and government activities. While it has achieved increased academic recognition, with degrees in cybersecurity being offered at major national universities, 79 not all agencies have developed complete cybersecurity systems. The Department of Homeland Security (DHS) has created the Cybersecurity and Infrastructure Security Agency (CISA), a national risk management center for US critical infrastructure. The cybersecurity branch notes that “[c]yberspace and its underlying infrastructure are vulnerable to a wide range of risks stemming from both physical and cyber threats and hazards.”80 Palo Alto Networks has noted that the supply chain is the weakest link in cybersecurity. The cybersecurity of each partner in the chain is controlled within its own organization so that one partner with weak protections exposes the rest of the partners to hackers. New vulnerabilities are developing through the “Internet of Things, digital buyer-seller relationships, and robotic process automation,” raising the need to know how you’re your “suppliers, and their suppliers’ suppliers, and so on down the value chain, have the same kind of protection.”81

Within the surface transportation element of the global supply chain, there are multiple points of cyber vulnerability. SCADA systems have long been used to manage industrial systems and power grids and now operate the engines of merchant marine vessels. Navigation is carried out through cyber bases systems using global positioning systems (GPS). Cyber control of road and railroad signals, train and ship scheduling, and bridge operations offers further opportunities for hackers to interfere.82 Damaging the navigation cyber connection can cause a ship to go off course or even get lost at sea. Disruption in train signals can cause derailments, which can lead to environmental damage, fires and impacts on communities along the tracks.

Recent incidents have demonstrated the cybersecurity threat to maritime transportation. In July 2019, the US Coast Guard assisted a vessel bound for New York that had been subjected to a malware attack. The ship’s owners failed to provide adequate cyber protection for the on-board computer that was used for electronic charts, cargo management, and communication with the port, pilots and Coast Guard. They determined that the vessel’s lack of appropriate cyber protection was “exposing critical vessel control systems to significant vulnerabilities.”83 A more serious attack occurred in December of 2019 when a ransomware attack dubbed Ryuk shut down a port facility for 30 hours. “The virus further burrowed into the industrial control systems that monitor and control cargo transfer and encrypted files critical to process operations. The impacts to the facility included a disruption of the entire corporate IT network (beyond the footprint of the facility), disruption of camera and physical access control systems, and loss of critical process control monitoring systems.”84 A Singapore-based cybersecurity firm warned that ransomware attacks against ports could cost the world economy $110 billion.85

The Department of Homeland Security and the Department of Transportation have developed tools to educate the transportation sector about cyber risks, and provides tools to guide the development of cybersecurity programs. Trucking, maritime and freight rail elements are all discussed in the Transportation Systems Sector Specific Plan, 86 but the integration from vendor through the supply chain is not addressed. Cross-sector dependencies with power and public safety are acknowledged, and the importance of partners and stakeholders is discussed, but there is no discussion of the weak link outside the transportation sector that may expose the supply chain to cyber attack.

## Resilience Add-Ons

### Add-On --- Trade

#### Cyber attacks on infrastructure collapses trade

Merk 18 [Olaf Merk, leads the ports and shipping work at the International Transport Forum (ITF) of the Organisation for Economic Co-operation and Development (OECD), Lucie Kirstein and Filip Salamitov, "The Impact of Alliances in Container Shipping", 11/2/18, https://www.itf-oecd.org/sites/default/files/docs/impact-alliances-container-shipping.pdf]

In addition to alliances, vertical integration risks also reduce system resilience. Integration of shipping, terminal handling and hinterland transport could mean that whole transport chains are in the hand of just a few players, creating huge leverage for cyber-attacks, especially if parts of the chain are digitally connected. This became painfully evident during the NotPetya attack that hit Maersk ships and terminals (Box 7). Vertical integration could be considered to be related to the emergence of alliances. As service differentiation for the sea-leg is difficult in alliances – as the product is basically the same – one of the few remaining possibilities for individual carriers to differentiate is via vertical integration.

Box 7. Cyber security and risks associated to vertical integration

On 27 June 2017, a major cyber-attack began hitting firms mainly in France, Germany, Italy, Poland, Russia, Ukraine, the United Kingdom, and the United States. The attack is suspected to have started when hackers compromised the update server of Ukrainian tax accounting software company M.E.Doc so that it would distribute a malware referred to as “NotPetya” throughout its network. The malware further propagated itself notably via an exploit using a vulnerable Microsoft Windows network protocol. After analysis of the encryption routine of the malware, experts from Kaspersky came to the conclusion that the attack, although appearing as a ransomware attack, did not allow victims to recover their data even after paying the ransom, and the aim was therefore suspected to be directed at major disruption instead of financial gain for hackers (Ivanov and Mamedov, 2017). The carrier Maersk was presumably contaminated by this malware via software used by one of its offices in Ukraine. Maersk was forced to shut down many of its operating systems to stop the attack from spreading. The company was unable to process new orders and cranes were operated manually at some of its 76 container ports. The disruption caused major delays and led to rerouting of several vessels to ports not, or less, affected (Odell et al./FT, 2017). At least 17 terminals operated by APMT got infected by Maersk’s central IT infrastructure (Reuters, 2017). A number of terminals were unable to identify which shipment belonged to whom and therefore needed to clear cargo manually. The largest Indian port JNPT operated by Maersk’s APMT was forced to shut down and the terminal Maasvlakte II in Rotterdam stopped operations completely for a full week, which led to a highly congested service level.

According to Maersk’s annual report for 2017, the attack mainly impacted Maersk Line, APM Terminals and Damco. The effect on profitability was estimated to be around USD 250-300 million, with the vast majority of the impact related to Maersk Line in the third quarter (Maersk, 2018). Maersk estimated a 20% drop in volume and lost out on carrying 70 000 40-foot containers within the two weeks of the attack. Besides lost revenue, the attack also involved high costs of rebuilding its IT infrastructure. At the moment of the cyber-attack, Maersk did not own any cyber risk insurance. The company reported that 4 000 new servers, 45 000 new PCs, and 2 500 applications had to be reinstalled (Chirgwin/The Register, 2018). Actual impacts on Maersk’s performance could be higher than reported and probably stretch beyond the second half of 2017 (Porter/Lloyd’s List, 2017a). In April 2018, analysts speculated that the attack could have cost Maersk group over USD 500 million in expenses and lost profit. Others situate the cost between USD 400-500 million because the effect from the attack continued in the fourth quarter of 2017 and led Maersk to make investments in new infrastructure and insurances. Furthermore, the cyber-attack could have had an extended impact on market shares until the first quarter of 2018 (Beck/ShippingWatch, 2018). Although for most affected terminals it took a few days before they could resume operations completely, shippers were affected by delays of up to two months, because Maersk reportedly had difficulties in allocating new slots and tracking and assigning correct data to containers. The impact was widely felt by interviewed shippers and Lloyd’s List reported a similar observation that nearly two months after the attack, Maersk was still dealing with containers in transit at the time of the attack (Porter/Lloyd’s List, 2017b). One of the interviewed shippers reports having received additional demurrage invoices due to complications and delays caused by the cyber-attack, which suggests the carrier might have tried to shift part of the costs of the attack to their consumers.

Maersk’s global coverage, as well as strong horizontal and vertical integration in the sector further facilitated the knock-on effect of the cyber-attack. Companies who are reliant upon common IT infrastructure will logically suffer business interruption simultaneously when that infrastructure is compromised. Since supply chains are highly interconnected and even more so with increasing automation and digitalisation, this can result in an insecure operating environment even for those firms that make cyber security a priority. However, there is not only interdependence in IT infrastructure, but also in the utilisation of common assets. According to SeaIntel analysis, 20 other carriers transported containers on-board Maersk vessels around the time of the cyber-attack (SeaIntel, 2017; 319). MSC was the most affected with 23 vessel sharing agreements and four slot-charters, followed by Safmarine and Hamburg Süd. The most affected outside the 2M alliance and Maersk ownership was CMA CGM, with six vessel sharing agreements and four slot charter agreements with Maersk. The shipping sector is the backbone of international trade and ports are a vital part of every country’s infrastructure. Any major disruptions in supply chains can therefore have impacts on the overall economy. The scale of the cyber-attack and the many interconnections that exist vertically and horizontally in this industry could transform the collateral and rather accidental damage on a firm that was presumably not directly targeted, into a systemic risk for global trade.

#### Trade disruption triggers multiple extinction scenarios

Langan-Riekhof ‘21

et al; Maria Langan-Riekhof is the Lead Author and is the new Director of the Strategic Futures Group at the National Intelligence Council, leading the Intelligence Community’s assessment of global dynamics and charged with producing the quadrennial Global Trends product for the incoming or returning administration. She has spent more than 27 years in the intelligence community as both a senior analyst and manager, serving at the CIA and on the NIC. She brings a background in Middle East studies and has spent more than half her career analyzing regional dynamics. Her leadership roles include: Chief of the CIA’s Red Cell, founder and director of the CIA’s Strategic Insight Department, and research director for the Middle East. She was one of the DNI’s Exceptional Analysts in 2008-09 and the Agency’s fellow at the Brookings Institution in 2016-17. She is a member of the Senior Analytic Service and the Senior Intelligence Service and hold degrees from the University of Chicago and the University of Denver - National Intelligence Council - Global Trends 2040 – Form the section: “Scenario Four – Separate Silos” - MARCH 2021 - #E&F - https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends\_2040.pdf

With the trade and financial connections that defined the prior era of globalization disrupted, economic and security blocs formed around the United States, China, the EU, Russia, and India. Smaller powers and other states joined these blocs for protection, to pool resources, and to maintain at least some economic efficiencies. Advances in AI, energy technologies, and additive manufacturing helped some states adapt and make the blocs economically viable, but prices for consumer goods rose dramatically. States unable to join a bloc were left behind and cut off.

Security links did not disappear completely. States threatened by powerful neighbors sought out security links with other powers for their own protection or accelerated their own programs to develop nuclear weapons, as the ultimate guarantor of their security. Small conflicts occurred at the edges of these new blocs, particularly over scarce resources or emerging opportunities, like the Arctic and space. Poorer countries became increasingly unstable, and with no interest by major powers or the United Nations in intervening to help restore order, conflicts became endemic, exacerbating other problems. Lacking coordinated, multilateral efforts to mitigate emissions and address climate changes, little was done to slow greenhouse gas emissions, and some states experimented with geoengineering with disastrous consequences.

*Note to students*: this ev appears to advance a cemented future – but it is an ebook report by the National Intelligence Council outlining possible futures \*if\* certain premises were to take place. Perhaps this is best explained by an except from the opening of this report: “Welcome to the 7th edition of the National Intelligence Council’s Global Trends report. Published every four years since 1997, Global Trends assesses the key trends and uncertainties that will shape the strategic environment for the United States during the next two decades. Global Trends is designed to provide an analytic framework for policymakers early in each administration as they craft national security strategy and navigate an uncertain future. The goal is not to offer a specific prediction of the world in 2040; instead, our intent is to help policymakers and citizens see (aware of) what may lie beyond the horizon and prepare for an array of possible futures”.

## Aff Extensions / A2s --- Attribution

### Ext --- Attribution Insufficient Now

#### Failure to share information makes Russia hybrid attacks successful

Beaulieu & Salvo 18 --- Brittany Beaulieu, fellow and program officer for GMF's Alliance for Securing Democracy, and David Salvo, deputy director of the Alliance for Securing Democracy (ASD) and a senior fellow at the German Marshall Fund, German Marshall Fund of the United States (2018), “NATO and Asymmetric Threats:: A Blueprint for Defense and Deterrence”, https://www.jstor.org/stable/pdf/resrep18856.pdf

While NATO and the EU have pledged to improve their information sharing and coordination of responses across the asymmetric toolkit, these efforts are under-funded and lack high-level coordination. Moreover, the absence of a mechanism to share NATO classified information with the EU, an old problem, prevents both organizations from more systematic cooperation in responding jointly to the hybrid challenge. The lack of information sharing among allies at NATO is another challenge. For example, the United States did not share much information about the Russian operation against the 2016 presidential election as it unfolded and only a meager amount afterward. In the lead up to the French and German elections, information was shared on a bilateral basis, rather than through the NAC. The reservations of some allies to discuss their own vulnerabilities to interference operations only exacerbate NATO’s organizational impediments to addressing hybrid threats in a timely and coordinated manner. A formalized information sharing or early warning mechanism could help to rectify this problem, as would decisions in allied capitals to elevate discussion on hybrid threats at the NAC and share more threat information and intelligence.

### Ext --- Info Sharing K2 Attribution

#### Info sharing is key to proper attribution --- solves false flags

Skopik and Pahi 20 --- Florian Skopik, Senior Scientist of the research program “IT Security, & Timea Pahi “Under false flag: using technical artifacts for cyber attack attribution”., Cybersecurity volume 3, Article number: 8 (2020), https://link.springer.com/article/10.1186/s42400-020-00048-4

The challenges related to false flags have been investigated before (Pihelgas 2015). Especially (Bartholomew and Guerrero-Saade 2016) takes a closer look into the problem and also surveys noteworthy actors in the field. Cyber Information sharing (Skopik et al. 2016; Wagner et al. 2016) is a common means to gather important data to aid the attribution process, for instance, information on attackers, their capabilities, used TTPs and so on.

It is important to note that attack detection is very much different from attribution, in that sense that not all sources (Zimmermann 2014; MITRE 2019) relevant to detect attacks (Caltagirone et al. 2013) are also appropriate for attribution. In contrast to pure detection of attacks, attribution sets its focus to relating actions to actors. A particularly important piece are therefore actor profiles (Chiesa et al. 2008) used to correlate identified actions to known capabilities and applied tactics and techniques of actor groups. The main problem of the attribution is a potential misattribution. Since the perpetrator attempt to cover up their tracks through a mixture of evasiveness, deception, and destruction of records or though false flags. This issue is well known among agencies and secret services. The NSA and NCSC released for instance a joint advisory APT group to avoid possible misattribution Footnote1. The information sharing, especially threat intelligence, is one essential aspect to detect false falgs. There are some initiatives worldwide, such as the Cybersecurity Information Sharing Act in the USA Footnote2, Cyber Security Information Sharing of ENISA Footnote3, or Cyber Information Exchange in the NATO Footnote4. The NATO Cooperative Cyber Defence Centre of Excellence is also aware of the issue and developed own definitions for false-flag, no-flag cyber operations (Pihelgas 2015) and influence cyber operations (Brangetto and Veenendaal 2016). Influence cyber operations are designed to influence the behaviour of a target audience. These false flag operations are part of the hybrid threats today, such as Russian aggression against Ukraine in 2014 and its intervention in Syria in 2015. One of the latest false flag operation is the TV5Hack (see “Illustrative application of CAM to identify false flags” section).

#### Increased intelligence sharing allows attribution

Shea 17 --- Jamie Shea Deputy Assistant Secretary General for Emerging Security Challenges at NATO, How is NATO Meeting the Challenge of Cyberspace?, PRISM , Vol. 7, No. 2, THE FIFTH DOMAIN (2017), pp. 18-29, https://www.jstor.org/stable/pdf/26470515.pdf?refreqid=excelsior%3A13066a3aa3cce031d0aff811a7cc9f2c&ab\_segments=&origin=

Beyond these two flagship initiatives of the 2016 Warsaw Summit, a good portion of NATO’s effort to step up its game in cyber defense, is to enhance its ability as a platform to assist the Allies across a whole spectrum of cyber defense needs. For instance, a new memorandum of understanding (MOU) between NATO Headquarters (HQ) and individual Allies has been offered to improve intelligence sharing, crisis management, and lessons learned from cyberattacks. Already 22 of the 29 Allies have signed this new MOU. NATO has established a new intelligence division with a strong cyber threat intelligence function, which should incentivize Allies to provide more early warning and advance notice of cyberattacks or malware and not only lessons learned and post–incident information. Enhanced intelligence sharing among Allies will not only help to parry cyberattacks or to limit their damage but also to build over time a much more detailed and comprehensive picture of hacker groups, proxies, methodologies, and attribution techniques.6

### A2: Attribution Doesn’t Deter

#### Attribution is key to early warning --- deters escalation

Clark & Landau 10 --- David D. Clark Massachusetts Institute of Technology Susan Landau PrivacyInk.com, “Untangling Attribution” Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010) National Academies of Sciences, Engineering, and Medicine. 2010. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington, DC: The National Academies Press. https://doi.org/10.17226/12997. <https://nap.nationalacademies.org/read/12997/chapter/4>

In February 2010, former NSA Director Mike McConnell wrote that, “We need to develop an earlywarning system to monitor cyberspace, identify intrusions and locate the source of attacks with a trail of evidence that can support diplomatic, military and legal options—and we must be able to do this in milliseconds. More specifically, we need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment—who did it, from where, why and what was the result—more manageable.”2

This statement is part of a recurring theme that a secure Internet must provide better attribution for actions occurring on the network. Although attribution generally means assigning a cause to an action, this meaning refers to identifying the agent responsible for the action (specifically, “determining the identity or location of an attacker or an attacker’s intermediary”3). This links the word to the more general idea of identity, in its various meanings. Attribution is central to deterrence, the idea that one can dissuade attackers from acting through fear of some sort of retaliation. Retaliation requires knowing with full certainty who the attackers are.

### A2: Attribution Impossible

#### NATO cooperation makes attribution possible.

Siim Alatalu 18. Member of NATO Cooperative Cyber Defence Centre of Excellence’s Strategy Branch, where he is in charge of cyber strategy and policy research and training related to NATO and the EU, as well as providing subject matter expertise to the Centre’s other flagship projects. Prior professional career includes several advisory and managerial positions at the Estonian Ministry of Defence since 2001. “NATO’s responses to Cyberattacks.” https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP\_148.pdf

Thirdly, NATO’s particular advantage in cyber defence could stem from cooperation with its partner countries and with other international organisations, especially the European Union. Neither the Alliance nor the Union is an island on its own when it comes to cyber threats and vulnerabilities. The EU can do a lot in areas that are relevant for NATO, such as cybersecurity certification of devices imported into and used in European markets. Dependence on non-EU and non-NATO software could become a critical national security concern, as illustrated by for instance the Kaspersky case in the US.24 As highlighted by the recent attributions, there could be a global will for cooperation between NATO and non-NATO countries as any of them could become a target, as well as a bridgehead for further spreads of malicious cyber activities, as demonstrated by the WannaCry and NotPetya attacks.

#### Attribution is possible---new tech and cooperation solve

Susan Davis 19. United States, General Rapporteur. Science and Technology Committee (STC). NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence. . 148 STC 19 E rev. 1 fin. https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT%20148%20STC%2019%20E%20rev.%201%20fin%20%20-%20NATO%20IN%20THE%20CYBER%20AGE.pdf

15. However, in recent years, governments, private companies, and research organisations have increased their ability to attribute attacks at higher levels of confidence. Forensic tools have improved, and private and state analysts have built up databases and characteristic patterns for known intruders. On a technical level, truly harmful cyber attacks are very complicated and involve many moving pieces. Thus, the more complicated the cyber attack, the more likely the attacker is to commit mistakes along the way, enabling a forensics expert to trace the origin of the attack (Lindsay, 2015). Indeed, governments within the Alliance and beyond are increasingly attributing malicious cyber incidents to states and their proxies. Such transparency on cyber incidents is increasingly collective, coordinated in policy and time, and independent of the scale, nature, or impact of the incident (Giles and Hartmann, 2019). The Rapporteur supports this emerging policy of naming and shaming perpetrators and encourages further conversations at the NATO level.

16. Even if states and their proxies could be confident they will remain anonymous, truly convincing strategic rationales for large-scale surprise attacks are lacking. Anonymous cyber attacks are not well-suited for coercion, for example. Coercion only works if the attacked entity knows whom to yield or make concessions to. As one analyst points out succinctly, “[p]urely anonymous coercion is almost impossible because communicating and understanding the power to hurt implies that there is someone doing the hurting and a target concerned about avoiding getting hurt” (Lindsay, 2015). As a result, if an opponent wishes to coerce through cyber attacks, he cannot hide himself. This would defeat the purpose. How can the victim give in to demands if it does not know who the attacker is? (In contrast, cyber criminals want to stay anonymous when, for example, they attempt to extort money from victims.)

### A2: Attribution Bad --- Increases Attack Risk

#### Attribution doesn’t trigger a military response --- plenty of steps below the escalation ladder

Lindsay 15 --- Jon Lindsay, Munk School of Global Affairs, University of Toronto “Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack”, Journal of Cybersecurity, Volume 1, Issue 1, September 2015, Pages 53–67, https://doi.org/10.1093/cybsec/tyv003 Published: 28 November 2015 https://academic.oup.com/cybersecurity/article/1/1/53/2354517

Attribution is not the same as punishment. It might be if the attacker really cares about a reputation for integrity: concerns about plausible deniability in covert action often turn on executive worries about blowback from domestic constituents, political rivals, and friendly allies as much as sanctioning by the victim. However, since retaliation can be costly for the one administering the punishment as well as the punished, a victim may decide not to do anything even after attribution if the costs and risks of punishing are too great. China conducts pervasive cyber espionage against Western interests, and there is good evidence available publicly and in US intelligence circles that the Chinese state is responsible, but so far naming and shaming actions have had little effect. The USA has had no stomach for more serious sanctions thus far, even as it routinely attributes Chinese (or Russian or Iranian) intrusions.

#### Attribution doesn’t INCREASE the risk of retaliation --- countries will punish even with imperfect knowledge

Lindsay 15 --- Jon Lindsay, Munk School of Global Affairs, University of Toronto “Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack”, Journal of Cybersecurity, Volume 1, Issue 1, September 2015, Pages 53–67, https://doi.org/10.1093/cybsec/tyv003 Published: 28 November 2015 https://academic.oup.com/cybersecurity/article/1/1/53/2354517

Furthermore, attribution is not required for punishment. A minefield, if advertised, protects an area from intruders whether they are known to the defender or not, since the trespasser selects a very specific punishment by the act of stepping on a mine. Defensive deception similarly turns the attacker’s ability to penetrate a system against the attacker, by enabling the intruder’s effort to trigger his own punishment or simply creating paranoia that he may have done so [ 16 ]. States often punish whole villages or classes of people when individual guerrillas cannot be brought to justice. This is not only unpopular but also expensive because a lot more force must be expended over a larger area. Indiscriminate punishment is usually a less effective deterrent or warfighting instrument in civil war than targeting killing [ 72 ], and may even counterproductively embolden insurgents, but it certainly does not depend on attribution. Likewise, a victim of cyber attack who wanted to punish some attackers could cease digital transactions with all trading partners or start attacking all suspects. Doing so, however, would quickly undermine the benefits that made internet exchange worthwhile in the first place and would be very unpopular. Inflicting even small punishments on a large number of suspects can be difficult to execute (so to speak) as well as politically illegitimate.

### Ext --- Attribution K2 NATO Cohesion

#### Attribution lacking --- Makes consensus building and cohesion impossible

Brunner 22 --- Isabella Brunner, PhD Candidate in International Law, Researcher and Lecturer at University of Vienna, “The Prospects for an International Attribution Mechanism for Cyber Operations – An Analysis of Existing Approaches”, Date written: Date Written: July 3, 2020, Date Published: 11 Feb 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3986297

In cases of cyber operations below the threshold of an armed attack, Article 4 of the Washington Treaty calls on the NATO members to ‘consult together’ if the ‘territorial integrity, political independence or security of any of the Parties is threatened’. 47 Here as well, attribution is important. The process of consultation includes exchanging information and opinions, 48 and might also be used to discuss the attribution of the act to a state prior to launching a collaborative NATO operation. Article 4 thus likewise enables the sharing of intelligence especially in the context of cyber attribution.49 At least once, NATO has arguably already joined a collective attribution initiated by the Dutch and British governments in the cyber context, condemning the Russian hacking activities against the Organisation for the Prohibition of Chemical Weapons in 2018.50 There is, however, no public information available whether NATO resorted to Article 4 in this context, nor whether it considered adhering to any evidentiary standards for attributing the act to Russia.

The consultation process can, in some circumstances, lead to a joint decision or action, 51 which may include condemning acts of the wrongful state (after having attributed the activity successfully). It is clear, however, that this would have to happen in consensus with all NATO allies, which could require that – especially in the context of attribution – all NATO members are equally equipped with the necessary information and capacities to make a profound decision. To build this community of trust where NATO members can share information without hesitation, the NATO Cyber Defence Pledge was adopted at the Warsaw Summit in 2016, where member states pledged to invest in the improvement of their national cyber defence capabilities. According to the NATO website, ‘almost all Allies have upgraded their cyber defences’ since adopting the Pledge.52 Measures such as these further facilitate intelligence sharing between states, as states with a higher level of security will trust other ‘more cyber capable Allies’ more than those with less secure cyber defense mechanisms. 53

NATO is also cooperating with regional organisations, such as the EU, on questions regarding better intelligence-sharing to counter cyber threats. In a Joint Declaration in 2016, the EU and NATO noted the ‘urgent need to: Boost [the EU’s and NATO’s] ability to counter hybrid threats, including by bolstering resilience, working together on analysis, prevention, and early detection, through timely information sharing and, to the extent possible, intelligence sharing between staffs; and cooperating on strategic communication and response.’ 54 Also, amongst other initiatives, the EU Computer Emergency Response Team and the NATO Computer Incident Response Capability have concluded a ‘Technical Arrangement on Cyber Defence’ in 2016, providing a framework where both sides can better exchange information and share best practices on cyber defence.55

In sum, NATO has realised that there is a need to increase its capacities to become an effective platform of assistance and cooperation for its members to counter cyber threats (which also includes attribution). Measures such as the Cyber Defense Pledge or cooperation agreements with other organisations seem to help with capacity-building and better cooperation. However, it is evident that an institutionalised system comparable to the EU’s ‘Cyber Diplomacy Toolbox’ does not exist.

#### Attribution is key to collective action and unity

Brunner 22 --- Isabella Brunner, PhD Candidate in International Law, Researcher and Lecturer at University of Vienna, “The Prospects for an International Attribution Mechanism for Cyber Operations – An Analysis of Existing Approaches”, Date written: Date Written: July 3, 2020, Date Published: 11 Feb 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3986297

To summarise, there is potential within the EU’s Cyber Diplomacy Toolbox and its newly adopted sanctions regime, NATO’s alliance and the US Cyber Deterrence Initiative, to tackle the ‘attribution problem’. These collective mechanisms might help release the burden of attribution by one state and increase the political pressure on the alleged wrongful state, which might even perhaps deter future ‘malicious’ cyber incidents. However, the biggest issue for collective attribution seems to be a lack of trust between states, which, in turn, hinders them to take collective action. Without having the possibility to assess the evidence regarding attribution by other states themselves and the fact that states usually underline that there is no international obligation to share evidence, 65 states will most likely be reluctant to support attribution claims. Closely interlinked with this is the question whether common evidentiary standards might be helpful to solve this problem. In any event, states will tend to refuse to attribute if doing so could potentially harm their international relations with the alleged wrongful state. The lack of technical expertise and insecure cyber defence systems within some states compared to other technologically well-equipped states does not help with building trust either. Hence why capacity-building is crucial, also for a collective attribution effort. To conclude, although there seems to be potential within the above-mentioned mechanisms, it is questionable whether states will make use of them or remain fairly reluctant to attribute.

### Ext --- NATO Cohesion Impacts

#### Allied mistrust sparks conflict in every region---nuclear war

Dr. A. Wess Mitchell 10, President of the Center for European Policy Analysis, Doctorate in Political Science from the Otto Suhr Institut für Politikwissenschaft at Freie Universität, Master’s Degree from the Center for German and European Studies at Georgetown University’s Edmund A. Walsh School of Foreign Service, and Robert Kron, Research Association at the Center for European Policy Analysis, 2/1/2010, “Counting the Costs of Insecurity in North Central Europe”, http://www.cepa.org/ced/view.aspx?record\_id=219

America’s deprioritization of allies creates opportunities for revisionist powers. Such transition is recurrent in geopolitics; international relations are always characterized by uncertainty. Policy makers have to navigate a landscape that is often difficult to delineate, full of strategic actors whose purposes are often obscure and whose power is difficult to assess. Intentions are notoriously hard to divine, in part because rival states obfuscate them but in part because often the states themselves do not have a clear and consistent perception of what they want to achieve. Uncertainty arises also out of a more quantifiable source of knowledge, an assessment of hard power, which is imperfect and results in widely different estimates. It is sufficient to recall the challenges of assessing Soviet power throughout the Cold War.

Moments characterized by alleged large shifts in relative power present particularly acute problems of assessing power and intentions, adding an additional layer of ambiguity and uncertainty. Rumors of change put in doubt the relatively well- known, or at least familiar, geopolitical situation. All parties involved are unsure about their position relative to the others, the extent of their political sway, and the match between their commitments and their power. The established great powers may have a crisis of confidence, while emboldened rising states are uncertain how far their influence extends as well as how solid and credible is the power reach of their weakening rival. Revisionist powers now openly but cautiously question what was the grudgingly accepted geopolitical status quo.

Rising powers are thus curious but careful. They are interested in pushing the existing boundaries of their influence but do not know how far they can do so without meeting a firm opposition of the other power. In the current case, U.S. rivals— China, Russia, and Iran— appear keen to assert their influence and establish what they deem their rightful position in their respective regions and in the world but are also eager to avoid a direct confrontation with the United States. Uncertain about their own power relative to the United States, they test the hypothesis of a growing American economic and military fragility and decaying political reach. To figure out the new map of power, and possibly to redraw it at low cost, revisionist powers engage in probing.

In this chapter we examine this behavior— the probing by revisionist powers. We define probing as a low- intensity and low- risk test aimed at gauging the opposing state’s power and will to maintain security and influence over a region. It is a set of actions that studiously avoids a direct military confrontation with the leading power by targeting the outer limits of its commitments and interests. There, along the outer rim of its influence, the hegemon is at the furthest of its commitments and power projection. The perception, or rather the suspicion, of its decline is most consequential along these frontiers of power because the revisionist state senses opportunities in its own neighborhood and searches for confirmation of the rival’s weakness. Probing is an opportunistic behavior. It occurs when the revisionist states detect a permissive international situation, namely, when they think that the existing great power is retreating. It is still a behavior that is characterized by self- doubt and uncertainty, although if unanswered it results in the confirmation of the belief in the rival’s decline and may lead to ever more assertive challenges to the international order and expansions of influence by the geopolitical challenger. Over the past few years, and with greater frequency and brazenness, regional powers opposed to the United States have been engaging in probing. Russia, Iran, and China in their respective regions have been working under the hypothesis that the United States is retreating, out of choice, fatigue, or weakness, or all three combined. The American retrenchment is more pronounced in the Middle East, with the ending of U.S. combat presence in Iraq and the drawdown in Afghanistan as well as the unwillingness to intervene in Syria, leaving a vacuum for Iranian influence. But there is an equally pervasive perception of American withdrawal or decline in the other two key regions, Europe and Asia. In Europe, the perception is that Washington is redirecting its strategic focus and resources toward Asia and has limited willpower to back its extended deterrent, giving Moscow a window of opportunity to redraw the map in Europe’s eastern “borderlands. ” And in Asia, a rising and confident China looks at a United States hobbled by financial crises, fiscal imbalances, and a decade- long military overstretch in the Middle East. The reasons are different, but the broad perception is similar: the revisionist states sense an opening left by a distracted and weakening United States. And they probe along the periphery of American influence, from Ukraine to the South China Sea through the Persian Gulf. ORIGINS OF PROBING BEHAVIOR Probing stems out of a tentative belief that the existing geopolitical order is amenable to change, and it seeks to confirm this suspicion. A perceived geopolitical change remains only that, perceived, until facts on the ground confirm it. An assessment of a state’s power is merely an estimate of how that state may fare in a clash with others. As such, it informs a set of expectations for the future, and it may or may not reflect reality. Often there is little agreement among powers as well as within those powers as to which assessment of power is correct.1 Today, for instance, questions about the continued resilience of American power abound both abroad and in the United States, and there are analysts on both sides of the argument.2 Regardless of where one stands on the issue of American relative decline or retrenchment, the mere existence of such a debate is a source of concern because it points to an absence of clarity on the geopolitical scene. The various strategic actors no longer know where they stand on the international pecking order and are confused as to how far their own influence can reach and what the responses of their rivals may be.3 These are periods of a tense peace but also of great uncertainty about the nature of the security environment. As a scholar put it, it is the “fog of peace” that makes strategic planning more difficult because it is unclear who the enemy is, how much power a potential rival may have, and where the boundaries of political influence are.4 As history indicates, often such an uncertain strategic environment degenerates into war, which is a “dispute about the measurement of power. ”5 The outcome of a war is the violent clarification of such confusion. It settles the dispute about the assessment of power. A victory or defeat in war, followed by changes in boundaries, military bases, or political affiliations of governments, is one way to prove or disprove a perceived alteration in relative power. As British historian A.J.P. Taylor observed, the “test of a Great Power is . . . the test of strength for war. ”6 After its defeat in the 1853– 1856 Crimean War, Russia was clearly militarily inferior to European states (even though the victorious powers, Britain, France, Turkey, and later Austria, also encountered serious difficulties in projecting power to the Black Sea theater) and consciously chose to retreat, reform, and rebuild its foundations of power, known as a policy of recueillement, in order to maintain its status as a European great power.7 There is no clearer confirmation of a state’s decline than a loss in a direct confrontation with a rising power; there is equally no better proof that the perception of relative decline was incorrect when the aspirant revisionist state is soundly defeated. In the immediate aftermath of a war it is therefore easier to assess one’s own power relative to that of the other players. War lifts the “fog of peace. ” But war is rarely pursued simply to clarify one’s own uncertain standing relative to the other strategic actors. To engage in war, the ultimate test of power, is exceedingly dangerous, and no leader wants to enter into a violent conflict simply as a way of assessing the power of its own state relative to the target. Wars are realms of luck and un knowns as much as of more calculable kinetic clashes, and consequently the outcomes do not always align with the expectations preceding them.8 In fact, the losing party in a conflict has often entered that war having overestimated its own capability relative to the rival. Many in Europe, for instance, expected in summer 1914 to be “home for Christmas, ” only to remain in the bloody trenches for several years. Given this inherent uncertainty, the risk of being proven wrong for both the perceived rising and declining powers is high, and great powers in history seem to stumble into wars rather than consciously pursue them as tests of strength. The risks of war are incalculable and thus extremely high. A less risky way of assessing a changing equilibrium of power is through probing. This is a form of strategic behavior meant to test existing perceptions of power relations, seeking at the same time to draw the presumably new boundaries of influence. The rising or revisionist state, in particular, is strongly motivated to test the will of its seemingly declining rival power. It has the aspiration, mitigated by the fear of the rival great power, to alter the existing geopolitical map. Such states, unhappy with the existing international order, which they perceive perhaps as imposed on them and certainly as increasingly not reflective of their own rising aspirations and power, have the most to gain from probing. If this behavior confirms the perception that the existing great power is on the wane and that the map drawn by it is no longer supported by its strength and will, the revisionist state may be able to reassert lost influence over its neighborhood and revise a previous settlement. At the same time, such a state has also a strong incentive to avoid a direct clash with its main antagonist lest the perception of its relative weakening turns out not to match reality. A strategy of direct confrontation is risky because its success is predicated on the relative weakness of the targeted power, the existing hegemon, and this is exactly what is unknown. If the probing power becomes convinced that its hypothesis of its own superiority (and of the relative decline of the rival) is true, then a direct clash may occur. But until that confirmation, a safer, less risky course of action is to engage in a probing behavior, akin to testing the water before jumping in. Probes target the frontier of the rival power’s influence, where its interests are less pronounced, its power is at its farthest projection, and its political clout at its weakest. At these outer edges the response of the great power is expected to be most restrained, while the gains of the probing state are most likely to occur. The purpose of probing, therefore, is to gauge the resolve of the targeted powers. We will return to this later, but here it is important to note that a probing action is also a way of showing the renewed or freshly acquired capabilities and aspirations that otherwise would remain latent and without tangible effects. One cannot revise an established order by keeping one’s own intentions and capabilities hidden. Showing a new military platform, often in a carefully choreographed event, is one way of signaling growing power. The 1907– 1909 voyage of the American “Great White Fleet, ” meant to showcase the emergent global naval strength of the United States, was one such episode. The round- the- globe cruise was not targeted at a specific power and did not aim to extend American influence over a particular state or region. Rather, it was a broad assertion of American capabilities and global reach, and the other powers, Great Britain in particular, certainly received it as a sign that the United States was a power to be reckoned with. But probing is more than showing off. It is not simply an action of strutting on the world stage with newly acquired military gadgets and political confidence but a precisely targeted action with clear objectives. Through probing, a revisionist state aims at changing the existing geopolitical order where it thinks it can, namely, at the farthest points of the ruling great power’s influence. Probing, therefore, is not just mere signaling of displeasure with the rules of the international order and the map of power; it aims to revise the order gradually and carefully, starting from the outer layers of the rival great power’s influence. FEATURES OF PROBING The purpose of probing is threefold. First, a probing state aims to check whether the rumors of its rival’s weakening are true. A probe is a test, meant to elicit a response from the targeted power. Second, the revisionist state that engages in probing behavior wants to avoid a direct military clash with the existing great power. The risks of being wrong about the rival’s resolve and capability are simply too big. Third, the state’s objective is to achieve, if possible, low- cost revision of the existing regional order. These purposes can be seen in the features that characterize a probe and distinguish it from other types of behavior, ranging from fullout aggression to commercial pressures and diplomatic démarches. First, probes are low intensity, vigilantly avoiding a direct war with the main rival power. They are below the horizon of direct military confrontation. The revisionist state has no interest in starting an allout military conflict with the rival great power, perhaps declining but still more than a match. The level of violence used, therefore, is low, and probes are limited projections of power in areas of less pronounced interest to the rival. A probing power engages in a lot of selfrestraint; it intentionally elects to keep the use of force at a minimum. It can but chooses not to escalate. A probe is a calculated gamble, not a foolish thrashing around. The desire to avoid a war with the existing hegemon often leads the revisionist to project power under cover of civilian or paramilitary forces, part of a larger trend of “civilianization” of conflict.9 By using unmarked units to harass a U.S. protégé, a state is able to de ny authorship of provocative actions and thereby avoid a more violent and direct war while at the same time chipping away at the rival’s influence and wealth. The possibility of denying that an aggression has occurred drives costs of revisionism lower. For instance, the sixteenth- century privateer Sir Francis Drake acted on behalf of Queen Elizabeth I, raiding Spanish shipping but never in an official capacity. The queen went so far as to tell a Spanish ambassador that “Drake was a private adventurer, and that she had nothing to object to his alleged execution. ” She was careful in not provoking Spain too much but eager to “singe the King of Spain’s beard. ”10 A similar approach can be seen around the world today. The initial Russian push into Crimea in 2014 was done anonymously with unmarked special forces, dubbed by Ukrainians as the “little green men, ” a clear example of a long- standing Russian practice of tactical deception and disguise (maksirovka).11 It was an indication that Moscow was unsure whether Ukrainian forces would react, and, in the event of a determined opposition, it maintained the option of either escalating with larger conventional forces or halting operations and denying. Moscow seemed to be more careful in masking the identity of its forces in eastern Ukraine, where the local opposition was more assertive and the Western displeasure with Russian aggression more pronounced. The greater the risk of a strong response from the actors targeted, the more carefully tailored, dissimulated, and low- intensity is the probe. The use of unmarked troops and paramilitary forces allows Russia to claim that no aggression has occurred, and thus no military response from Ukraine or from the West is warranted. China has been testing the limits of the influence of the United States and its allies in the South China Sea using an array of civilianlooking vessels. Its fishing fleet, combined with a fishery- enforcement fleet, is integrated into its military institutions and plays an active role in expanding China’s maritime reach. As Lyle Goldstein observes, this is part of a “strategy of ‘defeating harshness with kindness’ (yi rou ke gang)” whereby China deploys “unarmed fishing vessels or fisheries enforcement vessels to confront foreign vessels operating in its EEZ and claimed waters. ”12 This low- intensity push tests the fron tier of American influence in a way that makes a U.S. response difficult.13 A foray by a Chinese naval vessel into contested waters can be countered with the might of the United States and its ally’s navy; a probe by fishing vessels manned by Chinese fishermen does not warrant the involvement of the U.S. Seventh Fleet. This is risky behavior, but it also indicates a desire by China to avoid a war with the other regional powers as well as with the United States.14 If it is openly a military attack, a probe is conducted with a strong and perhaps warranted belief that the rival power will not intervene because it is distracted elsewhere and because it deems the targeted region to be of little immediate interest. This was the case of the Russian war with Georgia in 2008, when Moscow felt emboldened by NATO ambivalence to extending its membership process to Tbilisi and by the American strategic distraction by the wars in Afghanistan and Iraq (where a small Georgian contingent was deployed). The Russian gamble was based on the expectation of no meaningful Western, and American in particular, response. The objective was to chip away at the unwelcome Western influence in Russia’s neighborhood but without spurring an equally unwelcome Western military reply— to “singe America’s beard, ” as it were. Second, a revisionist state engages in probing because it sees it as a low- risk but high- reward behavior. The low risk stems in part from the first feature, the carefully tailored level of aggressiveness that is expected not to elicit a full- out military response by the rival. It is also related to the third feature, explained below, namely, the fact that the immediate target of probing is geographically and political peripheral to the interests of the rival great power, and consequently contributes to the low likelihood of a forceful military response. But on top of being pursued as a low- risk action, a probe can yield high strategic rewards. Most often the revisionist power seems to direct probing behavior to its immediate vicinity, hoping to expand its influence over neighboring and thus more controllable regions.15 It is there that it has the greatest chances of extending its own political shadow successfully. Probes are rarely long- distance projections of power because incursions deep into the rival’s sphere of influence are more liable to be met with more assertive responses as well as being less likely to establish durable control by the probing state. The farther the revisionist state engages in probing behavior, the more high risk and low reward it is, and vice versa. Hence the more likely locations for probing behavior are in the near neighborhood of the revisionist power. Furthermore, probes focus on strategically important regions, either resource rich or located along lines of communication, or both. Elizabethan England, for example, conducted raiding probes of Spain’s vulnerable transatlantic arteries bringing gold from the New World— not its stronger positions in the Mediterranean. Imperial Germany’s probes of the Anglo- French alliance targeted Morocco, located near the strategically important choke point of Gibraltar but beyond easy reach of the main British fleet. Today China’s probes of U.S. allies in Asia often target oil and gas fields in the South China Sea. In all these cases, since the goal of probing is to test the power and commitment of a rival state, it has to be directed at regions where the rival’s influence is present but not preponderant. It is unlikely that regions of no geostrategic value or with few resources have much of a presence of the rival great power, and as such they are not prime material for probing. A state may still have imperial aspirations in such regions, but not every extension of power is a probe. Probing is not simply grabbing new areas of influence but first and foremost to test the will of the rival. There may be, of course, the bonus that if the probe is successful, it may result in the addition of strategically important regions. The third feature of probing is that it is peripheral or indirect. The target of the probe is the periphery or the frontier of the tested power where the rival’s presence is at its farthest reach, its interests are less pronounced, and thus its response is expected to be muted. Fearful of a militarily assertive response, the state that is probing is careful not to target areas that are clearly considered of primary and existential interests, such as the rival’s homeland or its immediate neighbors. Hence the visits of Russian or Iranian naval vessels to Venezuelan ports are less a probe per se than an act of grandstanding, since all sides know that the United States could quickly bring overwhelming force to bear in the event of a crisis. These are temporary publicity stunts rather than a calculated attempt to test the hegemon’s commitment to maintaining the status quo. Probes test for perceived weaknesses, not strengths, and it is on the outer boundaries of the existing great power that its influence is likely to appear the most fragile. The revisionist power is interested in probing the power and influence of its rival in places where that influence is at its weakest, overstretched, and uncertain. During the Peloponnesian War the Spartan general Brasidas adopted such a peripheral strategy, but only a decade into the conflict. The initial Spartan approach of annual invasion of Attica, Athens’s immediate neighborhood, failed to inflict sufficient damage to end the war. It was only with Brasidas, sent north with a small force of helots (minimizing thus the risk to Spartan manpower), that Sparta changed its strategy to one similar to probing, by persuading or forcing distant Athenian allies in Thrace to switch sides. And many did reconsider their allegiance to Athens, because, as Thucydides observes, there did not seem to be much risk given the distance from Athens and their belief that this empire was on the wane.16 Striking the rival’s periphery, and its allies, not only was cheaper than assaulting it directly but also forced it to devote a lot of resources to reasserting the lost influence. Global powers in particular have a “periphery or frontier problem” that invites probing. A lengthy frontier, distant from the homeland and thus from key logistical bases, is difficult to protect. The sheer amount of power needed to outfit the distant outposts, combined with the uncertainty as to the location and timing of potential attacks, makes it impossible to have an impermeable frontier. When a power assesses threats, the key questions of “where, when, and by whom” are directly related to the length of the imperial frontier. A regional power has well- delimited borders and a clear idea of who the rival is. For instance, from the final decade of the nineteenth century on, Germany was burdened with the possibility of a two- front war, with France on one side and Russia on the other; a serious problem of military planning caused by poor diplomacy but not a source of strategic confusion. For a global power, it is that strategic clarity that is missing, resulting in the need to prepare for multiple contingencies and ultimately to stretch resources in several theaters of potential action.17 While imperial Germany could concentrate on its two- front problem, Great Britain at the turn of the twentieth century had to consider threats from Russia (in Central Asia, pushing toward India), Japan (in the Asian littoral sphere), France (in Africa as well as the Mediterranean), and Germany (in Europe and the North Sea in particular). Through deft diplomacy, it managed to neutralize the first three, allowing it to focus on the German naval threat, thereby limiting its “frontier problem. ” In practice, probing the periphery of a rival’s great power often translates into testing the strength of its alliances. Most great powers, or empires, expand their influence in informal ways, through political arrangements with local elites and formal alliances.18 The security of these great powers, in particular of ones with global reach, therefore resides not only in the safety of their borders but in their ability to hold rivals at a distance and thwart their challenges to faraway interests. They do so only in part through their own forces and rely heavily on the presence of allies that provide additional military strength and local deterrence (see chapter 5). Allies are at the periphery of influence and strength of great powers, and it is there that the powers’ commitment and influence are at their weakest. It is clear that a state will respond to an encroachment on its territorial possessions or to an attack against its forward deployed forces. It is less certain, however, that a state will respond in the same strong fashion to similar actions directed against its allies and their interests. The security guarantee extended to them, the foundation of the alliance, is a promissory note that carries a high degree of uncertainty. Placing bases with troops on the territory of an ally is a time- tested way of diminishing this uncertainty. As Thomas Schelling put it, the role of U.S. troops in South Korea was simply to die, buttressing the American security guarantee to its ally.19 The loss of American soldiers to an initial attack by the enemy would, so the argument goes, create powerful pressures for Washington to respond. French general Ferdinand Foch, when asked before World War I how many British troops would be needed for the security of France, replied, “One single private soldier . . . and we would take good care that he was killed. ”20 Probes by the revisionist power are not attacks against these bases and forces that underwrite the credibility of the extended deterrent. Rather, they target areas that may be of great importance to the ally but not necessarily to the security patron. That is the periphery of the periphery, so to speak, the tip of the great power’s commitment. The United States has a particularly pronounced “periphery” problem. There are few direct threats to the continental United States, short of a large- scale assault with weapons of mass destruction or the tragic yet relatively small and isolated terrorist attack. While the absence of a contiguous threat is a geopolitical blessing, it also means that most of the menaces to U.S. interests and security are outside of the North American continent. Hence, in the competitive international environment, “the strategic position of the United States rests ultimately on its ability to project power over great distances. ”21 In practice this entails managing alliances that maintain stability and keep U.S. rivals on the defensive in key regions of the world, in particular along an arc from Europe to East Asia through the Middle East. And historically this has been, and continues to be, achieved by extending U.S. deterrence beyond the North American continent to the countries, some allied by treaty and some neutral. Such an extended deterrence is a “ ‘three- nation problem’ involving an aggressor nation, the United States, and some smaller nation which is the object of the aggressor’s designs and which Washington seeks to protect. ”22 Probing by an “aggressor nation” aims to test U.S. commitment to these “smaller nations, ” which constitute the periphery of American interests and power. In the most successful case, probing could achieve a dual purpose: first, it tests the level and credibility of the commitment of the distant security patron, and second, it can weaken the rival alliance. It does so by targeting the foundation of the alliance, the belief that the alliance is beneficial to both parties and that it is effective. As Michael Mandelbaum has observed, alliances need to manage two concurrent fears: one of entrapment, namely, of being dragged into undesirable wars of limited significance and local interest, and one of abandonment, the apprehension of often the weaker ally of be ing abandoned by its security provider when the need comes. 23 Probing aims to increase the rival’s fear of entrapment while at the same time stoking worries of abandonment among its weaker and more dependent partners. By harassing the local interests of the rival’s peripheral allies, the revisionist power wants to drive up the risk of a local war, perceived by the rival as a distraction and a potential drain of resources. At the same time, it wants to indicate to the smaller allies that they may not rely on their security provider to defend their local, narrow interest, and that they may be abandoned. The goal is to drive a wedge in the opposing alliance by leveraging the fundamental dilemma of alliances— the fears of entrapment and abandonment. This is where probing becomes more than a simple test of the rival’s strength. By targeting the outer edges of the existing hegemon, and thus harassing its alliance system, the revisionist is engaging in a much more significant endeavor. The contest for regional, or global, control is in the end a contest for allies. A.J.P. Taylor observed that when Germany “was bidding for the domination of Europe” in the decade before the outbreak of World War I, “her chosen method was to isolate the independent Powers one from another. ”24 As we point out in chapter 5, allies are, among other things, an extension of the distant patron’s power. Were they to peel away from the side of their security guarantor— or vice versa, were the security guarantor to decide that the risk of continued support of a distant ally pressured by a regional revisionist power is too big— it would in either case signify a retrenchment of power for that offshore patron. The loss of allies is both a confirmation of the waning sway of that rival great power as well as a further reduction in its reach. To be alone in inter national relations is to be vulnerable, inviting further aggressive behavior from the rival. Walter Lippmann observed in 1943, “No one knew, not Hitler, not Stalin, not Chamberlain or Daladier, the relative strength of the Axis and of the opposing combination. Only when Hitler succeeded at Munich in separating the Franco- British allies from Russia, had he so altered the balance of power in his favor that a war for the conquest of Europe was from his point of view a good risk. ”25 War is an extension of successful probing. The benefits of targeting allies of a rival, rather than the rival itself, are well recognized in history. The astute observer of history and politics Niccolò Machiavelli noted in his Discourses that attacking a rival’s ally is always a preferred option: “For I know especially that if I assault his friend, either he will resent it and I will have my intention of making war with him, or by not resenting it he will uncover his weakness or faithlessness in not defending a client of his. Both the one and the other of these two things are able to take away his reputation and to make my plans easier . ”26 In the strategic behavior we describe, the probing power is not interested in “making war” with the rival, and therefore a probe is not a full- out attack on a rival’s ally or supported state. The risks of activating the security guarantees or assurances that ought to be at the foundation of that alliance are too big. But it is an offensive act of sorts, which threatens the interests of the rival’s ally. The security patron will either respond, thereby disproving the perception of its weakness, or will not, “taking away his reputation” and undermining its alliance. China has been particularly astute in picking geographic objectives that are important to U.S. allies but only indirectly important to the United States, such as the shoals and reefs around the Spratly and Paracel Islands. By ratcheting up the pressure in these areas, China causes the targeted states to intensify their demands for American assurance while diminishing U.S. willingness to back allies over seemingly petty issues that could lead to a larger conflict. Americans do not want to risk their lives for insignificant and distant rocks. Russia achieves a similar effect by reigniting NATO’s eastern frontier through its attack on Ukraine and a series of threats against exposed NATO members around the Baltic Sea. Those are areas that until recently have not been prominent on the U.S. strategic radar screen but are naturally vital to those smaller states inhabiting the region, which in turn are driven to make increasingly vocal requests for security reassurances from Washington. As in the case of the South China Sea, however, the local and limited nature of the rival’s probes generates in Washington as much a perception of threat as fear of a larger conflict, raising doubts about the benefits of extending security guarantees to these allies and partners. In the end, these peripheral probes pursued by U.S. rivals can create a wedge between Washington and its regional friends and allies. These three features— low intensity, low risk but high reward, peripheral— point also to the timing of the probing behavior. Probing is a strategic behavior that arises out of an uncertain assessment of power relations. It is the product of doubt, not confidence, in the resilience of the existing international order. As such it arises early on in the transition of power, when perceptions of rise and decline are not firm. The vagueness of the security environment creates among revisionist powers the perception of opportunities that a probing behavior aims to test. Hence probing should occur with less frequency in the immediate aftermath of a war, when, as we point out, an assessment of relative power carries the weight of the ultimate test, war. A defeated power may have all the incentives to upset the existing order, but unless it has no ability to evaluate its clearly weakened position, it has no capacity to do so. After a defeat probing may be tempting but is unfeasible. Such states are more likely to pursue a policy of recueillement (introspection, a moment of pause and strengthening), characterized by internal reforms, modernization, and very limited foreign engagements mostly aimed at dividing the opposing alliance.27 When, however, the perceived weakening of the founding power puts in doubt the existing international settlement, the desire to revise it is matched by the possibility of doing so. The perception of American weakening, or at least retrenchment, therefore opens up a window of opportunity for those powers that aspire to expand their own influence and resent the Western order and its institutions. THE AUDIENCES OF PROBING Another useful way of looking at the strategic behavior of probing is by considering the audiences involved. As we argued, a revisionist power pursues probing behavior to check whether new boundaries of influence are feasible given the perceived weakening of the rival. The main purpose is therefore to elicit a response from the targeted audiences. That response, or lack thereof, supplies information necessary to draw the new outline of the geopolitical map. Probing is first and foremost a violent and risky didactic exercise. The most direct audience is the immediate target of the probing behavior, usually an ally, or an aspirant to be an ally, of the rival great power. Probing here seeks to gauge the willingness and capacity of the targeted state to withstand pressure, and ultimately it aims to push that state to sever itself from its security patron. As we examine in chapter 4, vulnerable frontier allies of a great power actively consider alternative strategic options, especially when they perceive themselves to be under threat from a neighboring revisionist pow er and to have a fraying security guarantee from a distant patron. A probe is meant to ratchet up the threat perception while also attempting to establish a sense of strategic isolation and separation from the security provider. Hence as important as, if not more important than, the first audience is the second one: the distant but more powerful ally and security provider. Probing tests indirectly the regional staying power of the rival hegemon. While carefully avoiding direct confrontation, the revisionist power wants to assess the commitment of the opposing great power to its ally in the near neighborhood. What the revisionist is testing, therefore, is not the rival’s resolve to oppose other great powers, but the rival’s reliability to its own allies.28 Resolve is the willingness to risk war to achieve one’s own objectives: the more diffuse and distant the threatened interests, the less the resolve. Given that the target of probes is peripheral and not the rival’s homeland or troops and bases, the resolve is assumed to be small. Direct war between the revisionist probing state and the rival great power is unlike ly to erupt as a result. Moreover, the probing state is not interested in finding out whether the rival has the will to fight a direct war: the stakes would be simply too high and the outcome too uncertain. A direct challenge would test the resolve of the rival. Poking around the periphery, therefore, is a poor test of the rival’s willingness to fight a war. History seems to confirm this. For instance, as scholars have pointed out, Soviet leaders did not think that U.S. responses to peripheral threats (e.g., in the Third World) could serve as indicators of future American behavior when its core interests (NATO allies, Japan, or the U.S. homeland) were threatened.29 Whether the United States responded militarily or not to a Soviet foray in Angola or Ethiopia could not be easily translated into expectations of future American behavior in Europe. But it does affect the perception of whether the United States wants to fight in other peripheral areas. “If Soviet leaders were to gain the impression that the United States is firmly set upon a course of neo- isolationism and the absolute avoidance of intervention in local wars, they might become dangerously adventurous in the Middle East and elsewhere. ”30

Probing, however, tests the reliability of the rival great power— that is, its willingness to protect and stand by its ally or aspiring allies. The immediate target is not a test of the rival’s general credibility but only of its commitment to the security ties to the state. Probing wants to elicit a response (or lack thereof) from the rival great power regarding the seriousness of its commitment to the directly targeted state. To be perceived as a reliable ally means to instill the belief that promised security guarantees will hold even in cases of heightened tensions and, in final analysis, of conflict. Consequently a perception of low reliability results in the belief that the alliance is fragile and that it may be in the small state’s interest to seek accommodation with the nearby revisionist power. As delineated above, probes are care fully tailored to split the distant security patron from its regional allies, showing it to be unreliable.

Even if it achieves nothing else, probing can introduce doubts about the security guarantees, forcing the security patron to renew its promises. The less reliable the security patron is perceived by its allies, the more insistent are their demands for continued security guarantees. Probing thus imposes an immediate cost on the rival great power by reactivating a frontier region that until then was dormant and by pressing the rival to expend more resources and political capital to reassert its security guarantees.

Finally, the third audience is composed of the geopolitical onlookers, states that are watching the behavior and derive their own conclusions about the resilience of the existing great power. The strategic interaction spurred by a probe does not directly affect them, but they perceive it as a regionally circumscribed development with potentially more global repercussions. That is, a probe is limited to a specific region but has radiating effects as others also see it for what it really is: a test of the resilience and reliability of the great power that may be analogous in other regions.

Recent academic literature puts in doubt the idea that reputation for commitment is interdependent. Thomas Schelling, among others, articulated that idea in his classic work from 1966 where he argued that U.S. reputation was global, and a loss in one region would have negative impact in other areas. Reputation was not compartmentalized in different regions, in large measure because the rival, the Soviet Union, was one and the same across the world map. Hence “we tell the Soviets that we have to react here because, if we did not, they would not believe us when we say that we will react there. ”31 Academics have relentlessly questioned this argument, resulting in copious writings asserting that reputation is not interdependent and, according to some, does not even matter.32 Reputation is merely a cult and does not exist in international relations.33 Policy makers, however, disagree and continue to speak of reputation for resolve and reliability as something that not only matters and requires constant work but also is interdependent. They prefer to rely on time- tested authors, from Thucydides to Machiavelli, who consider reputation as indispensable to political power.34 In brief, there is a deep gap between academics and policy makers on the issue of reputation.

By observing recent events in the three frontier regions— Central Europe, the Middle East, and East Asia— we think that the truth is closer to Schelling’s view. It is clear that the effects of probing behavior do not remain confined to the immediate actors involved (the probing power, the direct target— usually a rival’s ally— and the rival great power). Other actors in the region are keenly aware of the revisionist state’s probing and of the responses of the United States. For instance, other states, from the Baltics to Poland and Ukraine, observed Russia’s war against Georgia in 2008 and its invasion of Crimea in 2014 with great trepidation.35 These wars were symptoms of a more assertive Russia; a source of worry in themselves. But they were also meant to elicit an answer from the United States. Any sign of American hesitation to respond quickly and firmly to Russian small wars in the two states was perceived as affecting directly these other states, not directly involved in the probing event. America’s reputation for reliability, in other words, was at stake, even though Georgia and Ukraine were not NATO members but only aspiring to closer security and political relations with the United States and the EU. Similarly, Pacific nations from Japan to Australia follow with great attention China’s probing behavior in the South China Sea that puts pressure on Vietnam, the Philippines, and Taiwan. They too seek to figure out whether the United States has the will to remain as a security provider in this region and to the “global commons” in general. How the United States responds to a probe in a particular region therefore affects its regional image.

The question is whether there is also a wider, global audience to regional probes. Do Middle Eastern leaders watch American responses to Russia’s probing in Eastern Europe? Do Kremlin elites draw lessons from U.S. actions along the “first chain of islands” in East Asia? Or, do Chinese neo- Mahanian leaders think the United States is on the wane if it accommodates Putin’s imperial fantasies? According to the latest academic literature, the answer should be negative: how the United States is perceived to be doing in one region does not translate into a similar perception elsewhere. The practical implication of such a view is that the United States should not have fought in Vietnam to prove that it would stand its ground in Europe; similarly, it ought not to oppose Putin around the Black Sea basin simply to demonstrate that it will oppose China in the South China Sea. But we are not so confident that there are no connections between regional demonstrations of will and power. It is at least plausible, and perhaps safer, to argue that there are wider, global effects of probing. First, the world is indeed global, and regions are not hermetically separated from each other. As Nicholas Spykman observed, “Global war, as well as global peace, means that all fronts and all areas are interrelated. No matter how remote they are from each other, success or failure in one will have an immediate and determining effect on the others. It is necessary, therefore, to see the world as a whole and to weigh the measures taken to achieve victory in the light of conditions in all theaters. ”36 Leaders watch and learn from other regions, more than previously in history when conflicts were limited by technology and geographic knowledge to a contiguous region. Because of their domestic opacity, it is difficult to prove that America’s rivals learn from U.S. behavior in other regions, but the question whether they do so needs to be asked. Chinese military officials, for example, have commented publicly on lessons for China from the U.S. handling of the war in Ukraine.37 As one analyst noted, “It might be impossible to determine definitively whether the Ukraine Crisis has impacted China’s risk calculus in hotspots such as the South and East China Sea, but the evidence . . . certainly suggests that such eastern reverberations are quite plausible. ”38 At a minimum we have to recognize that some cross- regional analyses do occur, and it is safer to assume that the U.S. reputation does not stay limited to a region.

Second, the much stronger effect of probing appears to be on U.S. allies and friends, the key geopolitical spectators. They watch how the United States treats other allies and form an opinion regarding American reliability. The former director of Saudi intelligence summed up the view of many officials from U.S. allied states in the Persian Gulf when he said in reaction to the Russian seizure of Crimea, “While the wolf is eating the sheep, there is no shepherd to come to the rescue. ”39 Israel was interested in the war in Georgia; Japanese analysts followed the Obama administration’s decision to cancel the Ballistic Missile Defense (BMD) program in Central Europe; and Polish experts watch U.S. moves in East Asia.40 The probing by revisionist states is first and foremost an attempt to test the strength of their rival’s commitment to its allies and friends. In sum, probing behavior by revisionist states targets these specific audiences in order to elicit responses from them. The goal is to figure out whether and how to draw the new map of power. And it puts the burden on the targeted audiences: their responses determine whether the probe is successful.

EVALUATION OF PROBING: SUCCESS OR FAILURE

From the perspective of the revisionist power that engages in probing, whether a probe has achieved its objectives determines its success or failure. The minimum objective of the probing state is to measure the rival’s staying power in its neighboring region, an objective that is achieved whether the targeted powers respond or not, but it is difficult to interpret. The targeted rival may be tempted to ignore the probe not out of a sense of its own weakness but in the belief that ignoring the test will send a signal of strategic insouciance from its pedestal of power. Also, because of the local and limited nature of a probe, directly involving only the regional actors, it is tempting for the distant security provider to leave the response to its allies and friends. A direct and strong intervention by the offshore patron would escalate the interaction, raising the chances of a larger war, an outcome that neither party desires. But the shrewdness of a probing strategy is that it puts the targeted rival power in the position of having either to escalate the tensions in order to respond or to choose a less confrontational approach but one that risks weakening its alliances. The response to the probe, not the probe itself, is perceived as a potential cause of war. This creates strong disincentives for the tested great power to react by opposing the revisionist state’s probe in a direct and forceful way, or to respond at all. For instance, in the case of China’s probing actions in the South China Sea, the Obama administration’s approach seems to have been to accommodate Beijing, acknowledging a decline in U.S. naval capabilities and welcoming a greater Chinese role in providing security to the global commons.41 Similarly, after Russia’s takeover of Crimea, Washington’s first response was to turn the episode into a strictly regional affair. As President Obama put it in February 2014, “Any violation of Ukraine’s sovereignty and territorial integrity would be deeply destabilizing, which is not in the interest of Ukraine, Russia, or Europe, ” tellingly not including the United States in the list of the affected parties.42

The problem is that the temptation of the existing great power to either ignore or regionalize the tension stemming from the revisionist state’s probes— an attempt to de- escalate the strategic interaction— also constitutes a response. It may, however, be one that serves for the revisionist power as a confirmation of its initial suspicion that the rival’s commitment to the region was on the wane. An unanswered— ignored or regionalized— probe is an indication that the existing map of power is open to revisions. Another way to put this is that a probe is a question of sorts: does the existing hegemon have the will and capacity to oppose the revisionist power? An attempt to dismiss the question or to let allies respond to it is a tacit admission by the tested great power that its interest in maintaining a strong foothold and influence in the region is in decline. Silence in response to a probe is telling. Probing, therefore, always elicits some sort of answer, and in this narrow sense it is a success.

The purpose of a probe is also to attain a secondary, albeit crucial, goal of beginning to redraw the map of influence without generating counterbalancing pressures from the tested great power and its allies. The most successful probe would be one that pushes the targeted small states and other regional spectators closer to the revisionist power (or at least convinces them to distance themselves from their existing security patron, the rival great power) while at the same time convincing the rival great power that it is too costly to maintain its political influence and provide security in the region. Hence the probe needs to be evaluated on what it achieves in the three audiences: the directly targeted neighboring small state, the distant security patron, and the geopolitical onlookers (in particular other states in the region). The success or failure of a revisionist state’s probe depends on the actions by these three groups, and, arguably, it can attain partial success by achieving a revision of the status quo in one audience but not the other.

For instance, a probe can succeed in extending the revisionist power’s influence over the immediate target, the ally or would- be ally of the rival, but at the same time it may generate more vigorous efforts by regional onlookers to counterbalance it through a variety of strategies, ranging from military modernization to tighter defense cooperation with the distant security patron. This seems to be the case for Russia’s takeover of Crimea. Moscow quickly conquered Crimea and destabilized Ukraine’s easternmost oblast, successfully demonstrating its ability and willingness to use force to achieve limited territorial adjustments. While Kiev maintains its political independence, it has also been shown to be weak and unable to oppose Russian pressures. The quasi– civil war in the eastern regions and Russia’s conquest of Crimea make Ukraine an unlikely candidate for a closer relationship with the EU and NATO, even if Ukrainian political elites and public opinion may continue to be in favor of it. Russia’s probe, in the form of its intervention in Crimea and eastern Ukraine, has thus been successful in neutering the westward drift of Kiev. The EU, and in particular states such as France and Germany, have now an even smaller desire to bring Ukraine closer, as it is deemed too dangerous and risky; Ukraine is not worth losing business deals with Russia, not to mention starting a war with Russia.

The Ukraine War has also damaged American credibility in the region. Washington after all had given assurances (not “guarantees, ” which are reserved for NATO members) to the Ukrainian government in the Budapest Memorandum of 1994. This is undoubtedly a Russian success. But there are also other consequences of Russia’s probing, unintended and unwelcome by Moscow. Some states in the Central European region, in particular Poland and the Baltic states, have awakened from the geopolitical vacation of the past two decades. The 1990s and the 2000s were characterized by a widespread sense that threats to the territorial security of the region were minimal, and most of the strategic focus was on economic cooperation with the EU and on keeping in the good graces of the United States through participation in wars in Iraq and Afghanistan. This is over, at least in part. While strengthening the EU continues to be a priority in Central European capitals, there is simply no more interest in “out- of- area” operations, which drain resources and time from territorial defense. From this perspective, Russian probes have altered the geostrategic outlook of some Central European states. The eastern frontier is what really matters to them now, as their threat assessment has changed. Russia, in other words, has reached an upper threshold in its probes, creating a backlash among some of the states in the region, which are pursuing diplomatic counterbalancing and defense modernization. They are also calling for more visible and permanent NATO (and in particular, U.S.) security presence on their territories to shore up the extended deterrent against Russia.

It appears therefore that Russia is less successful than the other revisionist power, China. Moscow is less subtle in its probes, choosing dramatic military interventions (Georgia and Crimea) that generate growing fear and opposition among some European states as well as the United States. In part Moscow’s more aggressive behavior is a result of a Russian assessment of the weakness and divisions of the West. But in part the seeming Russian rush to restore influence over its “near neighborhood” is due to internal demographic, economic, and political problems. The growing weakness of Russia, a great power more by courtesy and by nuclear weapons than by economic and political strength, gives little time to Putin to shore up his country’s position facing China’s rapid economic growth and Europe’s political appeal. It is a short- term approach of large probes, and it may be successful only by extending influence over its most immediate nearby target.43

China, on the other hand, may have a different time frame, allowing it to probe in a much more indirect and less violent way, though this could change in the months ahead. It is therefore more careful and guarded, pursuing a long- term strategy of small probes over, quite literally, small rocks in the South China Sea. The U.S. “pivot” or “rebalancing” to Asia makes American presence and resolve more pronounced, increasing the doubt of a U.S. retrenchment and thus, from China’s perspective, the need to be cautious in testing the limits of American influence and commitment. Moreover, the counterbalancing efforts of regional onlookers, from Japan to the Philippines and Vietnam, are increasing in intensity, in both the rhetoric used and the arms buildup. Similarly, unlike Russia in Crimea, Beijing has not succeeded in extending its direct control over a large piece of real estate. But in the end it may be more successful, because it is establishing a gradual change in the map of power, visible only after a decade- long period. Through its probes, China is pursuing a classic example of “salami tactics. ” As Thomas Schelling describes them, “If there is no sharp qualitative division between a minor transgression and a major affront, but a continuous gradation of activity, one can begin his intrusion on a scale too small to provoke a reaction, and increase it by imperceptible degrees, never quite presenting a sud den, dramatic challenge that would invoke the committed response. ”44 Many small probes into areas of contested influence do not individually invite a strong response, but they erode steadily the perception and in the end the reality of the opponent’s influence.

Moreover, a continuing sequence of gradual probes signals the seriousness of the revisionist’s intent to alter the status quo. In the mind of the hegemon, the steady drumbeat of low- intensity and peripheral incidents creates the impression that the revisionist both has special claims for and may someday be willing to fight over a particular piece of real estate. These claims are often backed up by legal, historical, or ethnic justifications and a creeping physical presence— in Ukraine, Russian forces and equipment; in the South China Sea, artificially created reefs. Over time, this places the onus of a response on the shoulders of the hegemon and its allies in the region for why the status quo should be maintained. For a weary hegemon like the United States today, probes communicate that the act of supporting the regional status quo is no longer cost free but will require a level of exertion that was not needed in the past, inevitably leading to questions of whether such effort and resulting escalation are worthwhile.

Nonetheless, it is certainly possible to see failed instances of probing, which achieve the opposite of the revisionist power’s intentions. The historic scorecard of probing states is mixed. A clear failure of probing would be if the targeted regional states and offshore security patron responded strongly, tightening their alliance and even initiating a direct war. This is an unintended consequence of a probe and can take several forms, from a tightening of alliances countering the revisionist power to increased military contingency planning and rearming. In the worst- case scenario, it results in a combination of actions that counterbalance the revisionist state more effectively and forcefully than before the probing behavior started. The revisionist state did not want nor expect this response before engaging in probing. It amounts to a disconfirmation of the initial hypothesis that the rival great power is in decline and retreat, and in the end it worsens the strategic position of the probing state.

The biggest loser may thus be the probing power, which puts in motion a series of strategic interactions that undermine its own strength. This was the case of Germany in the early twentieth century. Kaiser Wilhelm’s visit to Tangier in 1905 initiated the first Moroccan crisis, manufactured by Berlin to, among other objectives, probe the strength of the brand new and untested Franco- British Entente Cordiale. 45 By challenging French interests in Morocco in a nonviolent way, Berlin wanted to pressure Paris, “the weakest link in the surrounding chain” of states opposing Germany.46 But it desired to do that in an area and in a way that were expected not to draw Great Britain into a direct confrontation, so that Germany could demonstrate to Paris that the entente was in effect useless. Morocco was important to France but not to Great Britain, and the German Foreign Office expected that London would not back Paris. Great Britain after all was also seen as retrenching after a bloody war with the Boers and unable and unwilling to project power on land to guarantee the security of its French quasi- ally. As Friedrich von Holstein put it, the French would seek a rapprochement with Germany, in effect bandwagoning, “when they have seen that English friendship . . . is not enough to gain Germany’s agreement to the French seizure of Morocco, but rather that Germany wishes to be loved on its own account. ”47 Germany, however, greatly miscalculated the British need for a continental ally and resulting commitment to France. The Moroccan crisis was resolved in a multilateral conference in Algeciras where Berlin ended in a position that was considerably worse than before the crisis: its only support was from the weak Austro- Hungarian Empire, while London was firmly and actively on the side of Paris. Instead of weakening the nascent strategic friendship between Britain and France, “German bullying” strengthened it.48 From then on, the “European Balance of Power, which had been ignored for forty years, again dominated British foreign policy; and henceforth every German move was interpreted as a bid for continental hegemony. ”49 London reoriented its attention away from the empire and toward the European continent, gradually planning to ready an expeditionary force to come to France’s defense.50 Berlin’s probe in Morocco turned into a clear failure.51

Probing is low risk, insofar as it is tailored to minimize a strong reaction of the rival, but it is not danger free for the revisionist state. Despite the fact that it arises out of a desire to clarify an allegedly new map of power, the effects of probing are difficult to interpret. All parties involved— the revisionist power and the targeted states— can miscalculate their reactions. In a case of moral hazard, the smaller states, directly targeted by the revisionist power, may respond violently to the low- intensity probe, feeling secure thanks to the alliance with a more powerful patron. Or, sensing that their distant patron is no longer capable of maintaining its influence, they may decide the exact opposite and accept the hegemony of the rival. This was the case of Athenian allies in Thrace, switching sides under General Brasidas’s pressure and persuasion. They were mistaken because their “judg ment was based more upon blind wishing than upon any sound prediction. ”52 Athens rallied and sent large forces north to restore its sway.

The probing power can also be the one to miscalculate, either not seeing the success or ignoring the failure. The nature of probing is such that the effects are often not visible immediately and require time to alter the perceptions and realities of power. The episode of Spartan commander Brasidas is again telling. Sparta did not follow up on his successes, in part because Spartan kings were jealous of his military exploits, but in part because they thought the damage inflicted on Athens was sufficient to strike a deal and end the war.53 They were of course wrong, as the war continued for decades. Alternatively, despite being checked, the probing power may simply up the ante, seeking some gain. This may have been the case of Germany, which did not stop challenging France and Britain after 1905, despite its diplomatic isolation, the military conundrum of a two- front war, and a robust Franco- British entente. In brief, there is no easy single interpretation of a probe and its effects.

A related risk is that a probe may lead to an unintended and untimely escalation of the strategic rivalry. As we described, the purpose of probing is to see how permissive the geopolitical order is, and to that goal a probe is limited in geographic reach and means used. It targets an issue presumed peripheral to the rival great power, seeking, for instance, a small territorial adjustment that is costly to the weaker neighboring state but not deemed worthy of a direct conflict by the distant and more powerful security patron. But the limited nature of the probe is somewhat at odds with its ultimate purpose to check the limits of an allegedly declining rival great power. A probe is a low- intensity, local pinprick with wider repercussions; limited geographically yet potentially global in outcome. The probing state has a strong interest in keeping the crisis limited and circum scribed to the narrowly defined area, but it is also poking the rival great pow er to see what the reaction may be. It is banking on the fact that the probe is on the periphery of the rival’s influence and interests, and thus that the rival will not escalate the interaction. The probing challenger, in other words, is betting that its great power rival will fear entrapment, being involved in an undesirable conflict, more than loss of prestige, reputation, or influence. The revisionist power seeks to use the fact of alliances (which it lacks itself) as a source of competitive disadvantage for the hegemon. This is based on two reinforcing perceptions— first, that the commitment involved in their maintenance is an encumbrance depriving the hegemon of strategic flexibility; and second, that the hegemon’s temptation to devalue its own alliances suggests that it feels the weight of this encumbrance.

Probes therefore arise from a view that entrapment is the congenital flaw of alliances. They are the ultimate act of attempting to expose the dangers of entrapment to hegemon and ally alike. This is ultimately a gamble— an expectation, not a certainty. And the gamble can backfire, as there is always the possibility that a probe will result in a dramatic escalation since it is targeted at multiple audiences. There is thus a clear recognition that a probe has a much wider purpose than its immediate action may convey, and consequently the desire to keep it limited runs against the desire to have a much larger demonstrative effect. As a result, the interaction a probe initiates has an inherent risk of escalating into a much larger confrontation.54

The revisionist state neither desires nor expects the escalation, but its possibility and perhaps likelihood are a direct outcome of probing. A probe by definition crosses a limit, a tacit or an explicit line of influence, in the expectation that it no longer reflects the actual will and power of the rival state. The revisionist power tests limits that until then were accepted and unchallenged and takes the first step in an “escalatory ladder” of competitive behavior. For instance, Kaiser Wilhelm’s support of Boer independence in 1896 was a test of British strength in what Berlin wrongly thought was a peripher al area of the British Empire. Similarly, the Moroccan crisis in 1905 was a test of British commitment to France in a region that should have been of no importance to London. Both, however, were a “move in the European Balance of Power, ” and that, beyond the details of the individual probes, was becoming of paramount concern to Great Britain. 55 Both were met by a strong British response, intensifying the Anglo- British rivalry. Escalation here was a willful choice of the targeted power.

Finally, probing can be in many cases a violent act, raising even further the likelihood of escalation and war. Probing is a political act first and foremost, only at times pursued by military means, but it does involve a careful application of violence or threat of violence. This requires strict political control, which is easier to maintain if the probe is not militarized and violent. But the more violent it becomes, the more difficult it is to keep it under political control. The logic of war may overwhelm the political rationale. Bismarck was keenly aware that the limited wars he fought, such as the Franco- Prussian one in 1870, would result in political outcomes that were different from his objectives were other great powers to become involved. But his greatest obstacle was the German military, resentful of civilian interference in what they deemed to be affairs in their exclusive purview. Political control over a limited war is paramount, because otherwise operational war objectives can overwhelm the larger political goals.56 The fact that Russia and China probe through a variety of nontraditional means, such as fishing vessels in the South China Sea and specially formed battalions (Vostok) of Chechens, makes political control more difficult. There is an incentive to use such means in a more aggressive way than would be warranted by official state forces, because in case of defeat one can always deny control over them and claim that they are simply individual citizens. Moreover, the “civilian” paramilitary forces that the probing power uses (e.g., the “Russian separatists” in eastern Ukraine) may not be easily recalled if the conflict ceases to be useful. The civilianization of conflict has its own risks. This makes probing behavior inherently destabilizing to an international order, as it sets forces in motion that, once unleashed, can be hard to control.

Probing can, moreover, spiral into war, unexpected and perhaps unwanted by the revisionist power. For instance, in the third century BC, Rome started to probe Carthaginian power in Sicily. It extended protection to Messana (or, more precisely, to a band of mercenaries, the Mamertines, who controlled it), thereby asserting Roman influence in northern Sicily. The peaceful withdrawal of the Punic garrison from the area seemed to suggest that a war was avoidable and the probe successful in attaining a low- cost revision to the balance of power. But the Romans miscalculated and were emboldened by this small success. As Polybius put it, they “now cherished the hope that they could drive the Carthaginians out of Sicily altogether, and that once this goal was attained their own power would be greatly increased. ”57 Carthage sent a large force to Sicily and solidified its alliance with Syracuse against Rome and its new ally Messana. Rome then escalated and sent a large army to besiege Syracuse, starting the first Punic war, which lasted more than twenty years.58 What started as a low- cost, low- risk probe turned into a long and costly slugfest. To sum up, the risk of probing is that it may result in a slide toward a direct clash. Miscalculation and escalation by all parties involved can elevate what is a small, localized harassment into a wider, more violent war. Moreover, a pattern of probing may gradually lead all sides to accept war as necessary and perhaps inevitable, as each probe and reaction escalates the competitive interaction.

#### NATO key to countering China in SCS and ECS

Brzezinski 6/1 - Ian Brzezinski is a Senior Fellow at the Atlantic Council focusing on the Transatlantic Security Initiative and the Scowcroft Center for Strategy and Security. He is the Former Deputy Assistant Secretary of Defense for Europe and NATO Policy, 2020 (“NATO’s role in a transatlantic strategy on China”, available online at <https://www.atlanticcouncil.org/blogs/new-atlanticist/natos-role-in-a-transatlantic-strategy-on-china/>, The Atlantic Council)

On the eve of the NATO Summit in London last December, the Alliance’s Secretary General Jens Stoltenberg addressed the need for a collective response to China’s emergence as a global power. “This is not about moving NATO into the South China Sea,” he stated, “but it’s about taking into account that China is coming closer to us—in the Arctic, in Africa, investing heavily in our infrastructure in Europe, in cyberspace.” At the summit, NATO heads of state diplomatically declared that China has become a concern: “we recognize that China’s growing influence and international policies present both opportunities and challenges that we need to address together as an Alliance.”

Indeed, it is hard, if not impossible, for NATO to avoid China. Beijing presents a full spectrum challenge to the transatlantic community—a challenge whose potential mirrors, if not surpasses, that once posed by the former Soviet Union. China’s $14 trillion economy is expected to soon surpass that of the United States, and Beijing exercises that might in a predatory fashion around the globe, including in the United States and Europe. China threatens to boycott companies and countries that criticize its policies, leverages its debt instruments against poor nations, and is buying up critical infrastructure around the world. Its acquisition of European ports has raised concerns of top NATO commanders who warn that such ownership could adversely affect the Alliance’s ability to use those facilities in times of crisis.

China is a technological challenge to the West. It is a leader in 5G communications, artificial intelligence, hyper-sonic weapons, and quantum computing. It has demonstrated repeatedly that it is willing to exercise that prowess against Western interests and security. Chinese cyber espionage and disinformation campaigns have become part of daily life for all NATO allies, including both their governments and private enterprises.

Beijing’s military is a major driver behind China’s technological edge and is developing and exercising global reach. China’s $260 billion defense budget has a purchasing power estimated to equal or exceed 70 percent of that of the US defense budget. China’s military cooperation with Russia continues to expand and the two exercise not only in the plains of Central Asia but in the Mediterranean and Baltic Seas. Chinese military forces are the pointy of end of the spear Beijing uses to undermine the rules based international order. Its maritime claims and aggressive activities in South and East China Seas stand among its more prominent actions.

And, China’s leadership relishes its role as an ideological challenge to the West and the latter’s practice of liberal democracy. China usesits economic, technological, and military power to promote globally its form of national authoritarianism. Beijing even asserts that its political model has provided the most adept and agile response to today’s coronavirus epidemic.

So how should NATO should respond to China’s growing global assertiveness? What should be NATO’s China strategy?

When considering this issue, it is important to recognize that the foundation for a relevant NATO role in a transatlantic China strategy has long been established. For decades, the Alliance has been operating around the world. NATO has led the International Security Assistance Force in Afghanistan since 2003. Its naval forces have patrolled against pirates off the shores of Africa, commencing with operation OCEAN SHIELD in 2008. As a member of the Coalition to Defeat ISIS, NATO provides training to military establishments across the Middle East. And, on a daily basis the Alliance addresses terrorism, cyber-threats, disinformation, and other global issues.

Most relevant to addressing China are the Alliance’s long-standing relationships with key democracies of the Indo-Pacific region. NATO established Global Partnerships with Korea, New Zealand, and Mongolia in 2012, Australia in 2013, and Japan in 2014. These relationships are predominantly consultative, but most of these partners have contributed to NATO missions, including in Afghanistan.

As the transatlantic community’s lead instrument for security collaboration, NATO can contribute to the former’s relationship with China in three important ways. As a multinational security forum, it can foster among NATO allies and partners a shared awareness of China’s capacities and activities that generate risk to and opportunity for the North Atlantic community. NATO has long served as an important forum through which its Allies and partners share intelligence data and assessments needed to foster and facilitate collaborative action.

Second, NATO can help develop and promulgate a transatlantic security strategy and posture regarding China. That strategy’s objectives should include the development of a cooperative relationship with China as well the dissuasion of China from undermining the interests of the transatlantic community. The latter would define the appropriate role and means for the Alliance to contribute to deterrence and when necessary defense against Chinese aggression that imperil those interests.

Third, NATO’s civilian and military capacities should be used to facilitate the defense and security component of a Western strategy addressing China—including in the tasks of engagement, deterrence, and defense.

#### SCS war escalates to extinction.

Klare 17 – Michael Klare, Professor of Peace and World Security Studies at Hampshire College, “Escalation Watch: Four Global Hotspots for Trump”, Asia Times, 1-20, http://www.atimes.com/article/escalation-watch-four-global-hotspots-trump/

Within months of taking office, President Donald Trump is likely to face one or more major international crises, possibly entailing a risk of nuclear escalation. Not since the end of the Cold War has a new chief executive been confronted with as many potential flashpoints involving such a potential for explosive conflict.

This proliferation of crises has been brewing for some time, but the situation appears especially ominous now given Trump’s pledge to bring American military force swiftly to bear on any threats of foreign transgression. With so much at risk, it’s none too soon to go on a permanent escalation watch, monitoring the major global hotspots for any sign of imminent flare-ups, hoping that early warnings (and the outcry that goes with them) might help avert catastrophe.

Looking at the world today, four areas appear to pose an especially high risk of sudden crisis and conflict: North Korea, the South China Sea, the Baltic Sea region, and the Middle East. Each of them has been the past site of recurring clashes, and all are primed to explode early in the Trump presidency.

Why are we seeing so many potential crises now? Is this period really different from earlier presidential transitions?

It’s true that the changeover from one presidential administration to another can be a time of global uncertainty, given America’s pivotal importance in world affairs and the natural inclination of rival powers to test the mettle of the country’s new leader. There are, however, other factors that make this moment particularly worrisome, including the changing nature of the world order, the personalities of its key leaders, and an ominous shift in military doctrine.

Trump may lift gold as new leaders carry risk

Just as the United States is going through a major political transition, so is the planet at large. The sole-superpower system of the post-Cold War era is finally giving way to a multipolar, if not increasingly fragmented, world in which the United States must share the limelight with other major actors, including China, Russia, India, and Iran. Political scientists remind us that transitional periods can often prove disruptive, as “status quo” powers (in this case, the United States) resist challenges to their dominance from “revisionist” states seeking to alter the global power equation. Typically, this can entail proxy wars and other kinds of sparring over contested areas, as has recently been the case in Syria, the Baltic, and the South China Sea.

This is where the personalities of key leaders enter the equation. Though President Obama oversaw constant warfare, he was temperamentally disinclined to respond with force to every overseas crisis and provocation, fearing involvement in yet more foreign wars like Iraq and Afghanistan. His critics, including Donald Trump, complained bitterly that this stance only encouraged foreign adversaries to up their game, convinced that the US had lost its will to resist provocation. In a Trump administration, as The Donald indicated on the campaign trail last year, America’s adversaries should expect far tougher responses. Asked in September, for instance, about an incident in the Persian Gulf in which Iranian gunboats approached American warships in a threatening manner, he typically told reporters, “When they circle our beautiful destroyers with their little boats and make gestures that … they shouldn’t be allowed to make, they will be shot out of the water.”

Although with Russia, unlike Iran, Trump has promised to improve relations, there’s no escaping the fact that Vladimir Putin’s urge to restore some of his country’s long-lost superpower glory could lead to confrontations with Nato powers that would put the new American president in a distinctly awkward position. Regarding Asia, Trump has often spoken of his intent to punish China for what he considers its predatory trade practices, a stance guaranteed to clash with President Xi Jinping’s goal of restoring his country’s greatness. This should, in turn, generate additional possibilities for confrontation, especially in the contested South China Sea. Both Putin and Xi, moreover, are facing economic difficulties at home and view foreign adventurism as a way of distracting public attention from disappointing domestic performances.

#### NATO stops European militarization and war

Binnendijk 19 “5 consequences of a life without NATO”Hans Binnendijk - Distinguished Fellow, Transatlantic Security Initiative, March 19, 2019, https://www.defensenews.com/opinion/commentary/2019/03/19/5-consequences-of-a-life-without-nato/

NATO’s retirement would thirdly exacerbate divisions within Europe. NATO’s glue not only holds European militaries together — it provides the principal forum to discuss and coordinate security issues. The European Union is unlikely to substitute for NATO in this respect because it has no military structure, few capabilities and no superpower leadership to bring divergent views together.

Germany and France already seek a plan B should NATO collapse, but without the United Kingdom in the European Union, an all-European approach is likely to fail. The added insecurity of NATO’s collapse would also amplify current populist movements in Europe. The consequence could be renationalization of European militaries, a system that brought conflict to the 19th and early 20th centuries.

#### Extinction

Fisher 15 – Fisher, Vox Foreign Affairs Editor (Max, “How World War III Became Possible”, 6-29, <http://www.vox.com/2015/6/29/8845913/russia-war>)

Europe today looks disturbingly similar to the Europe of just over 100 years ago, on the eve of World War I. It is a tangle of military commitments and defense pledges, some of them unclear and thus easier to trigger. Its leaders have given vague signals for what would and would not lead to war. Its political tensions have become military buildups. Its nations are teetering on an unstable balance of power, barely held together by a Cold War–era alliance that no longer quite applies. If you take a walk around Washington or a Western European capital today, there is no feeling of looming catastrophe. The threats are too complex, with many moving pieces and overlapping layers of risk adding up to a larger danger that is less obvious. People can be forgiven for not seeing the cloud hanging over them, for feeling that all is well — even as in Eastern Europe they are digging in for war. But this complacency is itself part of the problem, making the threat more difficult to foresee, to manage, or, potentially, to avert. There is a growing chorus of political analysts, arms control experts, and government officials who are sounding the alarm, trying to call the world's attention to its drift toward disaster. The prospect of a major war, even a nuclear war, in Europe has become thinkable, they warn, even plausible. What they describe is a threat that combines many of the hair-trigger dangers and world-ending stakes of the Cold War with the volatility and false calm that preceded World War I — a comparison I heard with disturbing frequency. They describe a number of ways that an unwanted but nonetheless major war, like that of 1914, could break out in the Eastern European borderlands. The stakes, they say, could not be higher: the post–World War II peace in Europe, the lives of thousands or millions of Eastern Europeans, or even, in a worst-case scenario that is remote but real, the nuclear devastation of the planet.

### A2: No Hybrid War

#### Reject defense---false sense of security leaves us vulnerable

George Beebe 19, vice president and director of studies at the Center for the National Interest, a nonpartisan think tank in Washington. He is also the former head of Russia analysis at the CIA, “We’re More at Risk of Nuclear War With Russia Than We Think,” Politico, 10/7/19, https://www.politico.com/magazine/story/2019/10/07/were-more-at-risk-of-nuclear-war-with-russia-than-we-think-229436

In the 1950s and 1960s, Americans genuinely and rightly feared the prospect of nuclear war with the Soviet Union. Schoolchildren regularly participated in air raid drills. Federal, state and local governments prepared for operations in the event of a nuclear emergency. More than a few worried citizens built backyard bomb shelters and stockpiled provisions.

Today, that old dread of disaster has all but disappeared, as have the systems that helped preclude it. But the actual threat of nuclear catastrophe is much greater than we realize. Diplomacy and a desire for global peace have given way to complacency and a false sense of security that nuclear escalation is outside the realm of possibility. That leaves us unprepared for—and highly vulnerable to—a nuclear attack from Russia.

The most recent sign of American complacency was the death, a few weeks ago, of the Intermediate-Range Nuclear Forces Treaty—a pivotal 1987 agreement that introduced intrusive on-site inspection provisions, destroyed an entire class of dangerous weaponry, and convinced both Washington and Moscow that the other wanted strategic stability more than strategic advantage. The New START treaty, put in place during the Obama administration, appears headed for a similar fate in 2021. In fact, nearly all the key U.S.-Russian arms control and confidence-building provisions of the Cold War era are dead or on life support, with little effort underway to update or replace them.

Meanwhile, U.S. officials from both parties are focused not on how we might avoid nuclear catastrophe but on showing how tough they can look against a revanchist Russia and its leader, Vladimir Putin. Summit meetings between White House and Kremlin leaders, once viewed as opportunities for peace, are now seen as dangerous temptations to indulge in Munich-style appeasement, the cardinal sin of statecraft. American policymakers worry more about “going wobbly,” as Margaret Thatcher once put it, than about a march of folly into inadvertent war. President Donald Trump’s suggestion that the United States and Russia might explore ways to manage their differences diplomatically has produced mostly head-scratching and condemnation.

In my more than 25 years of government experience working on Russia matters, I’ve seen that three misguided assumptions underlie how the United States got to this point.

The first is that American policymakers think that because neither side wants nuclear war, then such a war is very unlikely to occur. Russia would be foolish, we reason, to cross swords with the powerful U.S. military and risk its own self-destruction, and many Americans find it hard to imagine that modern cyber duels, proxy battles, information operations and economic warfare might somehow erupt into direct nuclear attacks. If the Cold War ended peacefully, the thinking goes, why should America worry that a new shadow war with a much less formidable Russia will end any differently?

But wars do not always begin by design. Just as they did in 1914, a vicious circle of clashing geopolitical ambitions, distorted perceptions of each other’s intent, new and poorly understood technologies, and disappearing rules of the game could combine to produce a disaster that neither side wants nor expects.

In fact, cyber technologies, artificial intelligence, advanced hypersonic weapons delivery systems and antisatellite weaponry are making the U.S.-Russian shadow war much more complex and dangerous than the old Cold War competition. They are blurring traditional lines between espionage and warfare, entangling nuclear and conventional weaponry, and erasing old distinctions between offensive and defensive operations. Whereas the development of nuclear weaponry in the Cold War produced the concept of mutually assured destruction and had a restraining effect, in the cyber arena, playing offense is increasingly seen as the best defense. And in a highly connected world in which financial networks, commercial operations, media platforms, and nuclear command and control systems are all linked in some way, escalation from the cyber world into the physical domain is a serious danger.

Cyber technology is also magnifying fears of our adversaries’ strategic intentions while prompting questions about whether warning systems can detect incoming attacks and whether weapons will fire when buttons are pushed. This makes containing a crisis that might arise between U.S. and Russian forces over Ukraine, Iran or anything else much more difficult. It is not hard to imagine a crisis scenario in which Russia cyber operators gain access to a satellite system that controls both U.S. conventional and nuclear weapons systems, leaving the American side uncertain about whether the intrusion is meant to gather information about U.S. war preparations or to disable our ability to conduct nuclear strikes. This could cause the U.S. president to wonder whether he faces an urgent “use it or lose it” nuclear launch decision. It doesn’t help that the lines of communication between the United States and Russia necessary for managing such situations are all but severed.

A related, second assumption American policymakers make is seeing the Russian threat as primarily a deterrence problem. The logic goes something like this: Wars often happen because the states that start them believe they can win, but the United States can disabuse a would-be aggressor of this belief through a show of force, thus deterring conflict. Indeed, Washington seems convinced that showing the Kremlin it will punish Russian transgressions—through toughened economic sanctions, an enhanced military posture in Europe and more aggressive cyber operations—is the best path to preserving peace.

But, when dealing with states that believe they are under some form of assault, focusing on deterrence can be counterproductive. Rather than averting aggression by demonstrating the will to fight back, America might be unintentionally increasing the odds of a war. To a great degree, this is the situation the United States already faces. Years of enlargement of NATO and perceived U.S. involvement in Russia’s internal affairs have convinced the Kremlin that America poses an existential threat. In turn, Russia’s meddling in the 2016 U.S. presidential election, coupled with a string of aggressions against its neighbors, have convinced Washington that Moscow is going for the West’s jugular.

The United States experienced this spiral phenomenon with Georgia in 2008. Convinced that Russia harbored aggressive designs on its southern neighbor, Washington policymakers accelerated U.S. military training in Georgia, openly advocated bringing Tbilisi into the NATO alliance and issued multiple warnings to Moscow against military action, believing this firm resolve would deter Russian aggression. In fact, it had the opposite effect. Russia grew increasingly alarmed by the prospect of Georgian membership in NATO, while Tbilisi felt emboldened to launch a military operation in the breakaway Georgian region of South Ossetia, which yielded an immediate and massive Russian military response.

### Russia War Terminals

#### U.S.-Russia nuclear war outweighs

Sebastian Farquhar 17, leads the Global Priorities Project (GPP) at the Centre for Effective Altruism, et al., 2017, “Existential Risk: Diplomacy and Governance,” 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.

### Ext --- Hybrid War Impacts --- Populism

#### Russian hybrid tactics support populist movements

Scott Lawless 20, MA in international security, University of Denver, Summer 2020, “American Grand Strategy for an Emerging World Order,” https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-14\_Issue-2/Lawless.pdf

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

#### That spells the death of multilateralism

Maya Kandel and Caroline Gondaud 19, Kandel is a French policy planner, in charge of U.S. and transatlantic issues, and associate researcher at Université Sorbonne Nouvelle Paris 3, Gondaud is a French policy planner, dealing with European issues, “POPULISM, THE EUROPEAN ELECTIONS, AND THE FUTURE OF E.U. FOREIGN POLICY,” War on the Rocks, 6/11/19, https://warontherocks.com/2019/06/populism-the-european-elections-and-the-future-of-e-u-foreign-policy/

Populism has never been so scrutinized, analyzed, and questioned. One aspect of populism, however, remains less studied: its impact on countries’ foreign policies and on their interstate relations in an international system in flux. There is no single “populist foreign policy,” but populism impacts foreign policies: It holds a particular vision of international relations, a vision that carries increasing weight amid today’s tumultuous attempts to redefine the international system.

In this article, we consider populism not just as a rhetorical expression of protest, but as a political project, both illustrating and responding to a crisis of politics within contemporary democracies — in short, as a phenomenon carrying a political vision. We view populism in foreign policy as offering an alternative view of international relations, one that articulates the main criticism of the contemporary international system, its institutions, and its operating rules — what is commonly referred to as the “liberal international order.” In this sense, populism in foreign policy also encompasses challenges to this order brought by “revisionist” states, especially Russia and China.

The recently concluded European Parliament elections highlighted the influence of populists, illustrating the fears and anxieties of many European citizens in a complicated global environment, but also their uncertainty about the role of the European Union in this context. Notably, although the European Union and the multilateralism associated with it have historically been a common target for populists, today’s populist factions seem to have shifted away from advocating outright removal from the union. Rather, they seem poised to sow discord and dysfunction in the European Parliament from the inside. In this way, the impact of populism on the European Union may be even more concerning: The movement can affect not only the union’s political agenda but also its functioning — and ultimately its overall relevance — by proving the populists’ major contention about the bankruptcy of multilateral institutions.

Populism and Foreign Policy: An Alternative Vision of International Relations

The defining characteristic of populism is that it creates a division between the people and “the system,” which can also be labeled the elite, bureaucracy, or the “deep state.” Populism can be defined as a reaction to the crises of political representation provoked by globalization, a reaction opposing the winners of globalization (“the elite”) to its losers, “the people.”

In foreign policy, this translates into a fundamental hostility to multilateralism — though it does not prevent some populist leaders, such as Hugo Chavez and Vladimir Putin, from trying to create alternative “nationalist international movements.” The latest illustration is the initiative by former Trump adviser Steve Bannon, who sought to unite all right-wing populist parties in Europe in a “European Movement.” Finally, anti-Americanism (“anti-imperialism,” in several parties’ terminology) characterizes all international populisms, right and left, European, Iranian, Latin American. America is seen as the ultimate embodiment of “the system,” and as such responsible for the theft of sovereignty from any given nation or people.

The United States figures prominently in the history of populism as the first country to have had a “Populist Party” or “People’s Party.” Historian Walter Russell Mead has linked the populism of the Tea Party to what he famously identified as the Jacksonian tradition, offering a more sophisticated portrayal of contemporary American populism and its consequences for foreign policy. This vision is characterized by its nationalism, defined in this case as unilateralism; militarism (which is not synonymous with interventionism); and hostility to multilateralism, the United Nations, free trade, and, more broadly, the American role of guarantor of the postwar international order. This Jacksonian populism defends a Westphalian vision of the world, in which nation-states enjoy full sovereignty, and rejects the role of the United States as “world policeman.”

The populist phenomenon affects all continents, but doesn’t produce the same results in terms of foreign policy. One example is Narendra Modi, the Indian prime minister who was just re-elected in a landslide. Modi is a populist who, like U.S. President Donald Trump, uses Twitter as a communication tool to create the illusion of a new modern direct democracy, but has pursued a traditional agenda for Indian foreign policy. In the United States and Europe, by contrast, populists, even when not in power, have affected not only the agenda but also the content of foreign policies. There is a transatlantic specificity, due to the power of the United States, the role of Russia, and exchanges between right-wing populists on both sides of the Atlantic. The result has been the emergence of “multipolarity without multilateralism, where the plurality of global players do not imply any kind of collective and cooperative agenda.”Still, most “populist foreign policies” express concern about eroding sovereignty and a willingness to affirm the demands of the people and the national interests of the state outside of established processes of global governance. Contemporary populism is thus not only a reaction to difficult economic times, but also expresses the fear of loss of control over national destinies — the tendency of state apparatuses to forgo popular control to reach international agreements.

European populism typifies this fear of loss of control over national destinies. The leitmotif of most populist parties in Europe aims at “taking back control:” control of borders, control of economy, control of culture and identity, combined with the persistent idea that the elites, both national and European (the so-called “bureaucrats from Brussels”), have stolen “the people’s sovereignty.” “Taking Back Control” had been the motto of the Brexit Campaign in 2016 and, significantly, was taken up by Theresa May in her major speeches after the referendum.

Populists in Europe want the return of borders, closed to immigration in particular but also to the flow of free trade. They tend to be hostile to all forms of multilateralism, as showed by an excellent study by the European Council on Foreign Relations on “the world according to Europe’s insurgent parties.” Recent developments point to an increased convergence in populist proposals from both ends of the political spectrum. Notably, on immigration, left-wing populists have made a sharp departure from the universalist ideals that until recently characterized their project: See, for instance, the evolution of left-wing populist parties in Italy (Movimiento 5 Stelle), Germany (Aufstehen), and France (France Insoumise). A comparison between the French far-right and far-left votes in the European Parliament on issues related to international trade is telling: On the ratification on CETA (the trade agreement between the European Union and Canada), or on TIPP (the trade agreement with the United States), the right-wing “Rassemblement National” and the left-wing “Front de Gauche” voted on the same line, illustrating both sides’ rejection of free trade.

The rise of populism has changed the terms of the European debate on major issues — in this way, populists already influence policies, including at the center. One example is French President Emmanuel Macron’s proposals in favor of a “Europe that unites to protect.” Macron has understood that the European Union is increasingly viewed as a machine to deregulate, open borders, enhance competition among states and individuals and — especially — erode national sovereignties. According to him, the best way to combat this perception is to demonstrate that the E.U. level is the relevant level to protect European citizens, far more than the national one. Accordingly, his project focuses on the concept of “European Sovereignty;” that is, the capacity to act as a global player and to promote the interests of member states more efficiently at the European level than at the individual country level.

Populists and the European Parliament: A Tipping Point?

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

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

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

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

#### Extinction

Manfred Kohler 20, founder of the Regulatory Institute, “The Need for Global Protections Against Existential Risks,” The Regulatory Review, 6/11/20, https://www.theregreview.org/2020/06/11/kohler-need-global-protections-against-existential-risks/

As bad as the social and economic impact of the new coronavirus is, it could be worse. It could kill everyone it infects. A scenario with such a fully fatal virus would be known as an existential risk because it would threaten all human life on the planet.

Global nuclear war and climate change might also be other possible existential risks—although some contention still exists over the degree to which these would annihilate the entire planet. But almost no one disputes that a meteorite crashing into Earth could do so by suddenly and drastically altering the climate. Furthermore, experts also agree that still more deadly pathogens—viruses and bacteria—could pose such an existential risk.

But what is currently missing in international law is an adequate mechanism to compel nations to cooperate to minimize or mitigate the harms from existential risks. In addition to efforts to strengthen national regulation of research and technology risks, countries also need to pursue the adoption of a multilateral agreement to address existential risks while separately working to insert existential risk clauses in existing international agreements.

The fact that some human-made existential risks, and even natural existential risks, might be minimized by human action, makes prudent the development of new international law aimed at addressing those risks. Admittedly, some of these risks are more amenable to national policy than others. The consequences of existential risks are, however, by necessity global and therefore demand a global policy response. Hubs of such international coordination exist for some risks, such as the World Health Organization, the International Atomic Energy Agency, and the United Nations’s Office for Disarmament Affairs. Unfortunately, these international agencies often lack sufficient power and scope to respond effectively to existential risks.

Governments around the world should give particular focus to developing stronger international policies on urgent existential risks. I define a risk as “urgent” if the cost of reducing the risk or strengthening resilience increases rapidly over time, or if the risk is about to become unmanageable altogether. One risk that fits that description is climate change, even though its character as existential risk has been contested.

### Ext --- Hybrid War Bad

#### Hybrid war with Russia causes extinction

Łukasz Kulesa 18, Research Director at the European Leadership Network, “Envisioning a Russia-NATO Conflict: Implications for Deterrence Stability,” EURO-ATLANTIC SECURITY REPORT, February 2018, https://www.jstor.org/stable/pdf/resrep17437.pdf

“Hybrid” scenarios: trigger for conflict?

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

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

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

Escalation: Can a NATO - Russia conflict be managed?

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

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

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

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

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

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

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

Conflict termination

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

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

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

#### Extinction

Max Fisher, American journalist and columnist based in Washington, D.C. in the field of political science and social science, June 29th 2015,“How World War III became possible: A nuclear conflict with Russia is likelier than you think” https://www.vox.com/2015/6/29/8845913/russia-war

VI. How it would happen: The fog of hybrid war In early 2015, Pew pollsters asked citizens of several NATO states the exact question that analysts and policymakers from Washington to Moscow are gaming out: "If Russia got into a serious military conflict with one of its neighboring countries that is our NATO ally, do you think our country should or should not use military force to defend that country?" The numbers from Western Europe were alarming: Among Germans, only 38 percent said yes; 58 percent said no. If it were up to German voters — and to at least some extent, it is — NATO would effectively surrender the Baltics to Russia in a conflict. This poll is even worse than it looks. It assumes that Russia would launch an overt military invasion of the Baltics. What would actually happen is something far murkier, and far more likely to leverage European hesitation: the playbook from Ukraine, where Russia deployed its newly developed concepts of postmodern "hybrid war," designed to blur the distinction between war and not-war, to make it as difficult as possible to differentiate grassroots unrest or vigilante cyberattacks from Russian military aggression. Putin may already be laying the groundwork. In March of 2014, shortly after Russia had annexed Crimea, Putin gave a speech there pledging to protect Russians even outside of Russia, which many took as a gesture to the substantial Russian minorities in the Baltics. Then, in October, Putin warned that "open manifestations of neo-Nazism" had "become commonplace in Latvia and other Baltic states" — repeating the language that he and Russian state media had earlier used to frighten Russian speakers in Ukraine into taking up arms. This April, several Russian outlets issued spurious reports that Latvia was planning to forcibly relocate ethnic Russians into Nazi-style ghettos — an echo of similar scaremongering Russian propaganda broadcast in the runup in Ukraine. Martin Hurt, a former senior official of the country's defense ministry, warned that his country's ethnic Russian minority could be "receptive to Kremlin disinformation." Moscow, he said, could generate unrest "as a pretext to use military force against the Baltic states." In early 2007, Estonia's parliament voted to relocate a Soviet-era military statue, the Bronze Soldier, that had become a cultural symbol and annual rallying point for the country's ethnic Russians. In response, Russian politicians and state media accused the Estonian government of fascism and Nazi-style discrimination against ethnic Russians; they issued false reports claiming ethnic Russians were being tortured and murdered. Protests broke out and escalated into riots and mass looting. One person was killed in the violence, and the next day hackers took many of the country's major institutions offline. Russia could do it again, only this time gradually escalating further toward a Ukraine-style conflict. NATO is just not built to deal with such a crisis. Its mutual defense pledge, after all, rests on the assumption that war is a black-and-white concept, that a country is either at war or not at war. Its charter is from a time when war was very different than it is today, with its many shades of gray. Russia can exploit this flaw by introducing low-level violence that more hawkish NATO members would consider grounds for war but that war-averse Western European states might not see that way. Disagreement among NATO's member states would be guaranteed as they hesitated over where to declare a moment when Russia had crossed the line into war. Meanwhile, Russian state media, which has shown real influence in Western Europe, would unleash a flurry of propaganda to confuse the issue, make it harder to pin blame on Moscow for the violence, and gin up skepticism of any American calls for war. Germany, which is widely considered the deciding vote on whether Europe would go to war, would be particularly resistant to going to war. The legacy of World War II and the ideology of pacifism and compromise make even the idea of declaring war on Russia unthinkable. German leaders would come under intense political pressure to, if not reject the call to arms, then at least delay and negotiate — a de facto rejection of NATO's collective self-defense. In such a scenario, it is disturbingly easy to imagine how NATO's European member states could split over whether Russia had even crossed their red line for war, much less whether to respond. Under a fog of confusion and doubt, Russia could gradually escalate until a Ukraine-style conflict in the Baltics was foregone, until it had marched far across NATO's red line, exposing that red line as meaningless. But the greatest danger of all is if Putin's plan were to stumble: By overreaching, by underestimating Western resolve to defend the Baltics, or by starting something that escalates beyond his control, it could all too easily lead to full-blown war. "That kind of misperception situation is definitely possible, and that’s how wars start," Saideman said, going on to compare Europe today with 1914, just before World War I. "The thing that makes war most thinkable is when other people don’t think it’s thinkable."

#### Hybrid warfare triggers rapid nuclear escalation – defense is wrong

Łukasz Kulesa, Research Director at the European Leadership Network, “Envisioning a Russia-NATO Conflict: Implications for Deterrence Stability”, Feb 2018, https://www.europeanleadershipnetwork.org/wp-content/uploads/2018/02/180213-Envisioning-a-Russia-NATO-Conflict.pdf

“Hybrid” scenarios: trigger for conflict? One can envisage a number of “hybrid” scenarios of Russia-NATO conflict where operations which started in the cyber, economic, criminal, or “active measure” domains, below the threshold of conflict, trigger a military response or are followed by the physical use of force. As noted in the discussion on the definitions of a conflict, the threshold between crisis and military conflict may not be explicitly stated or otherwise clear to all sides; and it may also be ignored during a crisis. This aspect is especially relevant in the current period of increased interference in the internal affairs of NATO countries attributed to Russia and of the high volume of information ‘warfare’ between Russia and NATO countries. Russia remains vigilant about foreign interference in its internal affairs and the threat of subversion leading to a severe destabilization of the regime. In the past, Moscow has made accusations about foreign sponsorship of Chechen and radical Islamic terrorists targeting Russia, and has alleged the existence of training camps on the territories of NATO states for activists planning colour revolutions in Ukraine and Belarus. In the extreme circumstances of a crisis, if the Russian leadership became convinced that a non-military campaign against it (which might also involve cyber activities and what Russia calls attempts to instigate colour revolutions) had intensified, this could lead to a military response. “One needs to be wary of interpreting all disturbing developments as part of a grand Russian plan.” With regards to NATO, some of its members’ views mirror the Russian assessment that we are already in a state of conflict, in which the boundary between peace and war is blurred, and that their defences are being actively attacked through nonmilitary means. They are thus concerned about a scenario in which Russia initiates an attack that moves swiftly from non-military to military means. This scenario should be not dismissed. At the same time, one needs to be wary of interpreting all disturbing developments as part of a grand Russian plan culminating in a provocation or use of force. So there should be prudence before any country presses the “panic button” at the national or NATO / European Union level. There should also be close analysis of early warning indicators related to the gravity, intensity and diversity of incidents and to connections between them. The overall political context and state of the RussiaNATO relationship would also be important: what would be the political and strategic reasons for Russia to move from sub-threshold to abovethreshold activities? Individual NATO countries would have a decisive role in how some of the “hybrid” scenarios would play out. An Ally can choose to play down or up the importance of certain developments and incidents; it can seek NATO and/or EU support, decide to respond individually (including through actions that are escalatory), or use a mix of both approaches. The Ally’s overall reputation and patterns of international behaviour can matter for determining whether its “frontline” intelligence and assessments are to be trusted. But given the danger of alliance entrapment, NATO also needs to have multiple channels for corroborating the evidence and assessing developments. Escalation: Can a NATO - Russia conflict be managed? Once a conflict was under way, the “fog of war” and rising unpredictability would inevitably set in, complicating the implementation of any predetermined theories of escalation, deescalation and inter-conflict management. The actual dynamics of a conflict and the perceptions of the stakes involved are extremely difficult to predict. Simulations and table-top exercises can give only limited insights into the actual decisionmaking processes and interactions. Still, Russian military theorists and practitioners seem to assume that a conflict with NATO can be managed and controlled in a way that would bring it to a swift end consistent with Russian aims. The Russian theory of victory would seek to exploit weak points in an Alliance war effort. Based on the conviction that democracies are weak and their leaders and populations are risk-averse, Russia may assume that its threats of horizontal or vertical escalation could be particularly effective. It would also try to bring home the notion that it has much higher stakes in the conflict (regime survival) than a majority of the NATO members involved, and thus will be ready to push the boundaries of the conflict further. It would most likely try to test and exploit potential divisions within the Alliance, combining selective diplomacy and activation of its intelligence assets in some NATO states with a degree of selectivity in terms of targets of particular attacks. Any NATO-Russia conflict would inevitably have a nuclear dimension. The role of nuclear weapons as a tool for escalation control for Russia has been thoroughly debated by experts, but when and how Russia might use (and not merely showcase or activate) nuclear weapons in a conflict remains an open question. Beyond catch phrases such as “escalate to de-escalate” or “escalate to win” there are a wider range of options for Russian nuclear weapon use. For example, a single nuclear warning shot could be lethal or non-lethal. It could be directed against a purely military target or a military-civilian one. Detonation could be configured for an EMP effect. A “false flag” attack is also conceivable. These options might be used to signal escalation and could significantly complicate NATO’s responses. Neither NATO nor its member states have developed a similar theory of victory. Public NATO documents stipulate the general goals for the Alliance: defend against any armed attack and, as needed, restore the full sovereignty and territorial integrity of member states. It is less clear how far the Alliance would be willing to escalate the conflict to achieve these goals, and what mechanisms and means it would use while trying to maintain some degree of control over the conflict. The goals and methods of waging a conflict with Russia would probably have to be limited in order to avoid a massive nuclear exchange. Such limitations would also involve restrictions on striking back against targets on Russian territory. But too narrow an approach could put too much restraint on NATO’s operations: the Russian regime’s stability may ultimately need to be threatened in order to force the leadership into terminating the conflict. NATO would thus need to establish what a proportional self-defence response to Russian actions would involve, and to what extent cyber operations or attacks against military targets in quite different parts of Russia would be useful as tools of escalation to signal NATO’s resolve. Moreover, individual NATO Allies, especially those directly affected by Russia’s actions, might pursue their individual strategies of escalation. With regards to the nuclear dimension in NATO escalation plans, given the stakes involved, this element would most likely be handled by the three nuclear-weapon members of the Alliance, with the US taking the lead. The existence of three independent centres of nuclear decision-making could be exploited to complicate Russian planning and introduce uncertainty into the Russian strategic calculus, but some degree of “P3” dialogue and coordination would be beneficial. This coordination would not necessarily focus on nuclear targeting, but rather on designing coordinated operations to demonstrate resolve in order to keep the conflict below the nuclear threshold, or bring it back under the threshold after first use. Relying on concepts of escalation control and on lessons from the Cold War confrontation might be misleading. The circumstances in which a Russia -NATO conflict would play out would be radically different from the 20th century screenplay. Moreover, instead of gradual (linear) escalation or salami tactics escalation, it is possible to imagine surprizing “leap frog” escalation, possibly connected with actions in different domains (e.g. a cyberattack against critical infrastructure). Flexibility, good intelligence and inventiveness in responding to such developments would be crucial

#### Most likely scenario for escalation

Bert Chapman, Government Information, Political Science, and Economics Librarian and Professor of Library Science at Purdue University, “Recent U.S. and International Assessment of Baltic Security Developments”, Security and Defence Quarterly ISSN 2300-8741 eISSN 2544-994X 2019 September Volume 26 Number 4, https://securityanddefence.pl/Recent-U-S-and-International-Assessment-of-Baltic-Security-Developments,112252,0,2.html

Various U.S. military branches also recognize the importance of the Baltic to emerging U.S. national security interests, with this being reflected in their analyses of European geopolitical trends since 2014. A 2016 compilation published by National Defense University Press noted that Russian leaders could engage in military intervention to “protect” Russian minorities in neighboring states such as the Baltics, that Russian territorial seizure of territory in the Baltics would impose a military escalation burden on the United States including using nuclear weapons, that NATO countries must strike a delicate balance between reassuring Baltic allies and deterring Russian miscalculation while also calming tensions, and noting that Russia has recently deployed short-range SS-26 Iskander ballistic missiles to Kaliningrad adjacent to the Baltics. This work asserted that Russian attempts to destabilize the Baltics with a Crimean variant hybrid operation could result in NATO’s Article 5 being invoked, that Russia could overrun the Baltic countries within 48-72 hours but with the price of prompting a NATO response that Moscow could not maintain and shake Finnish and Swedish neutrality, that NATO battalions should have forward-based ground units possessing short-range air defense capability and the ability to eliminate offensive Russian military action from Putin’s strategic calculus, that Russian air defenses at Kaliningrad, Severomorsk, and St. Petersburg cover airspace encompassing and endangering Finland, the Baltic States, northern and southern Sweden, northern Norway, Poland, and eastern Germany, and the belief of Nordic states that hybrid war in the Baltics is the most likely regional flashpoint between the West and Russia (Charting a Course: Strategic Choices for a New Administration 2016, pp. 4, 103, 209, 238, 240-241, 360).

### Ext --- Democracy Impacts

#### Democratic norms key to check escalating wars involving Iran, Russia, Saudi Arabia, Israel, and the US. COVID’s placed all of this on the brink.

Nanda ‘20

Biren Nanda was the Ambassador of India to the Republic of Indonesia, Timor Leste and ASEAN from 2008 to 2012 and High Commissioner of India to Australia from 2012 to 2015. He has previously served as as a diplomat in Indian Missions in Singapore, Beijing, Shanghai, Washington, D.C., and Tokyo. He was the Consul General of India in Shanghai from 1996–2000, Deputy Chief of Mission in the Embassy of India in Tokyo from 2000–2004. He was a Senior Fellow in the Delhi Policy Group from 2016 to 2019. The Geopolitical Consequences of a pandemic – The Interpreter -Published 16 Jun 2020 - - https://www.lowyinstitute.org/the-interpreter/geopolitical-consequences-pandemic

A once-in-a-century pandemic has the potential to unleash an epochal geopolitical churn. There are major risks from potential conflict triggered by tensions between Saudi Arabia and Iran or from a conflict of interests between the US and Russia in the Middle East. Iran might exacerbate existing tensions by moving perceptibly closer towards a nuclear weapons capability or by activating its proxies as a response to extreme stress from the sanctions and the pandemic. Such a conflict might draw in the US and Israel, leading to a wider conflagration.

As the demonstrations in the US are echoed other countries, there will likely be different outcomes, depending upon the nature of the political system in place. Democracies are less likely to use force and more likely to introduce changes to address underlying causes. Authoritarian regimes, which suffer from a crisis of legitimacy, are more likely to use excessive force and less likely to address underlying issues, out of a fear of unleashing a chain of events they would be unable to control.

#### Liberal democracy solves existential impacts but US democratic norm-setting is vital

Kasparov 17 ---- Garry, chairman for the Human Rights Foundation, “Democracy and Human Rights: The Case for U.S. Leadership,” Testimony before the Subcommittee on Western Hemisphere, Transnational Crime, Civilian Security, Democracy, Human Rights, and Global Women's Issues, 2/16, <https://www.foreign.senate.gov/imo/media/doc/021617_Kasparov_%20Testimony.pdf> \*\*Modified for ableist language

The Soviet Union was an existential threat, and this focused the attention of the world, and the American people. There existential threat today is not found on a map, but it is very real. The forces of the past are making steady progress against the modern world order. Terrorist movements in the Middle East, extremist parties across Europe, a ~~paranoid~~ tyrant in North Korea threatening nuclear blackmail, and, at the center of the web, an aggressive KGB dictator in Russia. They all want to turn the world back to a dark past because their survival is threatened by the values of the free world, epitomized by the United States. And they are thriving as the U.S. has retreated. The global freedom index has declined for ten consecutive years. No one like to talk about the United States as a global policeman, but this is what happens when there is no cop on the beat.

American leadership begins at home, right here. America cannot lead the world on democracy and human rights if there is no unity on the meaning and importance of these things. Leadership is required to make that case clearly and powerfully. Right now, Americans are engaged in politics at a level not seen in decades. It is an opportunity for them to rediscover that making America great begins with believing America can be great.

The Cold War was won on American values that were shared by both parties and nearly every American. Institutions that were created by a Democrat, Truman, were triumphant forty years later thanks to the courage of a Republican, Reagan. This bipartisan consistency created the decades of strategic stability that is the great strength of democracies. Strong institutions that outlast politicians allow for long-range planning. In contrast, dictators can operate only tactically, not strategically, because they are not constrained by the balance of powers, but cannot afford to think beyond their own survival. This is why a dictator like Putin has an advantage in chaos, the ability to move quickly. This can only be met by strategy, by long-term goals that are based on shared values, not on polls and cable news.

The fear of making things worse has ~~paralyzed~~ [prevented] the United States from trying to make things better. There will always be setbacks, but the United States cannot quit. The spread of democracy is the only proven remedy for nearly every crisis that plagues the world today. War, famine, poverty, terrorism–all are generated and exacerbated by authoritarian regimes. A policy of America First inevitably puts American security last.

#### Democracy is a conflict filter – consolidation caps escalation of intra and interstate war

Albright 17 [Madeline Albright, currently a professor of International Relations at Georgetown University's School of Foreign Service, PhD from Columbia University, former US Secretary of State, Mehdi Jomaa is a Tunisian engineer and was the acting Prime Minister of Tunisia from 29 January 2014 to 6 February 2015 September 17 https://www.brookings.edu/wp-content/uploads/2017/09/fp\_20170912\_liberal\_democracy\_\_peace\_security.pdf]

Given these trends, the Community of Democracies has a new imperative: to demonstrate to itself and to the world that the core values of democracy and human rights are not only goods in and of themselves, but also the most promising path to peace and security in an increasingly turbulent world. The report we present here to their representatives and to all engaged citizens from civil society, parliaments, businesses, and youth seeks to show that the norms and practices of liberal democracy and human rights do in fact lead to better security outcomes over time and across multiple dimensions.

Based on a year-long research project gathering the empirical evidence on the relationship between democracy and security, and on accumulated experience with combating the scourge of extremist violence and terrorism, we can say with confidence that liberal democracy, when allowed to consolidate and flourish, is the best path toward achieving domestic and international peace and security. A series of policy briefs covering a range of security-related issues from civil war to digital technology were commissioned by the Community of Democracies’ Permanent Secretariat and prepared by the Brookings Institution’s Foreign Policy Program and the Institute for Security Studies.1 This research, which was complemented by consultations with policymakers, academic experts, and civil society during workshops held in India, South Africa, Mexico, Brazil, Poland, Sweden, and the United States, examines these linkages in substantial detail.

The evidence affirms the standard observation that democracies do not go to war against one another. But the data also prove that democracies are less likely to spawn internal armed conflicts or experience deadly terrorism because they channel dissent through nonviolent means and manage violence through respect for the rule of law and human rights. Authoritarian and failed states, on the other hand, are more likely to experience intra and interstate conflict, generate refugees, hinder women’s equality, and harbor violent extremists.

The research also shows that states at intermediate stages of democratization—hybrid regimes with mixed features of democracy and autocracy, elite-driven patronage systems, and/or weak institutions—are generally the most vulnerable to insecurity, whether from violent crime, terrorism, or entrenched poverty. These are states where there is both weak institutional capacity and weak political legitimacy, which together contribute to a breakdown in the social contract between citizens and the government. This report argues that to foster domestic and international security, and to address the underlying drivers of violent extremism, this social contract must be repaired. It is essential, therefore, to adopt strategies to institutionalize democratic governance, inclusive politics, and human rights in fragile states. Civil society—as independent participants, monitors, and critics of our democratic institutions—are also critical ingredients to any strategy for peace.

#### Democratic consolidation solves inter and intra-state escalation and miscalc

Albright 17 [Madeline Albright, currently a professor of International Relations at Georgetown University's School of Foreign Service, PhD from Columbia University, former US Secretary of State, Mehdi Jomaa is a Tunisian engineer and was the acting Prime Minister of Tunisia from 29 January 2014 to 6 February 2015 September 17 https://www.brookings.edu/wp-content/uploads/2017/09/fp\_20170912\_liberal\_democracy\_\_peace\_security.pdf]

Scholars and practitioners of diplomacy and international relations have long considered the proposition, articulated by theorists like Immanuel Kant, that societies governed democratically are more inclined to avoid armed conflict with each other. The accumulated evidence, in fact, remains strong that established liberal democracies do not go to war against each other. Leaders accustomed to the negotiated trade-offs of shared power and accountable to citizens through free, fair, and periodic elections, embedded in constitutional systems with independent judiciaries, free media, and civilian control of the military, have built-in checks against belligerence toward similar liberal democratic countries. Healthy democracies are better at credibly signaling their intentions to their citizens and to other states. Such transparency reduces the likelihood of miscalculations and is more likely to lead to peaceful settlements before the onset of direct military conflict. At least in the realm of interstate conflict, the empirical record suggests that a world of stronger democracies will be more peaceful.

With the decline of interstate war over the last many decades, particularly after the end of the Cold War, the international community has struggled instead with the persistence of internal armed conflicts of varying intensities, some of which also have international dimensions. Since the fall of the Berlin Wall in 1989, according to the Uppsala Conflict Data Program (UCDP), the number of civil wars has increased with a significant uptick since 2010. Notably, 70 conflicts involving nonstate actors were recorded in 2015, dwarfing the yearly average of 35 between 1989 and 2015. Similarly, armed conflicts between governments and rebel groups increased from 41 in 2014 to 50 in 2015—making it the second highest tally since 52 were recorded in 1991. Factors contributing to internal conflict, including defining elements of democracy and human rights such as elections and political repression, are complex and diverse. The historical record shows, however, that countries with strong records of respect for democracy and human rights are far less likely to experience civil wars than hybrid regimes.2

Stronger democracies are less prone to civil war for at least two reasons. First, at the elite level, healthy democratic institutions and regular electoral processes create incentives for political participation by a wide range of ideological actors at relatively low cost, while taking up arms involves much higher costs. Second, rebel groups are less likely to find support among citizens if popular grievances are being met through peaceful and credible political processes. Strong autocracies also tend to avoid civil wars because of the repression and cooptation employed by their state institutions.

#### Democracy solves WMD conflict

Halperin 11 (Morton H., Senior Advisor – Open Society Institute and Senior Vice President of the Center for American Progress, “Unconventional Wisdom – Democracy is Still Worth Fighting For”, Foreign Policy, January / February, <http://www.foreignpolicy.com/articles/2011/01/02/unconventional_wisdom?page=0,11>)

As the United States struggles to wind down two wars and recover from a humbling financial crisis, realism is enjoying a renaissance. Afghanistan and Iraq bear scant resemblance to the democracies we were promised. The Treasury is broke. And America has a president, Barack Obama, who once compared his foreign-policy philosophy to the realism of theologian Reinhold Niebuhr: "There's serious evil in the world, and hardship and pain," Obama said during his 2008 campaign. "And we should be humble and modest in our belief we can eliminate those things." But one can take such words of wisdom to the extreme-as realists like former Secretary of State Henry Kissinger and writer Robert Kaplan sometimes do, arguing that the United States can't afford the risks inherent in supporting democracy and human rights around the world. Others, such as cultural historian Jacques Barzun, go even further, saying that America can't export democracy at all, "because it is not an ideology but a wayward historical development." Taken too far, such realist absolutism can be just as dangerous, and wrong, as neoconservative hubris. For there is one thing the neocons get right: As I argue in *The Democracy Advantage*, democratic governments are more likely than autocratic regimes to engage in conduct that advances U.S. interests and avoids situations that pose a threat to peace and security. Democratic states are more likely to develop and to avoid famines and economic collapse. They are also less likely to become failed states or suffer a civil war. Democratic states are also more likely to cooperate in dealing with security issues, such as terrorism and proliferation of weapons of mass destruction. As the bloody aftermath of the Iraq invasion painfully shows, democracy cannot be imposed from the outside by force or coercion. It must come from the people of a nation working to get on the path of democracy and then adopting the policies necessary to remain on that path. But we should be careful about overlearning the lessons of Iraq. In fact, the outside world can make an enormous difference in whether such efforts succeed. There are numerous examples-starting with Spain and Portugal and spreading to Eastern Europe, Latin America, and Asia-in which the struggle to establish democracy and advance human rights received critical support from multilateral bodies, including the United Nations, as well as from regional organizations, democratic governments, and private groups. It is very much in America's interest to provide such assistance now to new democracies, such as Indonesia, Liberia, and Nepal, and to stand with those advocating democracy in countries such as Belarus, Burma, and China. It will still be true that the United States will sometimes need to work with a nondemocratic regime to secure an immediate objective, such as use of a military base to support the U.S. mission in Afghanistan, or in the case of Russia, to sign an arms-control treaty. None of that, however, should come at the expense of speaking out in support of those struggling for their rights. Nor should we doubt that America would be more secure if they succeed.

### Ext --- Hybrid War Bad --- Secessionism

#### Russian cyberwar causes secessionism, undermines European democracy, and destroys NATO.

Frydenborg 20 --- Brian Frydenborg, MS in Peace Operations from George Mason University's School of Public. BA from Washington and Lee University in Politics and History. Former intern in the United States Senate. "The History of Russia’s Cyberwarfare Against NATO Shows It Is Time to Add to NATO’s Article 5". Real Context News (RCN). 12-24-2020. https://realcontextnews.com/the-history-of-russias-cyberwarfare-against-nato-shows-it-is-time-to-add-to-natos-article-5/

The NATO Alliance has served for over seventy years not only as a foundation of preventing armed attacks from Russia and other major powers against most of Europe and North America, but also a foundation of one of the most peaceful and prosperous eras in world history. But there is one major type of warfare that has been hitting NATO member states intensely for years and increasingly so: cyberwarfare. And virtually all cybercampaigns of this cyberwarfare have been waged by Russia, part of Russian President Vladimir Putin’s overall war against the West, especially NATO but also even Western democracy.

Apart from some Chinese hacking/cyberespionage known to have begun at least by 2003, the first two serious cyberassaults (in these cases carried out much more so as part of geopolitical cyberwarfare campaigns) were Hezbollah’s and Israel’s surprising cyberattacks against each other during their 2006 war and Russia’s less-surprising but far larger cybercampaign against NATO-member Estonia in 2007, just three years after it had joined the Alliance. It was not long after that when it became clear Russia was absolutely a bad-faith actor with which we have needed, since the last years of the George W. Bush Administration and through the Obama and Trump Administrations, to take a much tougher stance, as I have argued before.

Unsurprisingly, then, the two countries that have led in cyberwarfare since are Russia and China, the first being the weaker of the two but also NATO’s (and America’s) clearest top state enemy and the second being the overall stronger of the two, but more restrained and America’s clearest top state rival for global power and influence. Though China has conducted its own massive hacking and espionage operations (not uncommon among major powers) and has its own influence operations, it is Russia that has without question been the dominant aggressor with acts far more hostile than hacking operations focused mainly on espionage. In fact, Russia is unique among major powers in carrying out significant acts of hostile cyberwarfare beyond espionage ever since its Estonia campaign. And while espionage against NATO states is bad for any of those states, espionage has long been viewed as separate from acts of war and should remain in a different category from acts of war in all but the most extreme of cases, a select level in which the latest Russian cybercampaign (detected to be only espionage so far even if at a historic level) seems begging to be included.

Since the Estonia campaign, Russia become dramatically more aggressive against NATO, often skillfully manipulating nationalisms (as I discussed recently) and flooding NATO member states with cyberwarfare, with election interference and boosting secessionism as common features. Notable cybercampaigns have been directed at the United States, the United Kingdom (including the Scottish independence and Brexit referenda), Germany, France, Italy, Spain, the Netherlands, Bulgaria, Norway, Estonia, Latvia, Lithuania, the Czech Republic, Canada, Turkey, Denmark, Romania, Poland, Slovakia, Montenegro, and even (North) Macedonia, unsurprisingly focused there on preventing its recent accession to NATO (and these do not even get into campaigns carried out beyond NATO territory).

These cybercampaigns involve thousands of Russian government paid-trolls and Kremlin-created bots operating thousands of fake accounts that create millions of Tweets, comments, and posts. And the way these operations tend to work is by promoting politicians and political parties coopted or compromised by or even favorable to Russia and Putin’s agenda and slamming their opponents or anyone critical of Russia and willing to stand up to Putin.

Many of the parties getting the most help (including funding) from Russia exhibit the same hackneyed brand of thoroughly boring right-wing ethnonationalism of the type embraced by Putin’s own United Russia party, which has in recent years forged alliances with several major political parties in Europe, including in major NATO states Italy, Germany, and France (and there are suspicions about the UK, where details of this remain redacted in the recent British parliamentary Russia report). Similar political interference efforts are known to extend beyond NATO countries.

Using its primary hybrid mix of disinformation, hacking, and propaganda, and with a network that combines top Kremlin figures, shadowy Russian government operatives, oligarchs in Putin’s pocket, and various state-linked media “outlets,” these operations have had far more effect than most people in NATO countries realize: helping to sway the views of many millions and dramatically distorting public discussion, politics, and policies in countries on everything from Ukraine (see the Hunter Biden “story,” for years a Russian disinformation campaign) and Syria to sanctions and even the current coronavirus pandemic. This model is skilled at preying on ignorance and confirmation bias to turn media outlets and citizens alike in these NATO states into Kremlin allies, whether as unwitting “useful idiots” or witting Fausts. From Donald Trump and France’s Marine Le Pen and Brexit champion Nigel Farage to Fox News’ all-stars and “contrarian” journalists Glenn Greenwald and Matt Taibbi, for a variety of reasons, extremists not only on the right but also on the left embrace or parrot Kremlin talking points and narratives after years of these effective influence operations, shaping debate from both within the halls of government power and newsrooms, corrupting and bending the debate to Russia’s ends. Russian disinformation is thus vastly amplified and passed on further as misinformation by the duped and again as disinformation by the corrupted so that public opinion, media, and even laws and policies become more anti-NATO, more anti-EU, more anti-American, more pro-secession, more pro-Russia, more pro-Putin as a result. And when the Kremlin’s candidates win, they and their allies may spout Russian disinformation to suit their ends, as former FBI counterintelligence agent Asha Rangappa explains is the case with the Trump Administration. They can also can move to obstruct efforts to both investigate Russian infiltration and hold Russia accountable for its cyberwarfare, with clear and indisputable examples of late from the Trump Administration and Boris Johnson’s UK government as illustrated clearly in the Mueller report and the aforementioned British parliamentary report, respectively. Even when the Kremlin’s chosen do not win, these Russian operations still manage to weaken their victorious opponents and skew political atmosphere.

All this has been the case to varying degrees from Washington to Rome, from London to Berlin, weakening NATO and its ability to collectively defend itself. Over time, the degree to which the pendulum has swung to more pro-Russian positions and people has been nothing short of remarkable and very much in part because of Russia’s concerted cyberwarfare effort. And all this further divides the Alliance and even member states’ own societies internally, which itself is also a major goal of Russia’s.

#### European secessionist conflicts go nuclear.

Barry Blechman et al. 15. Dr. Barry M. Blechman is co-founder and a Distinguished Fellow of the Stimson Center. Alex Bollfrass, Former Nonresident Fellow. Laicie Heeley, Former Fellow with Stimson’s Budgeting for Foreign Affairs and Defense program "Reducing The Risk Of Nuclear War In The Nordic/Baltic Region. Stimson Center". Stimson Center. 12-15-2015. https://www.stimson.org/2015/reducing-risk-nuclear-war-nordicbaltic-region-0/

Europe is currently experiencing escalating political and military tensions that are rekindling fears of war between Russia and NATO. Any such conflict would inherently include a risk of nuclear weapons use. The Stimson Center, partnered with Project High Hopes, is examining the results of such nuclear exchanges and, more importantly, developing initiatives to avoid such catastrophes.

Vladimir Putin has revealed that he was prepared to use nuclear weapons in the Ukraine crisis and would protect ethnic Russian populations through any means necessary. There are significant ethnic Russian populations in Estonia and Latvia with a history of disagreements and some conflict with the national governments. Any armed conflict between a Russian secessionist movement and a Baltic government could provide Russia an excuse for military intervention, which could easily devolve into a war with NATO and a risk of nuclear use.

Illustratively, one could imagine a scenario we call Escalation in Estonia, beginning with the seizure by pro-Russian rebels of local government buildings. Responding to an Estonian request, NATO mobi-lizes against the rebels, and Russian troops move across the border. Desperate to end the conflict before more NATO forces can arrive, in conformity with its doctrine “escalate to deescalate,” the Russians launch two nuclear-armed missiles on NATO forces. NATO, in turn, responds with two nuclear bombs delivered by US B-2 bombers on Russian military headquarters within Estonia. As a result, Tallinn is largely destroyed and nearly 100,000 civilians and military service men and women could be expected to die as a result of the conflict and its aftermath.

## Attribution Add-On

### Add-On --- De-escalation

#### Attribution is key to de-escalation and prevents accidental war

Goel 19 --- Sanjay Goel, Professor in the School of Business at the University at Albany, SUNY (UAlbany) , “How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race”, Connections QJ 19, no. 1 (2020): 87-95, https://procon.bg/system/files/19.1.08\_goel\_cyber\_warfare\_attribution.pdf

The prevalence and risk of cyberattacks continue to rise in parallel with our increasing reliance on the Internet for systems of economic production, supply and distribution chains, finance, power, transportation, and other critical infrastructures. Cyber warfare is becoming the next serious threat to national security 1 that can impact not only life and property but also financial markets. 2 According to the Centre for Strategic and International Studies (CSIS), the total number of cyber-attacks against government agencies, defense and high-tech companies, or economic crimes with losses of over one million dollars rose from 21 in 2014 to 58 in 2017. 3 This CSIS list, built on open-source data only, depicts a worrisome trend of rising cyberattacks attributed to state-sponsored groups acting against the political or economic interests of other states.

In testimony delivered to the US Armed Services Committee in January 2017, James Clapper, former US Director of National Intelligence, stated that more than 30 nations were developing offensive cyberattack capabilities as of late 2016. He further opined that “the proliferation of cyber capabilities coupled with new warfighting technologies will increase the incidence of standoff and remote operations, especially in the initial stages of conflict.”4 As policymakers warn of the dangers of cyber conflicts and exalt the virtues of cyber peace, most states consider cyberspace the fifth operational domain, with equal, or perhaps greater future importance to the traditional domains of land, sea, air, and space. State military and intelligence agencies continue to conduct cyber espionage and covert attacks on computer systems and networks in pursuit of strategic political or military objectives, both before and during conflicts. Yet, there is limited transparency on how states consider using their cyber capabilities, as only a few countries have publicly announced their cyber doctrines and underlying strategies. For example, McAfee, the global computer security software company, estimated in 2007 that over 120 countries were working on cyber commands, 5 whereas Dévai listed 114 countries that, as of 2013, were developing civilian and military cyber capabilities, policies, doctrines and organizations at varying levels of maturity or focus. 6 Considering that many of the officially declared ‘defensive’ cyber capabilities could easily be deployed in offensive cyber operations, as well as the fact that data assembled by cyber experts is often based on publicly available information only, it is not surprising that such estimations vary, and that the true state of cyber warfare preparedness and capabilities worldwide is difficult to ascertain. This high degree of uncertainty, when coupled with the low cost and easy acquisition of cyber weapons, ample and growing target selection, and multiplicity of types of attacks that may go unnoticed for a long time, contributes to a prevailing state of cyber insecurity in the international community. The problem is further exacerbated by the fact that there is no commonly accepted terminology of critical cyber terms (e.g., ‘cyber’ vs. ‘information’ security) among key cyber actors, which affects the ability of most likely strategic adversaries to establish common ground as a prerequisite for dialogue.

Cyber warfare is a broad term that refers to actions by nation-state actors (or other international organizations with mala fide intentions) to use hacking tools to achieve military objectives in another country. The tools for hacking are varied and can include malicious software, denial-of-service attacks, social engineering, fake news, and malicious insiders as well as tools for camouflaging identify of hackers or misdirecting attribution. The objectives could be tactical or strategic. The tactical objectives could be degrading the capability of an adversary both in the battlefield or in weapons development (e.g., Stuxnet) or espionage to collect intelligence. The strategic objectives could be the use of soft power such as propaganda to influence public opinion for regime change or altering the political outcomes of the election or hard power by leaving dormant malicious software in critical infrastructure to leverage during times of conflict.

The boundary between conventional and cyber war is blurring as conventional defensive and offensive capabilities increasingly use the Internet for command, control, communications, and intelligence, making information and communication infrastructures and networks both the targets and vehicles of military attacks. At the same time, the Internet has become the communications backbone required for the functioning of modern societies and economic systems. Therefore, the nature and means of the military defense of these systems also have to change and become more flexible to adapt to these emerging threats. Above all, the nascent cyber defense mechanism of any state must be able to provide the national political leadership with answers regarding a number of critical questions: What is the origin of a cyberattack; where did it come from? Who is responsible? What is the recommended course of action, or response?

Attribution

Attribution of cyberattacks is very important, especially to justify retaliatory actions against the perpetrators and prevent accidental retaliation against innocent targets. The entire domain of cyber norms and confidence-building measures is centered on visibility, i.e., being able to identify perpetrators of attacks and being able to ascertain adversarial strength. In the absence of such verification, the suspicion remains, and nation states assume the worst and prepare themselves by building stronger and stronger arsenals to maintain strategic equilibrium.

Anonymity is often regarded as a key foundational principle of the Internet, driven by the need to shield the identity of the user and dissociate users’ actions from their identity. 7 Such anonymity ensures the ability to speak freely without fear of retribution, which can be beneficial in political commentaries, debating contentious issues, asking personal questions, researching competitors, and purchasing goods or services without revealing personal choices. Privacy advocates have gone to great lengths to protect the anonymity of users by providing services, such as remailers and encryption, that further camouflage users’ identities and protect them from government surveillance. However, while beneficial in some contexts and circumstances, such anonymity also shields the perpetrators of crime and terrorism on the Internet. 8 The cloak of anonymity protects and enables perpetrators of money laundering, extortion, espionage, and theft. Similarly, actors engaging in cyber warfare leverage anonymity on the Internet to conduct surveillance, probes, and attacks without drawing attention to their actions. There has to be a balance between anonymity and security to ensure people’s right to privacy and security. 9

Forensics and Attribution

Despite the inherent anonymity of the Internet, users leave traces of their activities along the way. These traces can provide valuable clues that can reveal the identity of the attackers and their possible motivations. The goal of digital forensics is to collect the traces, connect the dots, and make inferences about the incident, including identifying the perpetrators, determining the mechanism of operation, and cataloging the information compromised or altered. The tools, processes, and knowledge for digital forensics are freely available. Still, the anonymity of the Internet makes such analysis difficult, especially in the case of cyber warfare, where relevant information of the attack is hidden behind country firewalls and protected by the sponsors of the attack.

Digital forensics can strip away some of the Internet’s anonymity and narrow down the field of perpetrators by piecing these clues together and creating a chain of evidence that can link the attacker to the incident. 10 Such evidential chains may not constitute irrefutable evidence in a court of law. Still, when combined with additional information such as legal, political, intelligence, and policy considerations, the resulting assessment could allow policymakers to formulate a national response to cyberattacks. From a national security perspective, as Healey argued, knowing “who to blame” can be more important than “who did it?”11 A proper response to this question provides national authorities with the ability to assess the situation during an evolving conflict and weigh possible responses from a range of economic, diplomatic, or other tools at their disposal. As a multi-dimensional issue that draws on all sources of information available, including technical forensics, human and signals intelligence, historical precedents, and geopolitics, attribution of attacks to a state actor in cyber warfare requires a genuinely national effort and the development of corresponding technical and non-technical capabilities. It is through these processes of data collection and sharing, and analysis and cooperation conducted at national and international levels, that digital forensics becomes instrumental in the operationalization and practical evolution of a robust confidence-building measure (CBM) regime.

The tools and techniques of cyberattacks are common to “cyber warfare,” “cyber terrorism” and “cyber activism.” Only by analyzing the actors, modes of operation, and motivations behind attacks, and their intended or manifested targets, can one differentiate between the three. In contrast to conventional warfare, it is very difficult to distinguish whether attacks on a website or the online theft of data are attributable to individuals in another state who are motivated by financial gain, political or religious ideology, or actions taken by that state’s intelligence agency or military (or their proxies). Since states may launch cyberattacks via proxies in other states, attribution difficulties are compounded, and present fundamental challenges during both conflict and peace times, when international cooperation and treaty compliance verification take hold.

Digital forensics involves gathering data logged in different devices, including computers, routers, electronic industrial control systems, and mobile devices, 12,13,14 putting it on the same timeline and making inferences to determine the anatomy of the attack/intrusion. Several pieces of relevant information can be used for tracing the activities of a person or a device, including IP-addresses, domain names, and time stamps. 15 These individual entries in different log files can be time-correlated to create a chain of evidence and demonstrate activity emanating from a specific source.

An equally important dimension of digital forensics is the detection of intrusion and post-incident analysis, whereby investigators need to understand how an attack was launched, what was stolen, damaged or changed, and how to prevent the attack from occurring in the future. 16 This involves analyzing the internal logs of actors involved in the cyberattack and piecing together evidence from multiple sources into a single timeline of events. The evidence can be collected from hard drives, RAM, USB drives, storage devices, and network appliances. The fundamental problem with such analysis is the sheer volume of the data. Also, to forensically examine data from the past, it needs to be stored. Data storage limitations, especially network devices that generate enormous amounts of data, also limit the possible time frame of analysis. 17 Other useful forensic techniques include analysis of social networks, as well as text analysis from social media to identify cyber warfare activities, such as propaganda, terrorist recruitment, or information exchange. Some of this analysis is done by hand, but a majority of it is done using automated tools that can sift through large volumes of text to flag relevant data for human analysts. Linguistic tools used for text analysis have become much more sophisticated over the last decade, from simple word counting to separating parts of speech and gaining limited language understanding. These forensic tools can help address the problems of attribution and provide means of dealing with contentious issues related to attribution and deflection of responsibility.

Forensics practices are well established and tools are available to rapidly analyze data and draw inferences from it. The data for analyses can be collected from devices and networks within organizations and Internet Service Providers (ISPs). There are, however, fundamental issues with forensic analyses and data collections that cross international borders and reach outside of a nation-state’s jurisdictional control. First, much of the data is stored in routers and devices that are with the ISPs, which are subject to local laws. The data can be in multiple sources on the network and needs to be acquired before analysis. If data is not collected shortly after the incident, it can be overwritten. Consequently, administrative delays in coordination across countries can undermine forensics efforts. Additionally, if a state is complicit in the launch of an attack, the veracity of the data itself can be in question. The data could have been doctored, tailored, or completely faked. Second, getting physical access to the perpetrator’s computer requires a level of cooperation among countries that may be possible in cases of crime, but strained or nonexistent during cyber warfare. Third, all data can be spoofed, i.e., a fake address of origin can be used in packets to conceal the real IP-address, making the problem of identification even more difficult. Finally, the use of anonymizing tools can camouflage the perpetrators further, making attribution complicated.

All of these challenges make technical attribution for international cyber incidents difficult, though not impossible. It is still possible and has dramatically improved over the last few years through sustained intelligence efforts. In addition to data collected directly from ISPs and organizations, data can be collected through the use of honey pots and prepositioned data taps across global networks. Intelligence agencies are continuously monitoring the activities of known actors (including nation states). They are building intelligence dossiers that can be coupled with knowledge gained from digital forensics to make more definitive attributions.

Knowledge of previous events, tools, and techniques of known actors can be used to trace the origins of attacks. There is no automated analysis process; rather, analysts painfully evaluate evidence and make probabilistic judgments for assigning attribution. There are different levels of attribution, with each level becoming more difficult to assign attribution or point of origin (nation-state, hacker group), specific device (computer used to launch an attack), and an individual responsible for launching the attack. It is even harder to accurately pinpoint the sponsor of an attack, in cases where the hacker/group is working as a proxy.

Discussion

There are limits to what digital forensics can accomplish. These tools will only work to the extent that there is a political will for international cooperation in data sharing and analysis. Important first steps would include the establishment of hotlines and the deployment at strategic locations of standard data collection devices that could not be tampered with. These could be foundational to support the forensic analysis of cyberattacks and international determination of instances of cyber warfare. An international body needs to be created and deployed in a neutral country to monitor and evaluate cyber conflicts, with observers present from warring nations. This body would be able to quickly request data access from different sources; lengthy procedures can delay and limit the collection of data, which can be ephemeral. This body will also have the technical expertise to analyze large volumes of data and determine attribution, as well as to confidentially handle intelligence without having to reveal its sources.

Digital forensics practices were developed to effectively piece together the evidence in criminal cases where: the data footprint is small; there is physical access to devices; and the perpetrators involved are relatively inexperienced with camouflaging techniques. This is very rarely the scenario when attacks are perpetrated by well-trained professional hackers. As a result, intelligence agencies have already adapted and scaled forensics procedures for nation-state cyberattacks; a lot of these practices are not yet in the public domain. We will need to create standard forensics procedures (publicly available) for investigating cross border attacks in which camouflaging techniques have been deployed.

Additionally, digital forensics is constantly lagging behind the torrid pace of technological evolution, both in types of applications and devices, as well as in volumes of data. 18 In the coming years, digital forensics will need to be able to contend with the extremely high volumes of data, as well as the sophisticated camouflaging techniques that are used in cyber warfare to become a credible factor in the attribution of cyber warfare activities. To be able to stay on course, we need to have an international forensics research institute for researching and updating forensics practices as information infrastructures evolve (e.g., connected vehicles, human-implantable devices, self-driving cars). We also need to train experts in each country on best practices (tools and techniques) in digital forensics so that they can conduct their investigations.

We must realize that attribution may not always be perfect due to purposeful misdirection or limitations of the analysis itself. This was illustrated by the attack on Sony Pictures Entertainment in November 2014. A hacker group calling itself the “Guardians of Peace” released confidential Sony data onto the Internet, including personal employee data, vast email and password files, internal documents and communications, unreleased copies of motion pictures, and much more. There are two conflicting theories of attribution: one suggests that the North Korean government was behind the attack, given the similarity of the malware used to that used in previous attacks by the North Koreans; 19 the other, based on linguistics analysis, suggests that Russians conducted the attack. 20 There is no conclusive proof supporting either theory, only circumstantial evidence based on the conventional triad of means, motives, and opportunity. To address this, we must resort to a probabilistic approach and define standards of attributions based on the confidence levels of attribution and permissible retaliation to prevent the disproportionate response from escalating into a kinetic conflict.

The demilitarization of cyberspace or a moratorium on the development of cyber weapons is no longer a possibility. However, nation states must come together to find common ground in cyber warfare starting with confidence-building measures, norms of behavior, and the applicability of international laws to reduce the possibility of a major catastrophic incident. Formal information sharing (both at CERT and diplomatic levels) and establishing hotlines will help deescalate future cyber incidents. There needs to be consensus building at the United Nations and other established international bodies such as the Office of Security and Cooperation (OSCE) to find ways of building consensus among nation states on preventing cyber conflicts and building confidence.

Conclusions

The Internet is a major economic and societal driver and instrument of knowledge dissemination with huge economic, political, and national security consequences. It is also a place for data theft, espionage, fake news, political influence, and propaganda, as has been evidenced in the Middle East, South Asia, and Europe. Nation-state attacks are constantly growing both in terms of frequency of attacks and sophistication. Such attacks undermine its influence as societal glue and diminish its influence on economic prosperity. There have been efforts to stem the escalation of cyber warfare; however, it has been very hard to build consensus among nation states on the mechanisms for de-escalation of cyber warfare. Lack of transparency in cyber weapon development and attribution of cyberattacks has been a critical barrier to the acceptance of confidence building measures. Improvement in data collection (intelligence) and forensic analytics capabilities has given us a much better cyber incident attribution capability. By building consensus among nation-states on protocols and procedures for attribution and clarifying the applicability of international law, we can start to build consensus on CBMs and norms and make the Internet safer and enable it to thrive. The paper suggests several initiatives to reduce the chances of cyber conflict as well as to prevent cyber conflicts from escalating, such as defining clear processes for attribution, creating neutral bodies for incident analysis, and limiting the scope of retaliation based on the confidence in attribution.

## Aff Extensions / A2s --- Solvency

### Ext --- Increased Info-Sharing Solves Resilience / Attribution

#### Resilience solves impacts

Abraham & Daultrey 20 --- Chon Abraham Associate Professor of Management Information Systems William & Mary Sally Daultrey Chief Intelligence Analyst Adenium Group, “Considerations for NATO in Reconciling Challenges to Shared Cyber Threat Intelligence: A study of Japan, the US and the UK”, in “Cyber Threats and NATO 2030: Horizon Scanning and Analysis”, Dec 2020, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE (CCDOE), https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030\_Horizon-Scanning-and-Analysis.pdf

Cyber threats are fundamentally changing the nature of warfare and the digital economy with implications for international collaboration and security cooperation (NATO, 2019). Governments and the leadership of multinational companies must understand threat vectors and threat actors to activate their collective response, both in peacetime and during targeted cyber operations. Efforts for developing approaches to exchange information on security incidents, known as Cyber Threat Intelligence (CTI) sharing, is an international imperative (Menges et al., 2019) and governments can no longer rely on voluntary compliance across business ecosystems and supply chains to operationalise international cyber defence. Cyber operations are increasingly understood as linked to strategic campaigns, particularly when initiated by adversarial countries seeking to shift the relative balance of power amongst targeted countries with rippling global effects (Harknett and Smeets, 2020; NATO CCDCOE, 2017). CTI sharing is therefore essential for all directly and indirectly targeted societies and countries to build a collective understanding of these cyber operations and strategic campaigns in terms of: (1) their true nature; (2) the global reach of effects; (3) the duration; and (4) the extent of data exfiltration and aggregation compromising national security. The sophistication and proliferation of cyber threats are outpacing the capacities of countries to respond using conventional decision structures, to be replaced by dynamic bilateral and regional collaboration architectures. CTI sharing is vital to protecting the global business ecosystem and shared security interests, yet not all nations have comparable capabilities to effectively share and act on threat information.

#### NATO CTI sharing solves resilience

Abraham & Daultrey 20 --- Chon Abraham Associate Professor of Management Information Systems William & Mary Sally Daultrey Chief Intelligence Analyst Adenium Group, “Considerations for NATO in Reconciling Challenges to Shared Cyber Threat Intelligence: A study of Japan, the US and the UK”, in “Cyber Threats and NATO 2030: Horizon Scanning and Analysis”, Dec 2020, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE (CCDOE), https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030\_Horizon-Scanning-and-Analysis.pdf

While the requirement for multinational cyber cooperation is challenged by unbalanced technical capabilities, strategic cultures and legal frameworks, NATO is well-positioned to enable partner and allied nations to share CTI, particularly by assisting with enabling use of its MISP and encouraging best practice in provisioning cyber authority structures for threat intelligence sharing as part of a potential international cyber security maturity, resilience development and assessment programme. For this programme, the NATO Cooperative Cyber Defence Centre of Excellence could take the lead in:

(1) reconciling incompatibilities and promoting level setting of threat intelligence capabilities across partner and allied nations to speed the flow of information;

(2) coordinating agreements to ensure trusted threat intelligence information is acted upon;

(3) enabling partners and allied countries to adopt a minimal set of classification standards, compatible ontologies and comparable personnel security clearances management programs that enable threat intelligence sharing;

(4) encouraging the development of a threat intelligence maturity scale that addresses technology, process, and workforce capabilities to aid nations in readily identifying specific improvements to benefit the international threat intelligence ecosystem; and

(5) developing mechanisms to promote accountability in global industries to build threat intelligence capacity and trusted sharing with public entities for the international cyber mission.

Making CTI sharing viable requires that partner nations start talking the same language and allow for some compromise on blaming, naming and shaming, to encourage the private sector to take more responsibility and contribute to the national cyber mission of their respective governments. Implications for NATO partnerships include identifying structures and practices among partners that are not constrained by strategic culture and exploring the scope for NATO’s role—as a non-state actor—in defining a ‘common operating language’ for CTI architectures and practices. Building comparable threat intelligence capabilities under the constraints we have identified in this study is extremely difficult. Yet, the requirement to accelerate and facilitate effective global cooperation in cyber defence is urgent. Thus, in undertaking this charge NATO can truly be unfettered in deliberation to thwart the ability of any entity to weaponise the cyberspace domain.

#### Solvency card

Skopik et al 16 --- Florian Skopik Senior Scientist of the research program “IT Security”., Giuseppe Settanni joined AIT in 2013 as scientist and is currently working on national and European applied research projects regarding security in communication and information systems, Roman Fiedler is Scientist at the AIT Austrian Insititute of Technology and runs projects in the areas of telehealth and ICT security, “A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing”, Computers & Security Volume 60, July 2016, Pages 154-176, <https://www.sciencedirect.com/science/article/pii/S0167404816300347>

Although cooperation between international stakeholders is hampered by many obstacles, it is beneficial for all sides. Cooperating international cyber incident response teams get most benefit in terms of joint incident handling, project conducting, resource and information sharing, and (social) networking.

Having an ecosystem of (international) interconnected sharing entities (critical infrastructure providers, governments, security organizations, etc.), like the one proposed in Kaufmann et al. (2014), would indeed ease the gain of situational awareness, allowing consciousness on the current cyber security situation of all the monitored infrastructures. This is the initial step required to effectively perform cyber defense and incident response. Being part of such ecosystem enables the participating organizations to get access to a large amount of relevant security information that can be essential while defending against ongoing cyber threats. Best practices, resolved security issues, newly discovered vulnerabilities and any other relevant information included in this shared knowledge are fundamental for protecting the organizations' infrastructures and prevent future incidents. Eventually, coordinated incident response methods can produce more effective results, thanks to the diversity of available resources and skills within the sharing community.

#### Increased sharing improves attribution and trust --- key to collective response

Ford 22 --- Christopher A. Ford, Distinguished Policy Advisor at MITRE Labs and a Visiting Fellow at Stanford University’s Hoover Institution. He previously served as U.S. Assistant Secretary of State for International Security and Nonproliferation, “Conceptualizing Cyberspace Security Diplomacy”, SPRING 2022, <https://cyberdefensereview.army.mil/Portals/6/Documents/2022_spring/03_Ford_CDR_V7N2.pdf?ver=jPNxXAqiUZX7kFHLgxwpUw%3D%3D>

I. Improved information sharing is a way to help drive situations rightward along the information strength (X) axis in ways that would, all other things being equal, create a greater likelihood of agreement. This could mean doing more to share with international partners intelligence reporting that supports attribution analysis, either passing it directly to partners with whom one has good cyber-intelligence relationships (e.g., within the “Five Eyes” partnership) or by downgrading information to be shared with others. Information sharing can also occur via public criminal indictments—which must meet due process standards and ultimately survive beyond a reasonable doubt proof standards for conviction if they get to court—or perhaps in connection with the imposition of sanctions.[43]

Whatever the means, however, building more effective mechanisms for secure sharing of attribution-relevant information would probably have the effect of making attribution agreement more likely. It can also help strengthen interlocutors’ perceptions of trust in the sharer, potentially causing agreement-conducive movement along the graphical Y-axis as well. (A country sharing more information with a second-party partner that is more trusted by the third-party target of diplomatic suasion than is the first country can also help spur movement along both axes: it enables the recipient of this information to leverage its own relationship of trust with the ultimate target.) Augmented information sharing can thus result in movement within the cubic situational space along both the X and Y axes, as depicted in Case I in Figure 13.

To the degree that attribution-relevant information can be shared publicly, or at least very widely within the broad open-source cybersecurity community, one might expect this to also support more positive outcomes in attribution diplomacy. The MITRE Corporation’s “ATT&CK Matrix,” for instance, compiles and displays information about known malicious cyber activity TTPs for cybersecurity professionals on an open-source basis,[44] providing a resource for cybersecurity officials around the world whose job it is to defend against such attacks. In cases where private sector or governmental attribution assessments have been made about specific intrusions, however, it might be possible in the future to include not just information about specific TTPs themselves but also an indication of which bad actor originated a given technique and with whom that technique’s use is most frequently associated. To the degree that subsequent attribution diplomacy relies upon analysis of cyber-attack techniques, such a public record of past associations between bad actors and specific TTPs could help increase the credibility of subsequent attribution assessments, strengthening diplomatic persuasiveness.[45]

## Aff A2s: T

### 2AC A2: Cybersecurity

#### Counter-Interp --- Cybersecurity includes information sharing --- Content is irrelevant

Stadnik 21 --- Ilona Stadnik, PhD candidate at the School of International Relations, St Petersburg State University, “Seeking a new order for global cybersecurity: the Russian approach to cyber-sovereignty”, in “NATO’s evolving cyber security policy and strategy”, Print publication date: January 2021, https://ebrary.net/173503/political\_science/seeking\_order\_global\_cybersecurity\_russian\_approach\_cyber\_sovereignty

The most common definition of cybersecurity refers to an operational and infrastructural level of information sharing, but not to its content per se. The common cybersecurity triad includes the principles of confidentiality, integrity, and availability. That means that information is available only for an intended circle of users, information is correct and complete without any breaches or unauthorized modifications, and that information can be accessed any time it is necessary. Parker (2002) added three more principles to the triad: possession or control, authenticity, and utility. The first principle indicates the necessity to maintain control over information because its loss threatens the security despite saving its confidentiality and integrity. The second principle is about the originality of authorship of the information. And finally, utility means that information is still usable after all other security precautions.

#### Sharing meets “cybersecurity”

ENISA 16 --- European Union Agency for Cybersecurity, “Information Sharing and Analysis Centers (ISACs)”, Website first archived June 2016, <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing>

Information sharing between national stakeholders but even in cross country cases is one important aspect for cyber security. Knowledge on tackling cyber attacked, incident response, mitigation measures and preparatory controls can be shared between the relevant stakeholders.

### A2: Security Cooperation

#### Sharing is caring… and its also SC

Mazarr 22 (Michael J. Mazarr, senior political scientist at the RAND Corporation, former professor and associate dean of academics at the U.S. National War College, former special assistant to the Chairman of the Joint Chiefs of Staff and senior defense aide on Capitol Hill, PhD public policy, University of Maryland, MA security studies, Georgetown University; with Nathan Beauchamp-Mustafaga, Jonah Blank, Samuel Charap, Michael S. Chase, Beth Grill, Derek Grossman, Dara Massicot, Jennifer D. P. Moroney, Lyle J. Morris, Alexander Noyes, Stephanie Pezard, Ashley L. Rhoades, Alice Shih, Mark Stalczynski, Melissa Shotak, David E. Thaler, and Dori Walker, all at the RAND Corporation; “Security Cooperation in a Strategic Competition,” RRA650-1, RAND Corporation, 2022, https://www.rand.org/content/dam/rand/pubs/research\_reports/RRA600/RRA650-1/RAND\_RRA650-1.pdf)

Definitions and Scope

To pursue this analysis, we first had to define the bounds of what we would assess. Official U.S. government definitions of security cooperation are very broad. One definition from the Defense Security Cooperation Agency states that security cooperation

comprises all activities undertaken by the Department of Defense (DoD) to encourage and enable international partners to work with the United States to achieve strategic objectives. It includes all DoD interactions with foreign defense and security establishments, including all DoD-administered Security Assistance (SA) programs, that build defense and security relationships; promote specific U.S. security interests, including all international armaments cooperation activities and SA activities; develop allied and friendly military capabilities for self-defense and multinational operations; and provide U.S. forces with peacetime and contingency access to host nations.3

Such definitions clearly include almost any security-related activity for any purpose. To scope the focus of the study, we reviewed official state documents and strategies and the literature on security cooperation to identify 11 types of activities:

1. military aid, which includes funding through the Foreign Military Financing (FMF) program, the Excess Defense Articles program, and other grants and loans

2. arms sales and transfers,4 such as U.S. arms sales through the Foreign Military Sales (FMS) and Direct Commercial Sales (DCS) programs

3. military capacity-building, such as U.S. activities under Section 1206 of the annual National Defense Authorization Act and Sections and 2282 and 333 of U.S. Code, Title 10 (the train and equip authority)

4. education and training, including international military education and training (IMET), professional military education (PME), and regional centers

5. personnel exchanges, such as U.S. activities under the Military Personnel Exchange Program and the State Partnership Program

6. military exercises, both bilateral and multilateral and those that involve foreign partners

7. access-related agreements, such as status of forces agreements (SOFAs) and agreements related to base access and information-sharing

8. armament-related agreements, such as those for co-development of systems and for research, development, test, and evaluation activities

9. sustainment of donor-nation equipment by the donor, the partner, or third parties

10. institutional capacity–building to strengthen the partner institutions that support security services

11. humanitarian assistance and disaster relief (HA/DR), which offers support for efforts to relieve suffering.

These categories offered a consistent template for gathering data across our various study components. A major challenge was that reliable and consistent data on each of the 11 categories were not available for all the competitors—not even for the United States. Especially at the unclassified level, there is simply no comprehensive roster of security cooperation activities by the United States, and neither China nor Russia publishes inclusive data sets of its programs. An additional challenge was that, in some cases, the different countries define the categories somewhat differently, so we could not develop data on entirely comparable sets of security cooperation activities.

#### Security coop includes info sharing

Donnelly & Maginnis 11 --- Brigadier General Edward P. Donnelly, U.S. Army, recently completed two years as the Army’s deputy director for strategy with responsibility for, inter alia, the International Affairs and Security Cooperation portfolios, and Lieutenant Colonel Robert Maginnis, U.S. Army, Retired, MILITARY REVIEW  May-June 2011, https://apps.dtic.mil/sti/pdfs/ADA542464.pdf

1. U.S. Department of Defense (DOD), 2010 Guidance for Employment of the Force (draft 30 April 2010) (Washington, DC: U.S. Government Printing Office [GPO], TBP), 166. Security cooperation is defined as “All DOD interactions with foreign defense establishments to build defense relationships that promote specific U.S. security interests, develop allied and partner military capabilities for self-defense and multinational operations, and provide US forces with peacetime and contingency access to a host nation.”

2. Ibid. The Guidance for the Employment of the Force consolidates and integrates DOD planning guidance related to operations and other military activities into a single, overarching document.

3. U.S. Army Field Manual (FM) 3-07, Stability Operations, (Washington, DC: GPO, 2008), <http://downloads.army.mil/docs/fm\_3-07.pdf>, G-2. Security force asssistance is defined as “The unified action to generate, employ, and sustain local, host-nation, or regional security forces in support of legitimate authority.”

4. George W. Casey, Jr., “The Army of the 21st Century,” Army, October 2009, 30.

5. DOD, Army Security Cooperation Strategy (draft 6 May 2010) (Washington, DC: GPO, TBP).

6. DOD, 2008 Army Posture Statement, available at: <http://www.army.mil/ aps/08/addenda/addenda\_e.html> (29 June 2010). “The ARFORGEN process is used to manage the force and ensure the ability to support demands for Army forces. ARFORGEN sequences activities for all active and reserve Army units to include: Reset, Modular conversion, Modernization, Manning adjustments, Soldier and leader training and education programs, Unit training, Employment; and Stationing decisions.”

7. Guidance for Employment of the Force, 2010, 25-27. There are 10 security cooperation focus areas in this document: (1) operational capacity and capability building, (2) human capacity/human capital development, (3) institutional capacity/ security sector reform, (4) support to institutional capacity/civil-sector capacity building, (5) combined operations capacity, interoperability, and standardization, (6) operational access and global freedom of action (U.S. defense posture), (7) intelligence and information sharing, (8) assurance and regional confidence building, (9) international armaments cooperation, and (10) international suasion and collaboration

#### SC and SA are the same

Watts & Biegon 17 --- Tom Watts, PhD candidate in the School of Politics and International Relations at the University of Kent, and Rubrick Biegon, associate lecturer and research administrator in the School of Politics and International Relations at the University of Kent, “Defining Remote Warfare: Security Cooperation”, Remote Control, November 2017, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/ORG\_RemoteControl\_SecCoop.pdf

Security cooperation is embedded in the institutional structures of foreign military assistance, as authorised under Titles 10 and 22 of the United States Code. Conceptually, ‘security cooperation’ (SC) overlaps with ‘security assistance’ (SA). They are distinct but closely-related tools of ‘building partner capacity’ (BPC), a term first coined in the 2006 Quadrennial Defense Review. BPC constitutes a ‘broad set of missions, programs, activities, and authorities intended to improve the ability of other nations to achieve… securityoriented goals they share with the United States’.9 In the fallout from the Iraq war, BPC became an urgent goal of US policy. It allowed the US to maintain a ‘long-term, low-visibility presence in many areas of the world where US forces do not traditionally operate’.10 In this respect, both SC and SA are tools to build the capacity of foreign partners to combat security threats with minimal (or no) involvement of US ‘boots on the ground’. SC encompasses all Department of Defense interactions, programmes and activities with foreign security forces to build relationships that promote US interests; enable partners to provide the US access to territory, infrastructure, information and resources; and/or to ‘build and apply their capacity and capabilities consistent with US defense objectives’.11 DOD-administered SA programmes are one element of this, which also includes combined exercises, information sharing and other types of military-to-military collaboration. SC has long been valued by Combatant Commanders as a tool for shaping the security landscape in their area of operations to favour American interests.12 It has been extensively used to develop relationships and interoperability between the American military and its overseas partners.

## Aff A2: Disads

### A2: Midterms

#### FP Doesn’t matter

Cook 22 --- Charlie Cook, One of the nation's leading authorities on U.S. elections and political trends,, Cook Political Report, Foreign Policy Unlikely To Save Democrats in the Fall, Feb 2022 https://www.cookpolitical.com/analysis/national/national-politics/foreign-policy-unlikely-save-democrats-fall

Given how monolithic partisans are in their approval ratings and actual voting, it is always useful to look only at independents, the ‘jump ball’ Americans. Biden’s overall rating among them was 35 percent (5 points below his approval among all adults). His best marks were on dealing with the coronavirus (45 percent approval), followed by foreign policy (37 percent), Russia (35 percent), and the economy (30 percent). It is pretty clear the president and his administration’s denial of the threat of inflation and slow reaction to it was exceedingly damaging to him. (While we are on the subject, it is fascinating to see Senate Democrats, after so passionately advocating for more infrastructure spending this past year, propose suspending the gasoline tax for the rest of the year, no matter that the gas tax is the primary regular funding source for transportation infrastructure. Panic is never pretty.)

While we don’t know the trajectory that the Russia/Ukraine crisis will take, and there are many factors that can impact on midterm elections, we do know that in the absence of a large number of U.S. military deaths, Americans rarely vote on foreign-policy issues, particularly in midterms. The state and direction of the economy, particularly change in real disposable personal income, is far more determinative.

#### Too soon

Rogers 1-4 [Kaleigh Rogers is FiveThirtyEight’s technology and politics reporter., 1-4-2022 https://fivethirtyeight.com/features/5-things-to-watch-going-into-the-midterms/]

Though 2022 has only just begun, the midterm elections are already looming over the political horizon. Democrats’ loss in the Virginia governor’s race last year — and their surprisingly narrow win in the New Jersey governor’s race — both suggested that we could be heading for a red wave in this year’s midterm elections. And overall, the political environment is looking favorable for Republicans. Based on House retirements — which can give us some clues about how the congressional elections might unfold — it also seems like Democrats are more worried than Republicans. Those worries aren’t unfounded, either, since the president’s party almost always struggles in midterm elections, usually losing ground in the House and often in the Senate too.

But there are also a lot of factors that could shake things up. Over the past year, Republican legislatures across the country have passed an unprecedented slew of laws to restrict voting access, including some states that will be most closely watched this November. Fears about inflation are simmering, but the labor market is recovering, albeit unevenly. Meanwhile, COVID-19 cases have surged to an all-time high, driven by the omicron variant, even if so far deaths and hospitalizations have not been as bad as last year. And finally, state lawmakers are in the process of redrawing congressional maps based on the results of the 2020 census, setting the geographic boundaries that will shape congressional power for the next decade (if the courts don’t strike them down).

It’s impossible, of course, to predict how all of these four moving pieces — voting restrictions, the economy, the pandemic and redistricting — will affect each other. But we do have a sense of the role they could play individually. So here’s an overview of what we know about what each of these indicators could mean for the midterms, and what kinds of surprises could be in store this year.

A wave of voting restrictions could affect turnout in swing states

Under the fraudulent pretense that widespread voter fraud cost former President Donald Trump the 2020 presidential election, at least 22 states have passed 53 or more new voting restrictions. And since the federal government has not yet passed federal voting rights legislation, these statewide bills could have an impact on turnout and voter enthusiasm heading into the midterms.

The number of voting restrictions that were enacted in 2021 is astonishing. In fact, according to the Brennan Center for Justice, the total number of restrictions passed in 2021 shatters the previous record-high, which was 2011, when 14 states enacted 19 bills by October of that year. And a lot of the bills passed this cycle have curtailed the expansion of absentee voting from the pandemic, but bills requiring proof of identity to vote and preventing the implementation of automatic voter registration were prioritized too.

The short- and long-term effects of these newest statewide laws are still a bit of an open question; we’ve never seen such aggressive and widespread GOP-led efforts to pass new voter restrictions, but also there’s conflicting research on the effects of proposals like these. On the one hand, some studies show that some policies, like voter ID laws, which have long been anathema to Democrats and voting rights advocates, don’t necessarily decrease voter participation, even among people of color. And although a number of Republican-led states targeted absentee voting after it helped clinch Biden’s 2020 victory, a recent study found that states that implemented absentee voting in 2020 didn’t see a huge increase in turnout when compared with states that did not implement it. So it’s not a foregone conclusion that states like Georgia, which has received national attention for pushing stringent and anti-democratic voter laws, will actually see lower turnout — at least probably not as a result of the restrictions. In fact, other reporting has found that, counterintuitively, some restrictions can backfire and instead boost turnout because voters might be more energized to cast a ballot.

That said, the totality of the laws that have been passed this cycle makes it hard to predict their effects this November. And the fact remains that some of the most restrictive measures on the books are in swing states, which could affect the midterm result, in addition to disenfranchising voters there. There’s also, of course, the possibility that the newest state laws will make administering elections more open to partisan interference, since many of the bills proposed by Republican legislatures reassigned election administration to highly partisan legislatures — which could allow elected lawmakers to overturn the will of the voters and determine their own preferred winners of elections.

Economic worries could play a role — but they might be trumped by partisanship

Inflation is accelerating at the fastest pace in decades, and although the economy is bouncing back in other ways, most Americans feel pessimistic about the country’s economic challenges. That could be a worrying sign for Democrats’ electoral chances in the midterms this year. Often, the economy is seen as a critical electoral indicator, particularly regarding presidential elections.

But the upcoming election cycle could be different. That’s in part because there’s evidence that the economy just doesn’t matter as much in midterm elections. More broadly, views of the state of the economy are also increasingly partisan — which means that Republican and Democrats’ views of the economy may be more influenced by politics than by how the economy is actually doing.

This is not to say that the economy can’t influence politicians’ electoral fates. In fact, political science research has found that voters do reward presidential candidates when the economy is good, and punish them when it’s bad. It’s the overall trajectory of the economy that’s most important here, too, according to Christopher Wlezien, a professor of government at the University of Texas-Austin. “You might have a low unemployment rate and a low inflation rate, but if the economy’s not growing, that’s not really a ‘good’ economy,” he said.

But researchers have consistently found that the economy isn’t as important of a factor in midterm elections. That’s not because the economy is only important every four years — it’s just that other factors, like the generic ballot (a measure of which party people would back for Congress), are better predictors of which way the midterms will go.

Partisanship, too, can have a dampening effect. Polling consistently shows that Americans’ feelings about the health of the economy shift dramatically depending on whether a Republican or Democrat is president.

That detachment from the actual health of the economy could be particularly pronounced in this year’s midterms because the pandemic has the economy in such an intense state of flux. On the one hand, Democrats can point to economic improvement since Biden took over last January — the unemployment rate is falling and wages are rising. But there are worrying signs as well. There are the surging inflation numbers, for instance, and metrics like the unemployment rate are relative. In the November 2021 jobs report, the unemployment rate was 4.2 percent — much better than April 2020, when it was a horrifying 14.7 percent, but still quite not back to its pre-pandemic levels.

This leaves plenty of room for Americans’ political identities to influence how they see the economy. Those assessments will still be based on voters’ everyday economic realities — whether they think the rent and the price of milk are rising, whether they’ve lost or gotten a job, whether their neighbors seem to be struggling or prospering. But their preexisting views about the parties will likely do a lot to shape how they view the economy.

Voters’ fears about COVID-19 could haunt politicians

As we approach the two-year anniversary of the start of the COVID-19 pandemic in the U.S., there is still much uncertainty about what the future holds. While vaccination rates continue to slowly climb, the highly transmissible omicron variant and the need for all Americans to receive booster shots highlight just how unpredictable this pandemic remains. Despite concerns around omicron, many Americans are unwilling to give up the small freedoms they’ve gradually clawed back, and even with the new variant, inflation now beats out COVID-19 as the top concern in polls. This may be what it looks like for COVID-19 to start to become a fact of life, rather than a temporary disaster. But whether the pandemic is top of mind for voters this November or not, it will inarguably play a role in the midterms — both politically and practically.

Let’s start with the practical ramifications. The 2020 election landed during an early wave of the pandemic, and most states made a number of special concessions to the way voters cast their ballots to make things safer and encourage physical distancing. But while these measures were enacted temporarily in some states, they’ve now become permanent in others. Nevada and Vermont switched to universal mail voting during the pandemic, for instance, and both have now made the change permanent, while many other states have now made no-excuse absentee voting (meaning voters don’t need a specific reason to vote by mail) the law of the land.

Even some states that have recently enacted voter restriction laws kept a few pandemic-time voting expansions. For example, despite taking steps to make it harder to vote, Georgia also required a minimum number of drop boxes per county (prior to the pandemic, drop boxes weren’t required at all). It seems that once voters tried out new, more convenient ways of voting, many didn’t want to go back to the old way of doing things.

But beyond changes to how we vote, the long tail of the pandemic will also likely play a role in for whom we vote — or that’s what many politicians are banking on, at least. On the Democrats’ side, there’s an effort to celebrate the party’s successes in responding to the pandemic, such as the relief package passed in March 2021, while also criticizing the response from Republicans. For example, during the California recall election last year, Gov. Gavin Newsom touted his pandemic response and later claimed his win demonstrated that voters appreciated a strong response to COVID-19. (How much of a role COVID-19 played in Newsom’s victory, however, is up for debate.) But Americans’ approval of the Biden administration’s response to the pandemic has precipitously dropped since early July 2021, around the time delta became the country’s dominant strain.

Earlier in the pandemic, approval of Biden’s COVID-19 response was much higher — higher even than his overall approval rating. Now, though, one of his few strong suits with the public has diminished, giving Republicans fresh ammunition. Republicans have leaned into calling out Democratic responses to the pandemic, like vaccine and mask mandates, as violations of freedom, although some Republicans have encouraged voters to get vaccinated (which hasn’t proven to be a particularly effective message with their voters). They’ve also begun firing up their base over the economic woes that have rippled out of the pandemic, such as labor shortages and supply chain delays.

There’s also a good chance that other issues will eclipse the pandemic. Along with the economy taking up more mental space lately, Americans’ concerns around the pandemic tend to ebb and flow with case numbers, as a series of pre-omicron polls from Fox News show. When asked in early August (as the late-summer surge was starting to grow), 69 percent of registered voters said they were very or extremely concerned about the pandemic. That number then grew to 74 percent in mid-September, as that wave was cresting, but when asked again in mid-October (with that wave on the retreat), it shrank back to 67 percent.

As vaccinations increase and more workers begin to trickle back into the office, it’s possible that the pandemic winds up playing a smaller role in the midterms than it has so far. In fact, even in November 2020, as cases swelled to record levels, COVID-19 didn’t play as big of a role in the election as many expected. By this November, it could be an even more minor player in our electoral circus.

Republicans stand to benefit from redistricting, but the overall impact might be small

We’re roughly at the halfway point in redistricting, as 32 states with 279 congressional districts have finished redistricting following the delayed release of the 2020 census last year.1 And while many states still have to draw their lines, we already have a decent idea of what the overall contours of the congressional map will be.

But given the amount of control Republicans have over the redistricting process — the GOP will draw more than twice as many districts as Democrats this cycle — it’s a little surprising that neither party looks set to make major gains in the House due solely to redistricting. We just haven’t seen a dramatic shift favoring one party in the states that have finished drawing their lines. Compared with the old national map, the number of Democratic-leaning seats (defined as seats having a partisan lean of at least 5 percentage points more Democratic than the country as a whole) has increased from the old map, while the number of Republican-leaning seats (R+5 or redder) hasn’t really changed.2

One thing we can point to, though, is that the number of highly competitive seats — those between D+5 and R+5 — is down. And that’s in large part because Republicans have so far been particularly successful in making competitive seats they control much safer for their party in 2022. The number of competitive Republican-leaning seats has shrunk from maps drawn the 2010 census, while the number of safe Republican seats has increased markedly. We can see this trend clearly in states where the GOP controlled redistricting, as previously competitive seats like Indiana’s 5th Congressional District or Texas’s 24th District have become far redder.

For Democrats’ part, they have also tried to create more Democratic-leaning seats in states where they controlled redistricting. So far, they haven’t increased the number of safe Democratic districts, but they have increased the number of competitive Democratic-leaning seats. This reflects their strategy to trade away some dark-blue seats in states like Illinois and Nevada to improve their party’s position in nearby districts that were more competitive on the pre-2022 maps.

The reduction in baseline competitive turf is an important feature of this redistricting cycle; it means that the two parties will be able to more easily lock in control over more seats and to narrow the already-thin campaign battlefield. Most congressional districts are currently quite safe for one party or the other, and that’s not likely to change. It’s true that 18 states haven’t yet finished drawing their lines, but we don’t expect one party to substantially benefit from these new maps. Yes, Republican mapmakers in Florida may draw lines that add a seat or two to their column, but Democrats in New York could produce a map that gives them a chance of flipping a handful of GOP-held seats.

And beyond those two states, about one-third of the remaining seats left to be drawn are not under one party’s control, usually because the state has divided government — as is the case in Pennsylvania and Wisconsin, for instance. A map in one state might end up benefiting one party more than the current lines, but this collection of maps could very well work out to be a wash in the end.

Still, there are wild cards to keep in mind, such as lawsuits that could overturn potential gerrymanders. Yet while Republicans have wider control of redistricting than Democrats, and while they have done quite a bit to shore up their incumbents, The Cook Political Report estimates that the GOP might gain only two to three seats from the redistricting process — a seat swing that is unlikely to decide the House’s fate on its own, considering the president’s party has, on average, lost 26 House seats in midterms since World War II.

What about an October surprise?

We’ve walked you through a host of factors that could influence the 2022 midterms, but sometimes a surprising last-minute event shakes up the race. A hallmark example of this is the 2016 presidential election, when FBI Director James Comey sent a letter to Congress days before the election announcing that the FBI had reopened its investigation into the private email server Hillary Clinton had used as secretary of state. The news dominated headlines, and her lead in the national polls fell nearly 3 points over the next week, with her going on to narrowly lose to Donald Trump.

Now, there aren’t many moments that count as “October surprises” — most day-to-day news events and candidate gaffes during a campaign don’t matter very much. But as the 2016 example shows, they can’t entirely be ruled out as a factor that could affect voter attitudes, especially if a fair number of voters haven’t made up their minds.

#### Elections disad is a lie – plan’s irrelevant

Bacon 10-7 [Perry Bacon Jr. is a Washington Post columnist 10-7-2021 https://www.washingtonpost.com/opinions/2021/10/07/perry-bacon-america-election-obsession/]

Every day is not Election Day. Most days are not Election Day. Most of what happens in the years between elections won’t affect what happens on Election Day. Yet the United States’ political culture has become singularly obsessed with elections, directing us away from important debates about issues and turning every question into an analysis of Wisconsin swing voters.

Of course elections matter, because they decide who gets to set policy. And with the Republican Party becoming more authoritarian by the day, state and federal elections matter especially now. If the GOP wins enough state legislative, gubernatorial and congressional races over the next few years, it may well use gerrymandering, voting-law changes and other moves to create entrenched one-party rule.

And perhaps because of the radicalism on the right, I am seeing a rise in political discussions framed around elections, from not only politicians and activists but ordinary citizens, particularly Democrats. Read political reporting, scroll Twitter or watch cable news, and you’ll notice that much discourse ostensibly about, say, the infrastructure bill, Afghanistan or President Biden is really focused on one all-consuming question: “How will this affect what swing voters in Wisconsin — or Pennsylvania, or Arizona — do in 2022 and 2024?”

Given the high stakes, the obsession is understandable. Nonetheless, it’s a bad development. Why?

First, some ideas deserve a hearing, even if they are unpopular. The civil rights movement of the 1960s could not have survived a daily analysis of how it affected the Democrats’ standing in swing states — the March on Washington was unpopular when it happened, as was the Rev. Martin Luther King Jr. at times. Today, it makes sense that the Republican policymakers keep pushing abortion limits — they believe that is the moral position and are willing to absorb some electoral heat for it. (And it might not be that much heat.)

On the Democratic side, defending the rights of immigrants and Black people may never be particularly popular, and I am not arguing that Biden should completely ignore electoral consequences and propose a major reparations program next week. But Biden generally should not act in morally dubious ways on racial issues simply to woo conservative White voters, not only because such actions would be wrong but also because there is limited evidence this would actually win him many White swing voters.

Second, debating on electoral terms can prevent important discussions about the substance of politics. “What should be in the reconciliation bill?” would be a more useful question to explore with the public and Democratic officials than “What are the electoral effects of passing or not passing the reconciliation bill?”

Third, if we knew the precise electoral effects of passing those bills (or most other things that happen in politics), those effects would be important to talk about. But the truth is we don’t.

Here’s what we really know: Most Americans will vote for the party they normally do. Voters don’t know much about policy details but have some generic predispositions that are heavily shaped by their ideology and media coverage. There is a small group of voters who don’t pay that much attention to politics who swing between the parties and/or vote in some elections but not others. The president’s party generally does worse in midterm elections and when he has a low approval rating.

That isn’t much to work with. Nonetheless, a whole class of elected officials, strategists, pundits and others constantly make confident claims. More conservative Democrats are arguing that the party will suffer electorally if it doesn’t pass an infrastructure bill as soon as possible, while more progressive Democrats argue that it will suffer if it doesn’t pass the reconciliation bill they favor. Democrats on neither side of this ideological divide argue that the party must pass something or voters will punish them next year. And Republicans confidently say that the Democrats will lose in 2022 if they push through the bills.

All of these arguments are at best overconfident and might be more accurately described as nonsense. There is little evidence that most voters carefully track the legislative success of a political party and vote accordingly — and undecided and intermittent voters know even less about what’s happening in Washington.

Similarly, it’s unlikely that the Democrats making slight moves to the right on racial issues will affect voters’ broader perceptions of the GOP as the party that is conservative on race and of the Democrats as liberal on those issues. I would bet that Republicans win the major statewide races in Texas next year despite the unpopularity of its recent abortion law — and my guess is most of the Democrats crowing about how that law will boost them electorally would bet on the Republicans, too.

I know that politicians have long used polling to inform their decisions. I know that the complaint that American politics is now a “permanent campaign” is not new. And I actually think it’s useful to know where the public stands on issues, because the government generally shouldn’t take actions that only a small minority of the public supports.

But the problem isn’t really polling. Rather, it’s the use of polls to center everything that happens in politics around those November 2022 swing voters in Wisconsin. We can have election month, maybe even election season, but when every day is Election Day, we are robbing our politics of real, substantive debates to instead concentrate on possible electoral outcomes that we can’t predict or control anyway.

#### COVID, inflation, and SCOTUS thump---no one runs on or votes for the plan.

Dan Balz and Marianna Sotomayor 5/16/22. Dan Balz is chief correspondent at The Washington Post. He has served as the paper’s deputy national editor, political editor, White House correspondent and Southwest correspondent. Marianna Sotomayor covers the House of Representatives, primarily focusing on Democratic and Republican leadership, for The Washington Post. Sotomayor joined The Post in 2021 from NBC News. "The forces steering the 2022 midterm elections". Washington Post. 5-16-2022. https://www.washingtonpost.com/politics/interactive/2022/big-picture-2022-midterms/

Every election has a story.

In 2010, the story was an angry tea party movement and a rebellion against President Barack Obama’s newly enacted Affordable Care Act. In 2018, it was a backlash, fueled by the energy and fury of suburban women, against the chaotic governing style and misogynistic belligerence of President Donald Trump.

The stories of some elections are often clearer in retrospect than they are in the moment, but there were blinking lights throughout 2010 and 2018 that the party in control of the White House was heading for trouble. The same can be said for 2022. President Biden’s approval ratings are in the danger zone, putting the Democrats’ slender majorities in the House and Senate in jeopardy. Many Democratic leaders are already braced, at a minimum, to lose control of the House.

Political volatility has become commonplace in a nation as deeply and closely divided as America today. Seven of the last eight elections qualify as change elections — a shift in the balance in some important way. And, if Republicans were to capture the House and Senate in November, Biden would become the fifth consecutive president to see his party lose both chambers of Congress on his watch.

But other than Democratic nervousness, what is the story of this year? What is motivating voters? What forces are steering the election, other than the tides of history?

Analysts point to a nation weary at a time in which there seems no escape from disorder, whether it be the long bout with the coronavirus or soaring prices or rising crime rates in cities or surging crossings of undocumented immigrants at the southern border. Added to all of that is the brutal war of aggression in Ukraine launched without provocation by Russian President Vladimir Putin, a conflict that is redrawing the international order.

“This is a country that is exhausted from politics,” said Democratic strategist Doug Sosnik, who served in the Clinton administration. “It’s exhausted from covid. It’s exhausted from uncertainty. It’s exhausted from inflation. It’s exhausted from the world unraveling. That’s not great when you’re in charge. But the second factor is disappointment. There was a notion that with Biden taking office we were going to come back to a sense of normalcy in the world.”

“Independent voters decide elections," said Richard Czuba, a Michigan-based analyst. "Right now [in Michigan] they are really worried about inflation — and it’s not just gas prices. You talk to people in focus groups and they will talk about milk and bread and cereal. They understand that gas prices have soared because of the war in Ukraine, but that’s not the case for food.”

There is another element that now threatens to affect the direction of these elections: the prospect that the Supreme Court will overturn Roe v. Wade, a monumental action that would elevate a battle over the future of abortion rights into the campaign debates. Such a decision in the case involving Mississippi’s restrictive abortion law could cut into what is now a Republican advantage in enthusiasm to vote in November.

Biden administration officials and Democratic candidates will offer their own story as a counter to the prevailing gloomy predictions. Their narrative will highlight passage of a major economic stimulus package and a bipartisan infrastructure bill, the creation of roughly 8 million jobs and the lowest unemployment rate in a half-century. Their story now also includes confirmation of the first Black woman to the Supreme Court — a promise kept by the president to one of his party’s most loyal constituencies. Democrats also will seek to offset their disadvantages by mobilizing voters around abortion and other cultural issues.

### A2: Deterrence/Disclosure DA

#### Turn --- hoarding vulnerabilities DECREASES cybersecurity --- makes our own systems more exploitable

Jardine 20 --- Eric Jardine Assistant Professor, Political Science, Virginia Tech, “Optimizing Cyber Deterrence”, In The Cyber Deterrence Problem, Aaron F. Brantly, ed. (New York: Rowman and Littlefield), page 87-104, 2020, https://osf.io/ns7b3

Deterrence is not straightforward in cyberspace. Maximizing deterrence by trying to maximize the retaliatory potential of the NSA will fail. Upwards of 20 percent of the weapons that the NSA attempts to hoard for a rainy day are likely to be found by adversaries and could then be used to target American systems. By keeping this 20 percent of zero-days under wraps, the NSA weakens the US deterrent by diminishing the costs that an adversary would need to undertake in order to successfully target US networks and devices. Punishment and denial are interconnected. Simple maximization of deterrent outcomes by maximizing the inputs to deterrence does not work.

#### Turn --- Nondisclosure of vulnerabilities causes more risk

Comninos and Seneque 14--- Alex, Justus-Liebig University Giessen, and Gareth, Geist Consulting, “Cyber security, civil society and vulnerability in an age of communications surveillance,” GIS Watch, 2014, <http://giswatch.org/en/communications-surveillance/cyber-security-civil-society-and-vulnerability-age-communications-sur>

Cyber security and vulnerability Cyber security discourse should focus more on information security vulnerabilities, rather than on threats and responses. This focus would help to delineate what constitutes a cyber security issue, avoid cyber security escalating to a counter-productive national security issue, and place a practical focus on the protection of all internet users.

A security vulnerability, also called a “bug”, is a piece of software code that contains an error or weakness that could allow a hacker to compromise the integrity, availability or confidentiality of information contained, managed or accessed by that software.17When a vulnerability is discovered, a malicious hacker may make an “exploit”18 in order to compromise data or access to a computer. Malware – viruses and Trojan horses – require exploits (or collections of exploits) that take advantage of vulnerabilities. Expertise in fixing vulnerabilities is improving but not keeping up with the pace of the growth. Compared to 15 years ago, all popular and contemporary desktop operating systems (Windows, Linux and Mac) offer regular automated security updates which fix or “patch” known vulnerabilities. While we are finding more vulnerabilities in code and viruses than ever before, we are also getting better at finding them. At the same time we keep producing more software code, meaning that the net number of vulnerabilities is increasing.19

Viruses and botnets, including Stuxnet and other state-sponsored malware, require vulnerabilities to work. Finding and fixing vulnerabilities contributes to a safer and secure internet, counters surveillance and can even save lives. For example, a vulnerability in Adobe’s Flash software was recently used against dissidents in Syria.20

There are two categories of vulnerabilities, each requiring different user and policy responses: zero-days and forever-days. Zero-days are vulnerabilities for which there is no available fix yet, and may be unknown to developers. Forever-days are vulnerabilities which are known of, and either do not have a fix, or do have a fix in the form of a patch or an update, but they are for the most part not applied by users.

Zero-day vulnerabilities

When a zero-day is found, the original software developer should be notified so that they may find a fix for the vulnerability and package it as a patch or update sent out to users. Furthermore, at some stage, users of the affected software that are rendered vulnerable should also be informed, so they can understand if they are or have been vulnerable and take measures to recover and mitigate for the vulnerability.

Throughout the history of computers, “hackers”21 have sought to use technology in ways that it was not originally intended. This has been a large source of technological innovation. Hackers have applied this logic to computer systems and have bypassed security and found vulnerabilities for fun, fame, money, or in the interests of a more secure internet. It is because of people that break security by finding vulnerabilities that we can become more secure. A problem for cyber security is that “good” (or “white hat”) hackers or “security researchers” may not be incentivised to find zero-days and use this knowledge for good. Rather than inform the software vendor, the project involved, or the general public of a vulnerability, hackers may decide not to disclose it and instead to sell information about a vulnerability, or package it as an exploit and sell it.

These exploits have a dual use: “They can be used as part of research efforts to help strengthen computers against intrusion. But they can also be weaponised and deployed aggressively for everything from government spying and corporate espionage to flat-out fraud.”22 There is a growing market for zero-days that operates in a grey and unregulated manner. Companies sell exploits to governments and law enforcement agencies around the world; however, there are concerns that these companies are also supplying the same software to repressive regimes and to intelligence agencies. There is also a growing black market where these exploits are sold for criminal purposes.23

#### Turn --- Cyberdefense outweighs any offensive capabilities --- deliberately weakening the internet guarantees successful attacks

Masnick 13 --- Mike, founder and CEO of Floor64 and editor of the Techdirt blog, Oct 7th 2013, “National Insecurity: How The NSA Has Put The Internet And Our Security At Risk,” Techdirt, <https://www.techdirt.com/articles/20131005/02231624762/national-insecurity-how-nsa-has-put-internet-our-security-risk.shtml>

But, really, the issue is that the NSA's actions aren't actually helping national security, but they're doing the exact opposite. They're making us significantly less safe. Bruce Schneier made this point succinctly in a recent interview: The NSA’s actions are making us all less safe. They’re not just spying on the bad guys, they’re deliberately weakening Internet security for everyone—including the good guys. It’s sheer folly to believe that only the NSA can exploit the vulnerabilities they create. Additionally, by eavesdropping on all Americans, they’re building the technical infrastructure for a police state. The folks over at EFF have dug into this point in much greater detail as well. Undermining internet security is a really bad idea. While it may make it slightly easier for the NSA to spy on people -- it also makes it much easier for others to attack us. For all this talk of national security, it's making us a lot less secure. In trying to defend this situation, former NSA boss Michael Hayden recently argued that the NSA, when it comes across security vulnerabilities, makes a judgment call on whether or not it's worth fixing or exploiting itself. He discussed how the NSA thinks about whether or not it's a "NOBUS" (nobody but us) situation, where only the US could exploit the hole: You look at a vulnerability through a different lens if even with the vulnerability it requires substantial computational power or substantial other attributes and you have to make the judgment who else can do this? If there's a vulnerability here that weakens encryption but you still need four acres of Cray computers in the basement in order to work it you kind of think "NOBUS" and that's a vulnerability we are not ethically or legally compelled to try to patch -- it's one that ethically and legally we could try to exploit in order to keep Americans safe from others. Of course, that ignores just how sophisticated and powerful certain other groups and governments are these days. As that article notes, the NSA is known as a major buyer of exploits sold on the market -- but that also means that every single one of those exploits is known by non-NSA employees, and the idea that only the NSA is exploiting those is laughable. If the NSA were truly interested in "national security" it would be helping to close those vulnerabilities, not using them to their own advantage. This leads to two more troubling issues -- the fact that the "US Cyber Command" is under the control of the NSA is inherently problematic. Basically, the NSA has too much overlap between its offensive and defensive mandates in terms of computer security. Given what we've seen now, it's pretty damn clear that the NSA highly prioritizes offensive efforts to break into computers, rather than defensive efforts to protect Americans' computers. The second issue is CISPA. The NSA and its defenders pushed CISPA heavily, claiming that it was necessary for "national security" in protecting against attacks. But a key part of CISPA was that it was designed to grant immunity to tech companies from sharing information with... the NSA, which was effectively put in control over "cybersecurity" under CISPA. It seems clear, at this point, that the worst fears about CISPA are almost certainly true. It was never about improving defensive cybersecurity, but a cover story to enable greater offensive efforts by the NSA which, in turn, makes us all a lot less secure

#### Turn --- hoarding vulnerabilities makes aggressive cyber attacks MORE likely

McGraw 13--- Gary McGraw, PhD, Chief Technology Ofﬁcer of Cigital, and author of Software Security (AWL 2006) along with ten other software security books. He also produces the monthly Silver Bullet Security Podcast forIEEE Security & Privacy Magazine (syndicated by SearchSecurity), Cyber War is Inevitable (Unless We Build Security In), Journal of Strategic Studies - Volume 36, Issue 1, 2013, pages 109-119

Also of note is the balancing effect that extreme cyber vulnerability has on power when it comes to cyber war. In the case of the Stuxnet attack, the balance of power was clearly stacked high against Iran. Subsequently, however, Iran responded with the (alleged) hijacking of a US drone being used for surveillance in Iranian airspace.10 Ironically, it may be that the most highly developed countries are more vulnerable to cyber warfare because they are more dependent on modern high-tech systems. In any case, failure to build security into the modern systems we depend on can backlash, lowering the already low barrier to entry for geopolitically motivated cyber conﬂict. Defending against cyberattack (by building security in) is just as important as developing offensive measures. Indeed it is more so. War has both defensive and offensive aspects, and understanding this is central to understanding cyber war. Over-concentrating on offense can be very dangerous and destabilizing because it encourages actors to attack ﬁrst and ferociously, before an adversary can. Conversely, when defenses are equal or even superior to offensive forces, actors have less incentive to strike ﬁrst because the expected advantages of doing so are far lower. The United States is supposedly very good at cyber offense today, but from a cyberdefense perspective it lives in the same glasshouses as everyone else. The root of the problem is that the systems we depend on – the lifeblood of the modern world – are not built to besecure.11This notion of offense and defense in cyber security is worth teasing out. Offense involves exploiting systems, penetrating systems with cyberattacks and generally leveraging broken software to compromise entire systems and systems of systems.12 Conversely, defense means building secure software, designing and engineering systems to be secure in the ﬁrst place, and creating incentives and rewards for systems that are built to be secure.13 What sometimes passes for cyber defense today – actively watching for intrusions, blocking attacks with network technologies such as ﬁrewalls, law enforcement activities, and protecting against malicious software with anti-virus technology – is little more than a cardboard shield.14 If we do not focus more attention on real cyber defense by building security in, cyber war will be inevitable.

#### China wont invade Taiwan

Lo 20 --- Alex Lo has been a Post columnist since 2012, covering major issues affecting Hong Kong and the rest of China. A journalist for 25 years, he has worked for various publications in Hong Kong and Toronto as a news reporter and editor. He has also lectured in journalism at the University of Hong Kong, “China invade Taiwan? You must be joking”, SCMP, Oct 24th 2020, https://www.scmp.com/comment/opinion/article/3106893/china-invade-taiwan-you-must-be-joking?module=perpetual\_scroll&pgtype=article&campaign=3106893

Suddenly, some very important people in the West are warning mainland China may invade Taiwan. It reminds me of other Western VIPs who thought the People’s Liberation Army would roll in the tanks at the height of violent unrest in Hong Kong last year.

Back then, sensible local businesspeople and informed expatriate commentators had argued otherwise. Doing so would mean the PLA had to take over the city, and Beijing would have to take ownership of all of the city’s domestic problems.

Similarly, despite Beijing’s sabre rattling, they won’t invade Taiwan without provocation. In any case, should it happen, it wouldn’t be an “invasion” but a civil war, something that strikes terror in the heart of every Chinese.

Influential Financial Times columnist Gideon Rachman warned, though, that “a distracted US is dangerous for Taiwan”.

“The US is now consumed by the most divisive presidential election campaign in living memory,” he wrote. “Under these circumstances, the Chinese government may doubt continuing American commitment to Taiwan.

“Beijing’s window of opportunity could look even more tempting … particularly if the [November] election result is disputed and the country is plunged into a political and constitutional crisis,” he said.

Paul Wolfowitz, the former No. 2 at the Pentagon and the brain behind the disastrous Iraq invasion and occupation, wrote in The Wall Street Journal: “A Chinese invasion would present the greatest threat to global peace in a generation … [The US must] deter the threat by committing to oppose it, by force if necessary.”

Wolfowitz never seems to learn from history or his own disastrous role in it. I bet, though, that the Chinese have learned from the Vietnam war, and the Iraq and Afghanistan aftermaths, just as they did from the collapse of Soviet communism.

If a Taiwan “invasion” is difficult, pacification and occupation of the island afterwards would be much worse. Taiwan is more than twice the size of Hawaii and about the same as Hainan. Large swathes of the island could turn into highly hostile and contested terrains.

The US and its Asian allies would for sure support a destructive insurrection for years to come. Diplomatically and militarily isolated, mainland China would end up wasting national resources and Chinese lives with no end in sight. If Vietnam was bad for the US, Taiwan would be 100 times worse for China.

President Xi Jinping could kiss his Chinese dream goodbye. Short of an outright declaration of independence by Taiwan, Beijing cannot afford a civil war.

#### Deterrence not key to prevent Taiwan war

Lungu 21 --- Andrei Lungu is president of The Romanian Institute for the Study of the Asia-Pacific (RISAP), “Taiwan invasion doesn’t hang in the military balance”, East Asia Forum, Aug 19th 2021, https://www.eastasiaforum.org/2021/08/19/taiwan-invasion-doesnt-hang-in-the-military-balance/

There is growing speculation and alarm about a possible Chinese invasion of Taiwan after Beijing sharpened its rhetoric towards the Taiwanese government and increased its military manoeuvres around the territory. The Biden administration is worried that if Chinese leaders are overconfident in China’s growing power and assume Washington’s decline, they might decide to invade Taiwan.

The US government has taken numerous actions to clearly signal its capacity and commitment to defend Taiwan. Growing diplomatic engagement with Taiwan, increased military manoeuvres, joint statements alongside Japan, South Korea and the G7, as well as developing a common response to a war over Taiwan with Japan and Australia are all part of this new framework.

Although these actions intend to decrease the risk of military conflict by strengthening military deterrence, they are unlikely to achieve it. This is because Beijing’s Taiwan calculus — which has always been more complex than simply focussing on the conventional military balance — involves three distinct factors that have dissuaded a Chinese invasion.

The first is military power. Chinese leaders still doubt whether China could defeat and then conquer Taiwan, let alone successfully fight the United States.

Secondly, there is an understanding that war over Taiwan would portend disastrous consequences for China’s economy, foreign relations and global image. Worse still, a conflict could pose an existential risk to the Chinese Communist Party: a war would mean fighting and killing ‘brothers and sisters’, while defeat would bring echos of 1895. A war would also undermine economic development — a pressing goal that is closely linked to the ‘great rejuvenation of the Chinese nation’.

The third factor is time. Chinese leaders wait based on the hope that ‘peaceful reunification’ is still possible and that time is on their side, as China’s power is growing. Their historical goal has been to prevent independence or a change of the status quo. Waiting still makes sense, as China is pursuing its decades-long military modernisation process.

By ignoring these last two factors, Washington risks focussing too much on the assumption that Chinese leaders have become overconfident about the erosion of military deterrence. Fear of the United States was never the sole factor preventing a Chinese invasion in the first place.

Hong Kong illustrates this thinking well. Without having to contend with the possibility of an opposing military, Beijing remained acutely aware of the economic and diplomatic consequences of sending military or paramilitary troops to directly suppress protests. It instead adopted a slower strategy of tightening control to reduce the political costs of its actions.

Beijing only imposed national security legislation on Hong Kong when the problem had gotten ‘out of hand’ — not as a proactive measure. The Chinese leadership tried to gradually build control over the territory for years, believing time was on its side. It only implemented radical measures when it believed the status quo was changing to its detriment.

Chinese leaders haven’t yet decided that an invasion of Taiwan is unavoidable because they still hope that ‘peaceful reunification’ is achievable, but they worry about Taiwan’s steady drift towards the United States. Beijing sees Washington’s growing ties with Taiwan as undermining the status quo and diminishing the prospects for ‘peaceful reunification’.

## Aff A2: CPs

### A2: DoD PICs

#### Note --- more aff ev is in the core file

#### CYBERCOM does intel gathering

Mizuhiro 22 --- Keisuke Mizuhiro, Visiting Research Fellow at the Institute of National Strategic Studies (INSS) of National Defense University (NDU), “Prospects for U.S.-Japan Cyber Cooperation: Critical Infrastructure Protection and Joint Operations Perspectives”, April 12, 2022, https://inss.ndu.edu/Media/News/Article/2997363/prospects-for-us-japan-cyber-cooperation-critical-infrastructure-protection-and/

Military cyber differences are even more pronounced, and with significant implications for bilateral cooperation between allies. Over the past decade, the U.S. military's role in cyberspace has been substantially strengthened. In 2010 a U.S. Cyber Command (USCYBERCOM), previously two sub-unified joint task forces under US Strategic Command (USSTRATCOM), was designated a unified four-star command and combined under the Director, National Security Agency (NSA) and focused on support of global networked cyber operations planned and executed by and through the US Combatant Commands. In 2018, USCYBERCOM was upgraded to a Unified Combatant Command. Still joined with NSA under a single 4-star commander, USCYBERCOM now has the responsibility for developing cyber-unique, global operations planned and conducted with the support of other US military commands. In this role, USCYBERCOM focuses on intelligence gathering, deterrence, and counterattack in cyberspace. As of 2019, USCYBERCOM consists of 133 teams and 6,200 personnel, including the Cyber National Mission Force (CNMF) which is tasked with deterring cyber attacks from China, Russia, Iran, and North Korea.

#### CYBERCOM responsible for sharing intel with allies

LOPEZ 19 --- C. TODD LOPEZ, writer at the U.S. Department of Defense, “Persistent Engagement, Partnerships, Top Cybercom’s Priorities “, MAY 14, 2019, https://www.defense.gov/News/News-Stories/Article/Article/1847823/

Air Force Maj. Gen. Charles Moore Jr., the command’s director of operations, spelled out several focus areas Cybercom has pursued in its first year as a unified combatant command. Chief among those priorities, he said, is “persistent engagement” -- being fully engaged with adversaries in the cyber domain, full-time.

“We recognize and understand the importance of being in constant contact with the enemy in this space, especially below the level of armed conflict, so we can defend ourselves and impose cost,” Moore said.

Persistent engagement also involves persistent presence -- the sharing of information to enable partners -- and persistent innovation of technology and techniques with partners that include other government agencies, allied nations and industry, Luber said. Both are critical to Cybercom’s success as it moves into its second year.

### A2: Adv CP

#### NRC fails --- too many differences

Robert G. Papp 19. Retired in 2017 after service as a naval officer and a career in federal civil service, including as director of the Center for Cyber Intelligence at the Central Intelligence Agency. PhD from Columbia University. “A Cyber Treaty with Russia”. https://www.wilsoncenter.org/sites/default/files/media/documents/publication/kennan\_cable\_no.\_41.pdf

Prospects for meaningful cyber negotiations with the Russian Federation, let alone a bilateral agreement or cyber treaty, seem almost impossible to imagine today. Our anguish over Russia’s meddling in American elections, preoccupation with alleged ties between the Trump administration and the Russian government during the recently concluded Mueller investigation, and major disagreements on geopolitical issues including Ukraine, Syria, and Venezuela, have left us at an impasse. Instead of genuine dialogue between the United States and Russia, we see the two nations talking past each other and posturing to both domestic and international audiences.

More alarmingly, the very framework of bilateral and multilateral arms control treaties that got us through the last decades of the Cold War, starting in 1972 with the Anti-Ballistic Missile (ABM) Treaty and the interim Strategic Arms Limitation Agreement (SALT I), is in disarray. This process of unraveling likely began in 2002 when the U.S. withdrew from the ABM Treaty. The Russian Federation suspended its participation in the1992 Conventional Armed Forces in Europe Treaty in 2007 and completely halted its participation in 2015. Most recently, the U.S. announced, on February 22, 2019, its intent to withdraw from the Intermediate-Range Nuclear Forces (INF) Treaty signed in 1987.

Given these developments, proponents of treaties with Russia, whether bilateral or multilateral, now seem few and far between. Even the architects of past agreements must justifiably wonder what has become of their life’s work. How, then, might negotiations leading to a cyber treaty be a viable policy option?

#### CP fails --- cant be enforced

Scott Neuman and Greg Myre 21. Scott Neuman Writer/Editor, Digital News @ NPR. Greg Myre National Security Correspondent @ NPR. "Hacks Are Prompting Calls For A Cyber Agreement, But Reaching One Would Be Tough". NPR.org. 7-2-2021. https://www.npr.org/2021/07/02/1009925791/hacks-are-prompting-calls-for-a-cyber-agreement-but-reaching-one-would-be-tough

Such discussions have been kicking around for years, but many cyber experts remain deeply skeptical that such an agreement could be reached, let alone enforced.

Cyber strikes are low-cost and high-reward

The first big challenge would be simply getting everyone to agree to the rules. Russia, China, Iran and North Korea have all been blamed for significant hacks against the U.S., and analysts say those countries see cyber strikes as cheap, effective and easy to deny.

It's not even clear if such countries would be willing to actually agree to terms, because cyber attacks for them are "really useful in their geopolitical positioning," April Falcon Doss, a former National Security Agency official who now heads a technology program at Georgetown's law school, tells NPR.

Compared to the arms agreements between the U.S. and Soviet Union, a cyber treaty would be extremely difficult to monitor and enforce. That's because the production, development and stockpiling of nuclear, biological and chemical weapons is fundamentally different from the ephemeral nature of cyber weapons, says Doss.

"If the question is whether or not a signatory to a nuclear arms control treaty is building up their nuclear stockpile, there will almost certainly be some evidence, factory production, storage of nuclear weapons," she says. "There will be satellite imagery or there will be on the ground reports."

Tests of nuclear weapons or ballistic missiles, such as those carried out by North Korea in recent years, are also relatively simple to monitor compared to the challenge of keeping an eye on the dark corners of the Internet to track down new cyber weapons, Doss says.

"Detecting their development is much harder because you don't have big stockpiles of missiles sitting around and there's nothing that's visible in that sense," she says.

Thomas Graham, a U.S.-Russia expert at the Council on Foreign Relations, says any analogy to a Cold War-style arms agreement would be tenuous.

"We're dealing with computer code. So this is radically different from some nuclear weapons," he tells NPR.

## Aff A2: Ks

### A2: Security K

#### Our securitization was good AND no generic links

Samuel Carruthers 19, Faculty of Social Sciences at Charles University, “Countering Disinformation: A Case Study of Government Responses to Russian Information Warfare,” Master’s Thesis, 2019, Institute of Political Science, https://dspace.cuni.cz/bitstream/handle/20.500.11956/110029/120343310.pdf?sequence=1

Ethics of Securitization

As discussed in the literature review, securitization is most often discussed as a ‘negative’ concept for several reasons. First of all, securitization argues that the normal democratic procedures for decision makers be abandoned in favor of a streamlined decision-making process handled by a small elite that dictate policy on security related issues. Critics assert that securitization is something largely inconsistent with the openness and accountability that liberal democratic systems value, therefore securitization is something ‘negative’ to be avoided in societies that place true importance on these values. But what if the issue being securitized is a direct threat to those very democratic procedures themselves. Are there issues that deserve to be securitized for the common good, and can government policies have a positive impact on society when these issues are securitized?

Experts on disinformation warn of the dire potential that such propaganda can have on a society, and argue that liberal democracies are especially vulnerable to them. New technologies have made the 21st century into a completely different type of information space than its predecessor. The internet has decentralized and democratized the flow of information to the point where somebody sitting on a laptop at home may be able to make the same impact with a blog as a major newspaper with an article. With less institutional control and traditional media gatekeeping on the flow of information, the internet is a truly democratic platform.148 These democratic processes; freedom of information, freedom of speech, freedom of the press, and free elections; are precisely what make liberal democracies so vulnerable to disinformation and propaganda. With knowledge of these asymmetric vulnerabilities, the Kremlin consciously aims “to take advantage of the free flow of information in a democratic society, the effect of that information on public opinion, and the electoral mechanisms through which public opinion determines a country’s leadership.”149

One foundation of a democratic society is the ability to make decisions in the public forum based on shared truth. When voters go to the polls, they may make a judgement on which candidate or which proposal they favor based on the information that they have consumed. Traditionally, they may differ on what course of action may be the best way to handle a problem, but there is an agreed upon reality that is a matter of fact; it is shared. Disinformation, from Russia and other actors hostile to the West, promotes falsehoods to the point where society cannot have a shared truth. Imagine four people each with a different source of news. One reads the New York Times, one watches Fox News, one reads Breitbart, and one watches RT. Each one of these people will not only come to radically different conclusions about what solutions are best for society, but also about what the basic facts of reality are in the first place. One person may be out on the streets protesting the disappearance and rape of a young Russian girl by Muslim migrants, while the next person may be aware that the story is a complete falsehood that never happened to begin with. Russian efforts in the EU show that these situations are not a hysterical fear-mongering reaction to new technologies and new sources of information, but that they are already a reality.

Disinformation creates a situation where people can have opposing realities because the information they consume is so radically different from that of their neighbor. Critical theory in international relations warns that securitization subverts democratic decision-making processes, but disinformation destroys these very democratic processes that are so fundamental for liberal democratic societies to function the way they are intended. It is impossible to imagine normal democratic processes solving these types of problems when those processes are being eroded by propaganda to the point where Western societies may no longer have normal democratic processes if this trend continues. In order to maintain these democratic norms, securitization may be a necessary process, even a ‘positive’ concept that can yield positive results and protect the democratic values that have propelled the European project into existence.

From the perspective of states, it is difficult to see why they would not wish to securitize the issue of Russian disinformation more. States tend to place an emphasis on matters of physical and territorial security over all else, which is why issues such as nuclear weapons, or rising military power in China, or international terrorism are prioritized in terms of security policy. States’ desire for physical security explains why these issues tend to be some of the most securitized political issues, with decisions made regarding military policy in Afghanistan by military panels rather than public referendums. Walt, arguing from the realist perspective, argues that states “place particular emphasis on the preservation of the state’s territorial integrity and the physical safety of its inhabitants.” 150 Material harm is of the utmost importance while more ethereal issues, like democratic procedures, freedom of the information space, and societal resilience towards propaganda are not prioritized in the same way. Disinformation has threatened some of the building blocks of democratic societies throughout the EU, and if these democratic systems fail, it isn’t difficult to imagine that physical security would come under threat as well. In the case of Spain, the issue of the Spanish government’s territorial sovereignty over Catalonia was attacked by Russian disinformation, exacerbating the political wounds of the independence referendum. The disinformation campaign questioned Spain’s fundamental right to exist in its current form, yet Spain did not place the integrity of their media space as an important security issue despite this. There needs to be a shift in the importance and value that European democracies place on the fundamental democratic principles that allow their system to flourish. They should be prioritized with the same importance that states place on more traditional measures of power. Securitization of disinformation with the liberal democratic system and democratic processes themselves as the referent object, has the potential to have a more ‘positive’ outcome than emphasis on hard power, or immigration, or other issues that contribute to the ‘negative’ conception of securitization.

Successful Securitization and Societal Resilience

In the case studies it is clear that some European countries have securitized Russian disinformation while some have not. Namely, the United Kingdom and Lithuania have successfully securitized disinformation, while Spain, Germany, and the supranational institutions of the EU have not securitized disinformation. Those that have not securitized, have identified Russian disinformation as a perceived security threat and have several securitizing actors currently at play. The potential audiences of the securitizing speech acts, those within the security apparatus, NGOs, think-tanks, and even the wider public of these countries have accepted that Russian disinformation is a security threat that warrants greater action by their governments. Thus far, they have not taken measures that could by any means be considered extraordinary, having allocated a relatively small number of resources and minimal effort towards combating disinformation, and therefore cannot be considered to have securitized the issue. These countries, and the EU, are possibly in the early stages of the process of securitization, though this does not necessarily mean that they will complete the process by taking more extraordinary measures against disinformation. In fact, there could be a reversal and disinformation could slip back into the realm of normal politics and become desecuritized.

Some clear trends emerge in the countries who have successfully securitized disinformation. First, propaganda narratives have a weaker effect on society when disinformation has been securitized, failing to have their desired impact and cause major rifts in the public. They also show that securitization of disinformation is possible without implicitly violating democratic norms of freedom of speech and open access to information. This becomes clear in looking at the contrast between Lithuania’s countermeasures against disinformation compared to those of Germany and Spain. In Germany, the Lisa case was dealt with almost exclusively via the normal criminal and legal channels, with the police investigation into Lisa’s accusations of kidnap and rape by migrants and police handling of most public statements related to the controversy. 151 They have begun to enact minor laws that aim at punishing hate speech and disinformation when posted on popular social media platforms as well.152 Spanish authorities have started task forces devoted to alerting the national government when disinformation narratives start to dominate a story online. 153 Spanish and German officials at the higher levels of national authority in their respective foreign and defense departments gave minimal statements regarding the controversies, and have preferred to continue dealing with Russia through dialogue over more overt confrontation that could complicate communication. Both Germany and Spain have taken a more reactive approach to countering disinformation, choosing to deal with it on a case-by-case basis as an incident unfolds.

Lithuania has taken similar messages to alert national authorities on dangerous narratives as they develop online, but it has also taken extraordinary measures that encompass a broader scope. The Lithuanian government has supported efforts at every level of society; political, economic, educational, and cultural. 154 Their wide spread programs focus not only on dealing with each case as it emerges, but also on strengthening the fundamental resilience of society at the source through teaching media literacy in secondary schools, funding Russian language media for the susceptible minority group, and sensitizing the public to the dangers of propaganda by making disinformation a security issue linked to the physical security and existence of the state.155 Their bans on Russian media channels during disinformation campaigns, while possibly construed as violations of a free press, are necessary to prevent media from spreading out right falsehoods. The news media, both Lithuanian and Russian language, should be held accountable and has a responsibility to act as a gatekeeper of the truth. Many media channels in Lithuania have voluntarily chosen to follow such a route, choosing not to report on ‘fake’ news stories that can be detrimental to society by becoming ‘real’ news through regurgitation by legitimate media outlets. It is important not to confuse the right of free speech of an individual with that of a news organization with ties to a foreign country, and such acts should not be considered violations of democratic norms when it comes to protecting the fundamental values of democracy.

The countermeasures taken by a country undoubtedly play a role in the impact disinformation narratives may have in that country. With Lithuania’s ‘successful’ securitization of disinformation, fake stories and attempts at propaganda have often fallen on deaf ears, with little real success. Lithuania’s overarching, comprehensive strategy at countering disinformation is the reason the NATO rape allegations failed to cause a large disruption in the news cycle.156 This strong contrast is seen with Germany, where the story of a rape by migrants of a young Russian girl caused an uproar and led to protests in Berlin and a diplomatic row with Moscow. 157 Spain also fell short, with Russian disinformation exacerbating a contentious independence referendum in Catalonia and influencing public opinion at home and abroad on the status of Catalan autonomy. Government policies that fail to securitize disinformation and alert society to the dangers of propaganda lead to false stories having explosive consequences.

Both Spain and Germany’s strategies of dealing with disinformation narratives as they arise is simply not effective enough. The state can spend time and resources trying to discredit every fake news story that finds its way to the public forum, but there will always be one to take its place. It is like fire prevention; a fire alarm can be an important part of fire prevention, alerting the fire department to come extinguish a blaze. But there are more important measures as well, such as building structures with fire resistant materials, or teaching people what to do in case of a fire. These types of continuous measures, like the policies Lithuania pursues, make society more resilient and prevent disinformation from causing a fire in the first place.

Policies aimed at improving societal resilience towards disinformation are being utilized in other countries with successful outcomes as well. Latvia uses a sweeping media literacy program from an early age to improve critical thinking in its citizens.158 Finland, a country with a long history of hostility with Russia, uses similar programs, emphasizing not only the need to publicly correct false narratives, but also the importance of creating a positive counternarrative to disinformation that is repeatedly applied to offer an alternative vision.159 These countermeasures only appear in countries that have securitized disinformation, as Finland and Latvia have similar histories as Lithuania and treat disinformation in similar terms, and they are much more promising than government authorities attempting to play catchup with internet trolls and false stories.

Internationalization of Countermeasures

Another key conclusion comes from the other case of successful securitization in the United Kingdom. The UK, in its securitization of disinformation following the assassination attempt on Sergei Skripal, internationalized the threat by creating a set of countermeasures that could be implemented along with its allies. The UK successfully convinced 20 allies to expel Russian diplomats in a coordinated effort at punishing Putin’s regime for the incident and the subsequent disinformation surrounding it.160 Theresa May, as a securitizing actor, not only convinced her public in the UK of disinformation as a security threat, but convinced the international community that such behavior “threatens the security of us all.” 161 Compared with the minimal Spanish attempts at coordinating counter disinformation at the EU level, and German attempts to keep the Lisa Case under the authority of Berlin’s police department, British efforts at securitizing their incident by bringing it to the attention of the international community and launching a unified response were highly successful.

This lesson of internationalization should be critical for the EU to deal with disinformation. Securitization needs to take place not only at the national level of member states, but also at the supranational level of the EU as an institution. The EU itself is under threat of Russian disinformation just as much as individual member states, with experts warning of further regionalization of Europe and the EU after Brexit. In this critical time for the continued existence of the EU, the threat of disinformation “requires new international instruments to manage it.” 162 Thus far, member states have shown a preference for taking individual routes in order to deal with disinformation. The importance of joint initiatives could be especially important during elections, a time in which the ability of national and EU authorities to cooperate is critical. During the European elections of 2019 for example, consisting of four days of simultaneous elections across 28 individual member states, “the failure of one government to properly mitigate disinformation efforts threatens the credibility of the entire electoral process.” 163 This problem of coordination cannot be understated, as some countries do not even have their own systems in place to monitor disinformation, allowing “local and national actors to spread fake news more freely” and leaving these countries defenseless against propaganda.164

It is essential for the EU to act as a bloc and start joint initiatives to counter disinformation. Russian efforts, as shown in the case studies, are not exclusive to one particular area of Europe, but threaten all member states. Issues Russia chooses to target; the migrant crisis, espionage, the use of chemical weapons in a member state, the solidarity and legitimacy of the NATO, and even the territorial sovereignty of some countries; should alarm every single member of the EU. These issues are not unique to one country, but they are issues that countries even outside of the EU are currently confronting. Europe is targeted as a bloc, and therefore it should respond as a bloc. Such a response, as seen in with the UK’s diplomatic expulsion, has a larger impact as a bloc rather than individually. Division will only encourage more provocations. Acting on a unified front in securitizing disinformation and reacting with countermeasures will do much more to potentially deter Russia from continuing down the same path in its relations with Europe. The EU needs to stop hesitating, and start throwing its full weight on the economic, political, and informational fronts.

‘Positive’ Securitization

The two trends discussed in the sections above also show that disinformation can be securitized without wide violations of democratic norms and exclusionary tactics towards Russian minorities in Europe. By arguing for securitization, this paper is not arguing that democratic principles should be thrown out in favor of extraordinary measures that subvert the democratic process, indeed the democratic process is of the utmost importance because these principles are the referent object of a European push to securitize disinformation. And according to polls in all of the countries involved in the case studies and the EU as a whole, the general public agrees that disinformation constitutes a security threat that could be detrimental to liberal democratic norms. Efforts like media literacy, cooperation with news organizations, and comprehensive strategies that deal with disinformation at every level of society are still extraordinary without necessarily violating democratic norms. These policies aim to sensitize the public to disinformation. They do not aim to monitor the public in a surveillance state and punish individual views that are unfavorable to European states. On the other hand, these policies are not afraid to prevent large news outlets from spreading lies that harm the ability to make democratic decisions based on shared truths. Diplomatic expulsion and unprecedented international cooperation on information issues are extraordinary measures taken without abuse of state power as in the War on Terror. Policies that aim to provide alternative news sources to Russian speaking minorities in Europe are not exclusionary ‘othering,’ but are inclusive and offer a broader, diverse, and more positive view of the Russian diaspora than as a monolithic fifth-column prone to side with Moscow and Putin’s regime over their new homes. These policies need to be inclusive to mitigate the risk of disinformation and the subsequent disillusion with European governments. A conscious, just policy of securitization of disinformation must take democratic principles, inclusion of diverse viewpoints, and the treatment of Russian minorities into account while avoiding the misuse of state power in order to succeed.

#### Hybrid warfare disrupts NATO’s ontological security---reproduces the narrative of the “other” and turns the K---strengthening collective identity solves

Bahar Rumelili 15, Professor and Jean Monnet Chair at the Department of International Relations, Koc University, Istanbul, “Identity and desecuritisation: the pitfalls of conflating ontological and physical security,” Journal of International Relations and Development volume 18, pages52–74 (2015), https://link.springer.com/article/10.1057/jird.2013.22

With regard to ontological security, the distinction between security and insecurity is the more critical one. In a state of ontological insecurity, the Self experiences instability and uncertainty of being. Ontological insecurity refers to a state of disruption where the Self has lost its anchor for the definition of its identity and, consequently, its ability to sustain a narrative and answer questions about doing, acting, and being (Kinnvall 2004). It may arise from deep uncertainty (Mitzen 2006a) and/or from the failure to have its sense of Self affirmed by others (Zarakol 2010). Conversely, in a state of ontological security, the Self experiences a stable, certain, and consistent social existence, where it remains in control about its identity and capacity for action. While I do not rule out the possibility of a state of ontological asecurity, where the Self is simply not concerned with the stability and certainty of its identity, I do not explore this possibility and how it varies across different states of physical security in this article.

Having identified different states of physical and ontological security, I make the further assumption that since ontological and physical security are distinct, states of security do not vary uniformly across the ontological and physical layers of security. One can be at a state of physical insecurity while being at a state of ontological security, and vice versa. Consequently, Table 1 charts out the four possible states of security based on the conception of security as both ontological and physical.

The state of ontological insecurity/physical (in)security is one where the Self experiences concern about physical harm and the instability and uncertainty of its being. Ontological insecurity tempts actors to engage in practices that mark Others as not only different, but also as morally inferior and threatening (Campbell 1992). Ontological insecurity and physical (in)security reproduce one another. As actors seek ontological security through constructing Others as threats to their security-as-survival, they mobilise their physical defences in the pursuit of physical security through representing the sources of threat as different and morally inferior.

Similarly, in a state of ontological security/physical (in)security, actors experience stability and certainty of being in a relationship where the Other is constructed as threat to their security-as-survival. Consequently, they remain locked into conflict-producing routines to maintain their certainty of being (Mitzen 2006a). In protracted conflicts such as in Cyprus and Israel/Palestine, this state of security sustains a stable Self/Other relationship based on enemy roles. When in such a state of security, minority and majority groups, migrants and host societies perceive and represent each other’s identities as radically different and inherently incompatible, and reproduce these perceptions and representations through acts of securitisation in order to ensure their ontological security. The states of ontological insecurity/physical (in)security and ontological security/physical (in)security are both securitised states; however, whereas the former compels actors to construct new narratives of difference and threat and engage in the securitisation of new issues to regain their certainty and stability of being, the latter compels actors to reproduce the existing narratives and continue the securitisation of existing differences and conflicts to maintain it.

The state of ontological security/physical asecurity is certainly the most attractive state of security from a normative point of view. Security communities in international relations, and in particular, the European non-war community (Wæver 1998) and the Nordic community (Browning and Joenniemi 2012) constitute the best examples of such a state of security in international relations. A collective identity discourse makes it possible for states in security communities to maintain the us/them distinctions, which are necessary for the certainty and stability of being, while remaining in a state of physical asecurity vis-à-vis one another (Mitzen 2006b; Browning and Joenniemi 2012). In this state of security, conflicts are sustainably resolved; issues that have propelled conflict in the past are either settled or have shed their physical security-ness, and are negotiated in normal political channels. Yet, identity differences maintain their ontological security-ness as groups reproduce their distinct identities through various social and cultural practices.

#### Hybrid warfare disrupts NATO’s ontological security---contingency planning solves by isolating NATO from existential fear

Maria Mälksoo 18, Senior Lecturer in International Security at the Brussels School of International Studies, University of Kent, “Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO,” European Security, 27:3, 374-392, https://dl1.cuni.cz/pluginfile.php/772169/mod\_resource/content/0/malksoo.pdf

Hybrid warfare indicates a multitude of possible contingencies, generating anxiety about one’s ability to remain oneself and to continue to act. It is thus linked to “anxiety over the vulnerability of [Western] power” (Bell 2012, pp. 230–231), threatening the West about losing its particularistic form of existence (cf. Creppell 2011, p. 455). Anxiety, in contrast to fear, which per Giddens (1991, p. 43) constitutes a response to a specific threat, concerns “perceived threats to the integrity of the security system of the individual” (Giddens 1991, pp. 44–45, cf. Browning and Joenniemi 2017, p. 38; Rumelili 2015). OS-seeking aims to mitigate the effects of such hard uncertainty, bringing it within bearable limits (Mitzen 2006, p. 346). Routines are instrumental here, as they “pacify the cognitive environment … ‘inoculating’ individuals against paralytic, deep fear of chaos” (Mitzen 2006, p. 347).

Being able to survive the “hybrid threats” is directly pertinent to the survival of the EU and NATO as particular kinds of organisations, underpinned and driven by specific values – which cannot be sacrificed or diluted in the struggle for physical and institutional survival. Yet, hybrid warfare disturbs the OS of the EU and NATO in subtly distinct ways. Due to the particularities of their institutional set-ups and historical foundations, the OS drives of the two organisations are somewhat distinctive. NATO’s history is occasionally told through its surpassing of a sequence of crises, albeit the end of the Cold War and the collapse of its original enemy created a situation of unprecedented uncertainty and ontological insecurity for the Alliance. Meanwhile, the EU’s ontological insecurity is a more recent phenomenon, stemming mostly from the Eurocrisis and the looming possibility of a Grexit a few years ago; the refugee/migration crisis in Europe of 2015 (Dingott Alkhoper 2018; Mitzen 2018); the actual UK decision on Brexit in 2016 (Browning 2018); and the rise of populist politics within the EU (Kinnvall, Manners, Mitzen 2018) and the United States. NATO as a military alliance has been historically more accustomed to the othering practices of concrete geographical places, whereas the EU is generally regarded as an organisation that has risen above geopolitical othering, juxtaposing itself to Europe’s dark past instead (Rumelili 2018, Subotic 2018, and Della Sala 2018). Accordingly, the EU might be more at home with hybrid threat management due to its historically broader conceptualisation of security through the paradigm of intertwined risks rather than being focused more strictly on “the threat, use and control of military force” in the manner of a traditional defence alliance (Walt 1991, p. 212; Manners 2002). Regardless of its perpetual transformer’s self-image, hybrid threats represent the uncomfortable “hard” or “fundamental” uncertainty for NATO (cf. Mitzen 2006, p. 346) and are thus ontologically disturbing for the security of its self as a traditional alliance with a collective security pledge bound to “armed attack” against one or more of its member states.

In order to achieve OS, actors strive for “routinizing their relations with significant others” (Mitzen 2006, p. 342). Routines help to keep ontological fears at bay, out of everyday discursive consciousness (Mitzen 2006, p. 348). From this perspective, NATO’s naming and shaming strategy vis-à-vis Russia as part of its hybrid warfare countering strategy links the uncertainty emanating from the hybrid nature of the new threats to the known and routine relationship with its traditional antagonist.8 The incapacitating difficulties related to planning ahead in anticipating and countering hybrid engagements are thus somewhat alleviated by the latter’s attachment to a known rival. Russia’s hybrid intervention in Ukraine has concurrently provided NATO with the familiar parameters of the cognitive “cocoon” (Giddens 1991, pp. 39–40) which enables the alliance to reproduce its cognitively “knowable” world. A Mitzenian reading of NATO’s emerging response to hybrid threats/warfare thus points at the renewed routinisation of the “programmed cognitive and behavioral responses” to Russia as the alliance’s original nemesis.

Restoring traditional vigilance vis-à-vis Russia, buttressing the forward defence along the Alliance’s eastern flank with the respective military reinforcements, contingency planning and exercises, the emerging response of NATO to the hybrid menace could also be read as an attempted restoration of a known normative order for the North Atlantic Alliance. Hybrid warfare endangers the basic features of the said normative order (or that of the broadly conceived Western security community in general, including the EU as well) as its efficient countering would likely compromise the underlying principles for this order’s particularistic existence (cf. Creppell 2011, p. 450). As a threat of subversion, hybrid warfare exposes the internal vulnerabilities in the body of the traditional security alliance (NATO) and a self-proclaimed post-modern security actor (i.e. the EU; cf. Cooper 2004). This concerns, in particular, the ever-elusive (and contested) balance between national/organisational security and individual liberties (cf. Waldron 2003, Neocleous 2007), as strategic communication is inherently at odds with free speech as a core value of Western liberalism. Countering hybrid warfare is conducive of generating a security predicament of perpetual pre-emption which, by definition, would indicate pre-emptive gathering of all sorts of data, thus likely infringing on the privacy of the individuals for the sake of the organisational/regional/national security. This precautionary logic resonates with the risk society approach which characterises the struggling with a sheer volume of risks with potentially fundamental consequences as a key feature of modernity, implying that “decisions are … made not in context of certainty, nor even of available knowledge, but of doubt, premonition, foreboding, challenge, mistrust, fear, and anxiety” (Ewald 2002, p. 294).

#### Securitization of Russian disinformation is positive

Samuel Carruthers 19, Faculty of Social Sciences at Charles University, “Countering Disinformation: A Case Study of Government Responses to Russian Information Warfare,” Master’s Thesis, 2019, Institute of Political Science, <https://dspace.cuni.cz/bitstream/handle/20.500.11956/110029/120343310.pdf?sequence=1>

\*ableist language changed

Conclusion

This thesis aimed to identify similar processes occurring throughout the EU by analyzing how four individual member states have approached the issue of disinformation. In looking at incidents of disinformation in the UK, Germany, Lithuania, and Spain, research was conducted to analyze the incidents themselves and how governments responded, placing that response into the wider context of securitization within those countries. It is clear that there is an ongoing process of securitization taking place in Europe around the issue of disinformation. Not all countries researched have demonstrated that disinformation has been fully securitized, but every country had elements of securitization taking place, such as securitizing actors and speech acts meant to draw attention to propaganda as an existential security threat. While these countries did show the initial factors in securitization occurring, they chose to deal with disinformation through the route of normal politics rather than extraordinary politics. It can be concluded that the level of securitization of Russian disinformation within a society, that is the treatment of propaganda and false narratives as a security threat and how deep a country is within the process of securitization, played a direct role in shaping the policies those countries pursued in order to counter disinformation.

Examining the different cases, the research showed how history, experience, and threat perceptions related to Russia influenced securitization of disinformation. The United Kingdom securitized Russian disinformation in the aftermath of a catalyst event, the attempted assassination of former GRU agent Sergei Skripal and the subsequent disinformation campaign in its aftermath. The UK government propelled disinformation to extraordinary politics in its diplomatic expulsion of Russian diplomats coordinated with its allies. Lithuania securitized Russian disinformation over a long period of time because of its complex history with Russia and the Soviet Union, and its experience of a slow barrage of disinformation since it regained independence. Due to decades of experience, Lithuania pursues a more comprehensive strategy at countering disinformation, which seeks to address the threat at multiple levels of society and multiple stages as false-narratives spread.

It was clear that other countries, and the EU as an organization, had not fully securitized Russian disinformation, although they showed signs they were in the process of securitization. Germany, in response to a young girl’s explosive accusations of rape in the context of the migrant crisis, showed a clear preference for dealing with disinformation through the normal political channels of Berlin’s police department. Spain took minimal responses through its foreign and defense ministries and is still in the early stages of instituting policies aimed at alerting the government to disinformation narratives. As a bloc, the EU also failed to enact extraordinary policies to counteract disinformation from Europe’s Eastern neighbor, with a lack of coordination between the individual member states and the supranational EU bodies.

While some countries have securitized disinformation, other have chosen a different route, and we can see how the different policies enacted by these countries can either protect society or make society more vulnerable to disinformation. Those countries that have securitized disinformation have also had the most success in countering it. Continuous policies that not only track disinformation narratives and discredit them as they emerge on a case-by-case basis, but also build resilience at the source through policy efforts in the social, cultural, educational, and political realm have proven more effective. Media literacy, Russian language programming, and public statements exposing false stories can all have an impact. Disinformation narratives have often failed to cause the same explosive consequences in those countries that have instituted comprehensive strategies to counter it. Internationalization of counterdisinformation policies, seeking solidarity and joint initiatives with like-minded allies, has also proven more effective cultivating societies that are less vulnerable to fake news. Diplomatic expulsions, online tracking, and coordinated alert systems have the potential to ensure that the more vulnerable countries in the EU do not let disinformation exert influence on political processes and thereby endanger the bloc as a whole.

This paper has also argued against ‘negative’ conceptions of securitization in relation to the issue of disinformation. It has warned that disinformation is indeed a security threat to liberal democracies in the West, with its ability to destroy foundations of shared truth and potentially ~~cripple~~ [destroy] democratic decision-making processes. While critical IR theorists believe securitization should be avoided to protect openness and accountability, and frame the process in a negative light, this paper has argued that securitization

is a necessary protective measure and does not inherently lead to abuse of state power. Policies pursued by the case study countries that have successfully securitized disinformation prove that while still extraordinary, countermeasures against disinformation do not necessarily need to violate the democratic values they are meant to protect. These policies do not need to be exclusive towards Russian minorities, but can be inclusive and contribute to public life. If European countries and the EU as an institution value the democratic principles that govern their societies, a conscious, successful securitization of disinformation may be beneficial and even have ‘positive’ results. Viewing disinformation as a national security threat is the path forward for the EU to respond to Russia.

## Maybe relevant for a wave 2

#### Interoperability

<cite>

In the age of digitization, information systems play a more integrated and important role in modern society than ever before. This also applies to critical infrastructures that are essential for the functioning of society today. At the same time, however, these systems are becoming increasingly complex and vulnerable to attacks. It can be observed that today’s systems are mostly defended by traditional security measures that only provide basic protection against common threats. In contrast, reliable protection of systems against sophisticated and targeted attacks remains a problem and continues to intensify the arms race between threat actors on the one side and security experts on the other. To be ahead in this game, a trend towards the exchange of Cyber Threat Intelligence (CTI) information has emerged to be aware of threats at an early stage. This can either strengthen threat prevention or contribute to the mitigation of already occurred incidents and improve the overall system security.

The benefits of CTI exchanges are recognized and promoted by various governments, industry and research. This has already led to legal reporting obligations for industries that are relevant to the functioning of the society in different economic areas such as the United States1 , the European Union2 and Germany3 . At the same time, the industry has started to introduce a wide range of threat intelligence platforms such as the Collective Intelligence Framework (CIF)4 and community solutions like Open Threat Exchange (OTX)5.

But while sharing CTI undoubtedly can create benefits, there are issues on how to conduct the exchange of threat intelligence. The structure as well as the content of threat intelligence reports are essential aspects for a mutual understanding of the shared information and, therefore, for the success of the exchange itself. To support the exchange process, several organizations have developed competing formats and standards to represent CTI, which are already used by companies to some extent. The formats differ in their focus on certain CTI areas, notations and presentation concepts while actually serving similar purposes. This can lead to several issues, such as incompatibilities or comprehension problems, which may even question the whole exchange process. Uniform definitions and notations and a common understanding of the data structures is therefore an important success factor for the exchange CTI information. With this work, we make the following contributions as a step towards unification of CTI data structures:

– We introduce a meta model that describes the key elements of threat intelligence formats

– We propose a common notation for CTI base elements to support the mutual understanding for available components

– We apply our findings to a unified model, which serves as a basis for the understanding and discussion of future opportunities in the area of threat intelligence sharing

The remainder of this paper is organized as follows: In section 2 we cover the Related Work. Section 3 introduces a meta model and unified notation for CTI data structures. Section 4 introduces a unified CTI model based on the meta model and the unified notation as well as a discussion about possible starting points for improving the current situation based on this model. The paper is concluded in section 5.

#### Rift between NATO and EU

https://www.streitcouncil.org/post/bridging-the-transatlantic-cyber-rift-recommendations-for-improving-cyber-cooperation-between-nato

Information-Sharing Issues

Although NATO and the EU have made great progress improving cyber cooperation, issues with sharing information – particularly classified information – have hindered their efforts. Currently, the two organizations lack official channels for sharing classified information.[12] There are several reasons for this rift, most notably a lack of trust between NATO and the EU via different standards and practices in sharing and storing information.[13] As will be discussed below, two essential differences are the handling of private information and the use of cloud computing.

Private Information

When it comes to handling private information, EU member states are bound by the General Data Protection Regulation (GDPR), which codifies that citizens have the right to data protection and lays out rules governing how organizations can collect and store personal information.[14] However, NATO is not bound by GDPR regulations. In particular, NATO member states who are not part of the EU have zero obligations to follow these rules.[15] For example, the GDPR strengthens protections related to the “right to be forgotten,” in which EU citizens can demand that their personal data be deleted. But, the “right to be forgotten” does not exist in the US.[16] This circumstance creates concerns that NATO and its non-EU member states may not respect the privacy of EU citizens.[17] For instance, in July 2020 the European Court of Justice (CJEU) ruled that mass surveillance of digital data carried out by the US National Security Agency (NSA) violates the privacy right of EU citizens, as EU citizens have no recourse under US law to challenge the collection of their data.[18] This ruling invalidated the US-EU Privacy Shield, which was designed to allow personal data to be transferred to the US, and was a key part of transatlantic digital trade.[19]

Cloud Computing

Meanwhile, both NATO and the EU are turning to cloud computing as a platform to coordinate operations and store information.[20] However, their standards and practices are dissimilar in scope and nature. NATO’s cloud regulations are focused on ensuring security and interoperability in a military environment. Moreover, NATO’s guidelines for cloud computing include its Federated Mission Networking (FMN) standards, which “establishes the framework for cooperation between command-and-control networks for coalition forces.”[21] And FMN standards for cloud computing security mandate that all affiliates use a variety of cryptographic algorithms, including the Advanced Encryption Standard, a type of cipher that encrypts data in multiple rounds and is the standard for the US government and military.[22] By contrast, the EU’s cloud regulations are focused on ensuring cloud security for businesses and consumers. The main regulation is the EU Code of Conduct for Cloud Service Providers, which does not provide specific security measures that need to be taken, but instead mandates companies’ security be compliant with ISO 27001.[23] ISO 27001 establishes a process to create an information security management system, including creating a risk assessment system producing “consistent, valid and comparable results.”[24] In regard to government clouds, the EU does not have specific regulations, but does offer a guide for best practices using the Plan-Do-Check-Act (PDCA) model. In the PDCA’s four phases, governments first determine what they need to cloudify and what risks there are; select necessary security controls and implement them; review the measures after implementation to see what problems have arisen; and finally act on those problems.[25] Without EU-wide regulations governing military cloud computing, it is difficult for NATO to share information for fear of information ending up on clouds not compliant with its own security standards.

Recommendations for NATO and the EU

Given the lack of trust between NATO and the EU, the first step to improving information-sharing is to increase the two organizations’ faith in each other. As mentioned above, standards and practices related to collecting and storing private data and the use of cloud computing are two areas where NATO and the EU have serious differences. Therefore, creating shared standards and practices for securing classified information is the best way to bridge this transatlantic cyber rift.

Private Information

To deal with issues surrounding private information, NATO and the EU should work together to create a data protection framework for NATO that meets minimum standards to protect data. The first step in this direction is creating a permanent forum to deal with data protection issues, such as the EU-US Trade and Technology Council (TTC). In December 2020, the EU proposed the TTC to serve as a forum for the US and EU to deal with issues related to emerging technology and trade standards.[26] The TTC would bring together representatives from the European Commission, members of US departments and agencies, and private industry representatives.[27]

One of the TTC’s first remits should be to revive the US-EU Privacy Shield. This act will remove hurdles to US-EU trade, demonstrate that both sides can and will work together, and allow them to coordinate their response to the CJEU’s decision in July 2020. Another important step is creating redress for EU citizens whose data is collected by US intelligence agencies. For example, making improvements to the Privacy Shield Ombudsperson, a position created to handle complaints and provide redress.[28] In fact, the CJEU declared that the Privacy Shield Ombudsperson was ineffective because the position – appointed by the US President – lacked independence.[29] In turn, the US could agree to make the position independent by establishing a new position via Congress.[30] After the US-EU Privacy Shield is renegotiated, the TTC can act as a forum for future negotiations between the two sides, such as handling the digital standards and data privacy portion of any future trade negotiations. In addition, having the US and EU agree on standards will encourage other NATO members, and perhaps non-EU member states, to follow suit. Nevertheless, there are problems with the TTC. After all, the TTC would be a forum to negotiate on a wide variety of issues related to trade and technology, including digital taxation and 5G.[31] Thus, certain issues could derail the TTC’s discussions on digital privacy and data protection.

Cloud Computing

Meanwhile, the first step to developing shared standards and practices for military cloud computing is to develop EU standards. A sound starting point is by creating a new project to develop standards on how EU member states’ militaries use cloud computing through the Permanent Structured Cooperation (PESCO), a program in which EU member states collaborate on projects to improve security.[32] Given that NATO has much more advanced military cloud computing capabilities than the EU, NATO should assist in developing these standards and practices. For example, the Defence and Related Security Capacity Building (DCB) Initiative, which helps NATO partners, non-partners, and international organizations improve their security and defense capabilities. In theory, the EU would first request NATO’s help with cloud computing. Then, if approved via the North Atlantic Council, NATO would send funds, advisors and technical experts.[33] Furthermore, the two largest issues NATO should help the EU with are creating standards for security and interoperability. For security, this means developing standards around encryption, such as NATO recommending the EU use the Advanced Encryption Standard that it uses. For interoperability, this means ensuring all systems use a similar Application Program Interface (API), or APIs, which defines a list of possible commands and the format to issue those commands, thus allowing programs to interact with one another.[34] EU member states must also use APIs compatible with one another and with NATO member states.

The advantage of the aforementioned approach is that it allows the EU to develop cloud computing capabilities compatible with NATO – capabilities that both sides consider secure. By the same token, our approach creates a framework that the two sides can use to work together on other emerging technologies. Yet there are some problems with this proposal. First, the US may not be willing to assist the EU, as some US government officials have worried that EU military efforts will lead to “duplication, non-interoperable military systems, diversion of scarce defense resources, and unnecessary competition between NATO and the EU.”[35] The issue of duplication and non-interoperability would not be an issue here. But, the other two problems may be enough to convince US officials that cooperation is not in their best interest. The second problem is that the EU may be reluctant to seek NATO’s help, due to fears that NATO could impede digital sovereignty. A third problem is that US companies – which, in 2019, controlled about 70% of the world market – are too dominant in the cloud computing sector, and this dependence puts the autonomy of European data at risk.[36] Finally, allowing NATO to help set standards and practices may be seen as “Americanizing” European defense clouds while increasing dependence on American firms. Despite these potential setbacks, NATO and the EU must overcome mutual distrust and apprehension if they aim to conquer cyber security concerns.

Creating a Platform

Once trust has been established, NATO and the EU should create official channels to share classified information. First, these two organizations must determine what information can be shared, who can receive the information, and what sort of framework will exist for sharing this information.[37] Sharing classified information requires NATO and the EU to develop a shared classification scheme, ensuring individuals above a certain security clearance can access information. Subsequently, the two organizations would have to determine what types of devices can access the platform. For example, allowing portable electronic devices to access the platform fosters remote work, but also enables more cyberattacks.[38] The second step is to create a security architecture for this platform. One possible piece of security architecture comes from the US Department of Defense’s Comply to Connect Program (C2C). C2C verifies that a device which attempts to connect to a network is authorized to do so and is compliant with security policies.[39] This verification process prevents unauthorized users or potentially compromised endpoints from accessing classified information. C2C also monitors all devices accessing the network, allowing the administrator to know who is using the network without having to manually update a list.[40] The main disadvantage of C2C is that it is currently being used on a limited scale, and it is not entirely clear how it will work across the entire Department of Defense, much less on a transnational level.[41] But once a platform is up and running, it is necessary to create mechanisms for getting user feedback, including surveys and allowing users to submit error reports – allowing NATO and the EU to assess how well the platform is working and fix any problems that emerge.[42]

Conclusion – Bridging the Transatlantic Cyber Rift

NATO and the EU ought to create shared standards and practices for sharing information, particularly in the areas of handling private information and using cloud computing. To deal with the problem of handling private information, the two organizations should create and utilize a forum, such as the TTC. Moreover, the TTC could help renegotiate the US-EU Privacy Shield Agreement. To deal with the problem of cloud computing, the EU should create standards and practices related to military cloud computing, best done by a project such as PESCO. NATO could then assist the EU in developing these standards, using the DCB Initiative as the framework for aid. Lastly, the two organizations should create official channels to share classified information, making sure to create a shared classification system while setting up a security architecture to protect classified information. These recommendations will dramatically improve the security of both NATO and the EU, creating a groundwork for the two organizations to develop better cooperation to deal with security threats inside – and even outside – the cyber domain.

#### CBM (but is that IS with hostile actors?)

Housen-Couriel 22 --- Deborah Housen-Couriel, Chief Legal Officer and Vice-President Regulation for Konfidas Digital Ltd., a cyber and data protection consulting firm, She currently serves on the Advisory Board of the Hebrew University Law School’s Cyber Security Research Center and as a research fellow with the Reichman University’s Interdisciplinary Center Herzliya’s Institute for CounterTerrorism, Chapter 3 “Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace” in “Cyber Peace Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace”, edited by Scott J Schakelford et al, published in 2022 by Cambridge Univ Press, Pages 54-

Building on this understanding of IS as a best practice, it is argued here that IS further supports sustainable cyber peace as a CBM at the international level, among the states, international organizations, and multinational companies that are critical to ensuring global cybersecurity. The framing of IS as a CBM, rather than as a binding, substantive norm to which these entities are subject as a matter of law or policy, is beneficial to the utilization of IS platforms at the international level (Borghard & Lonergan, 2018). By sidestepping substantive multilateral commitments, IS can be more readily utilized to support cybersecurity and cyber peace. Examples where this has occurred include the UN’s 2015 GGE (United Nations General Assembly, 2015), the OSCE’s 2016 listing of cybersecurity CBMs (Organization for Security and Co-Operation in Europe, 2016), and the 2018 Paris Call for Trust and Security in Cyberspace (Principle 9).

CBMs were originally used in the context of the Cold War to further disarmament processes in the context of the diplomatic and political standoff between the USSR and the West. Nonmilitary CBMs have been defined more generally as “actions or processes undertaken … with the aim of increasing transparency and the level of trust” between parties (Organization for Security and Co-operation in Europe, 2013). They are “one of the key measures in the international community’s toolbox aiming at preventing or reducing the risk of a conflict by eliminating the causes of mistrust, misunderstanding and miscalculation” (Pawlak, 2016, p. 133). CBMs are also critical in the global cybersecurity context and have been described as a “key tool in the cyber peacebuilder’s toolkit” (Nicholas, 2017).

In a 2017 in-depth study of eighty-four multilateral and bilateral initiatives addressing the collective action challenges of cybersecurity, including treaties, codes of conduct, agreements, memoranda and public declarations, IS was found to be included as an agreed cybersecurity measure in more than 25 percent of such initiatives (twenty-one out of the total eighty-four) (Housen-Couriel, 2017, pp. 51–52). Moreover, the analysis was able to isolate several specific elements of IS, discussed above, that were individually included in this top quarter: IS measures in general15; establishment of a specific national or organizational point of contact for information exchange; and sharing of threat indicators (Housen-Couriel, 2017, pp. 51–52).16 These elements were three out of a list of a dozen CBMs that occur with sufficient frequency to be included in a “convergence of concept” with which diverse stakeholders – states, regional organizations, intergovernmental organizations, specialized UN agencies, standards organizations, private corporations, sectoral organizations, and NGOs – have incorporated into cybersecurity initiatives.17 The study concluded that, while such cyberspace stakeholders are frequently willing to incorporate general arrangements for IS (it is in fact the leading agreed-upon cyber CBM in the initiatives that were studied), and even to specify a national or organizational point of contact, they are less willing to commit to a 24/7, real-time exchange of cybersecurity related information (Housen-Couriel, 2017, p. 67). This finding indicates a gap that should be considered in the context of further leveraging IS in the context of cyber peace.

Nonetheless, as noted above, IS as a CBM holds the advantage of bypassing the present, considerable challenges of achieving formal and substantive multistakeholder agreement on substantive cyber norms, until such time as such binding norms are legally and geopolitically practicable (Efroni & Shany, 2018; Finnemore & Hollis, 2016; Macak, 2017). A few examples of binding domestic law and international regulatory requirements for organizational participation in IS platforms do exist, such as the pan-EU regime established under the EU NIS (Directive 2016/1148), the Estonian Cybersecurity Act of 2016, and the US Department of Defense disclosure obligations for contractors when their networks have been breached. However, there are many more based on voluntary participation, such as the CISCP and FS-ISAC reviewed above, Israel’s FC3, and the global CERT and CSIRT networks of 24/7 platforms for cyber threat monitoring, including the EU network of more than 414 such platforms (European Union Network and Information Security Agency, 2018).

For the purposes of its analysis in this chapter, IS constitutes as a nonbinding CBM that also constitutes a best practice for bolstering cybersecurity and cyber peace, yet does not require a binding legal basis for its implementation. The critical issue of the use of regulatory measures, both binding and voluntary, to promote IS for optimal cybersecurity and cyber peace is, as noted above, an issue for further research.

#### “Improved information sharing is a way to help drive situations rightward along the …”

<https://cyberdefensereview.army.mil/Portals/6/Documents/2022_spring/03_Ford_CDR_V7N2.pdf?ver=jPNxXAqiUZX7kFHLgxwpUw%3D%3D>

#### Maybe an advantage

A Shared Cyber Threat Intelligence Solution for SMEs

#### Aff

<https://books.google.com/books?hl=en&lr=&id=uYiRDgAAQBAJ&oi=fnd&pg=PA237&dq=disclosure+of+zero-days+weakens+cyber+capabilities&ots=gLT2K-6akz&sig=RDsrDbaS-UABlUofUZzCDMTA_yk#v=onepage&q=disclosure%20of%20zero-days%20weakens%20cyber%20capabilities&f=false>

#### Interop

https://www.civilaffairsassoc.org/amp/the-rhetoric-vs-the-reality-understanding-nato-s-capacity-to-address-russian-gray-zone-conflict

Despite this, examples of solidarity remain the exception, as challenges persist between NATO nations to integrate capabilities. First, there is no alliance-wide synergy of response tools enabling NATO nations. The 2015 Strategy on NATO’s Role in Countering Hybrid Warfare deferred on this, conceding the primacy of individual nations over collective action in countering hybrid acts.[18] Thus, several controlled technical resources are restricted to national use and remain unavailable to NATO formations.[19] Intelligence collection also remains varied between states. Intelligence sharing, a major tool in attributing hybrid threats, also remains limited. For example, there is not an Alliance-wide technical architecture for sharing near-real-time intelligence, especially between the NATO command structure and its subordinate formations. Protocols defining appropriate response options are limited and delineated command authority in multi-domain operations clarifying suitable, or legally appropriate responses to threshold activities are non-existent. This is especially challenging when Russia’s gray-zone behavior bypasses the norms of democracy and the rule of law abided by the US and NATO.