# Wave 1 – Aff Compiled

## Adv 1 – OCOs

### UQ – Integration

NATO has intent to integrate offensive cyber operations now but its request-based system undermines efficacy – unification of protocols and intel-sharing is key

Lonergan and Montgomery 22 – Dr. Erica Lonergan is an assistant professor in the Army Cyber Institute at West Point. She is also a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University. Erica previously served as a senior director on the Cyberspace Solarium Commission. Retired Rear Admiral Mark Montgomery, US Navy, is the senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies. Mark previously served as the executive director of the Cyberspace Solarium Commission. ("Pressing Questions: Offensive Cyber Operations and NATO Strategy"; Modern War Institute; https://mwi.usma.edu/pressing-questions-offensive-cyber-operations-and-nato-strategy/; 1-25-2022, Accessed 6-24-2022)//ILake-AZ

Offensive Cyber Operations in NATO Strategy Above and Below the Level of Warfare

Historically, NATO’s cyber posture has largely focused on defense and resilience—and this continues to form the bulk of NATO’s approach. The alliance maintains that its “main focus in cyber defence is to protect its own networks (including operations and missions) and enhance resilience.” At the 2014 Wales summit, NATO endorsed the Enhanced Cyber Defence Policy, which affirmed that cyber defense is part of collective defense and that the alliance would incorporate cyber defense into its planning and operations. In 2016, NATO members pledged to improve their cyber defenses through training, education, exercises, and information sharing.

But the seeds were also planted in 2016 for NATO to consider a potential role for offensive cyber operations. That year, the alliance recognized cyberspace as a domain of military operations, comparable to land, sea, and air. At the 2018 Brussels summit, NATO began to more seriously consider offensive cyber operations. Specifically, NATO created the Cyberspace Operations Centre to coordinate requests for member states to provide offensive cyber effects through the Sovereign Cyber Effects Provided Voluntarily by Allies process. Following the 2018 summit, then-Secretary of Defense James Mattis stated in a press conference that five states—the United States, the United Kingdom, Denmark, the Netherlands, and Estonia—were contributing cyber forces to “help NATO fight in this important domain.” More recently, in June 2021, NATO convened in Brussels and committed to a Comprehensive Cyber Defence Policy. A key feature of the new policy is the prominent role of offensive cyber operations. In Brussels, member states committed to “employ the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats.”

NATO’s shift to incorporating offensive cyber operations into existing strategy and policy has focused on integrating offensive effects into conventional military plans and operations in the context of a conflict. While NATO’s updated strategy is a positive development,—particularly the mismatch between the alliance’s clear distinction between wartime its limited focus on conflict scenarios for employing cyber power fails to accurately account for the cyber threat environment NATO faces and peacetime and the approach of adversaries like Russia, who adopt a competition-conflict continuum. Additionally, the focus on employing offensive cyber during a high-end conventional fight is also not consistent with how several NATO members are already engaged in gray zone offensive cyber operations.

The primary threat to NATO allies in the cyber domain is not from high-end, decisive cyberattacks. Instead, cyber threats more frequently and effectively manifest as gray zone tactics designed to have a corrosive effect without rising to the level of warfare. There are numerous examples of this type of threat. For instance, in July 2021, NATO publicly condemned a range of malicious cyber behavior, including the Microsoft Exchange hack (which NATO attributed to China) and ransomware attacks targeting critical infrastructure. Russia has leveraged cyber and disinformation operations to interfere in democratic elections in the United States in 2016, 2018, and 2020; France in 2017; and Germany in 2017 and 2021—to name just a few examples. Russia also conducted distributed denial-of-service cyberattacks against government websites in Montenegro during the lead-up to, and following, Montenegro’s ascension to NATO in 2017. And when NATO forces were positioned in the Baltics beginning in 2017 as part of NATO’s enhanced forward presence, two threat actors, GhostWriter and Secondary Infektion, conducted a range of disinformation campaigns.

Additionally, the reality is that several NATO members are already speaking publicly about offensive cyber operations below the level of warfare and their statements and actions have an effect on the entire alliance. In particular, NATO member nations have not reached a political consensus about the role of offensive cyber operations. In 2018, the US Department of Defense and US Cyber Command issued new strategy and policy documents that articulated a role for the military in conducting offensive cyber operations below the level of armed conflict outside of US-controlled cyberspace (part of the “defend forward” strategy), and there has been some reporting about US offensive cyber operations. For instance, in 2018 the United States disrupted the Russian-linked Internet Research Agency from interfering in the midterm elections. And, more recently, in December 2021 General Paul Nakasone, commander of US Cyber Command, publicly acknowledged that the military played a role in disrupting ransomware groups targeting critical infrastructure. The United States has also worked with other NATO allies, such as Estonia and Montenegro, to conduct “hunt forward” cyber operations on allied and partner networks to uncover and disrupt malicious cyber activity.

Other NATO allies have also been more transparent about offensive cyber operations. In 2020, the United Kingdom announced a significant investment in its National Cyber Force, its organizational arm for offensive cyber operations, and its 2022 National Cyber Strategy emphasized the role of offensive cyber operations. In November 2021, General Nakasone and the director of Government Communications Headquarters—the UK government’s principal signals intelligence agency—stated jointly that the two governments were collaborating to “impose consequences” in cyberspace to disrupt adversary operations. The Netherlands has also publicly alluded to conducting offensive cyber operations.

Next Steps: Addressing Challenges and Mitigating Risks

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

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

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

#### Analysis of NATO countries proves opposite

Marrone and Sabatino 21 – Alessandro Marrone is the Head of the Defense Program at the Istituto Affari Internazionali in Rome and Ester Sabatino is Research Analyst for Defence and Military Analysis at the The International Institute for Strategic Studies. “Cyber Defence in NATO Countries: Comparing Models” Published 2021. <https://d1wqtxts1xzle7.cloudfront.net/65693094/iaip2105-with-cover-page-v2.pdf?Expires=1656100418&Signature=GHDFg-q6Oy29igACe~s1a00WuObIobCutomMJMI5t90rwn8AItAiAmfGvzOiRtoREH2y1Pusv9Q6VI06Pa8zA0rtsxcza1XWLk-u2djuFKb~e86ZbgwJI7~YI~gKSeH3C9dPNWTc8ikBNkD4E7bdCwlX6JjhocJu0XXlzbPO5c89uOV7FkQlQgMB1OV1WTVXOEwept~mTrHrQGZJk~Ny2YiVdNuh4qmA8kyluwEMAF~TUIOfCM-qFria7gpup2Wz4O2bC4W-D6oBREg9lqeeuU7l53Aoog196oK7F1~Fh1dBEgsvQoEhkTuox18akvt-Ar90yOWFnnBR0qTgLjK1hA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA> // DG

**The analysis** of five national case studies **has resulted in** the identification of different approaches towards cyber defence, as **proof of how much has yet to be accomplished in defining shared doctrines and procedures.** Among the countries taken into consideration, **a substantial divide can be traced between states** that envisage the possibility of carrying out exclusively defensive actions, and those that count on the ability to perform offensive operations also in the absence of a cyber-attack.

Among the first group are Germany and Spain, which envision cyber deterrence as the country’s ability to promptly and adequately respond to a cyber-attack, enacting what is defined as hack-back. Additional differences between Berlin and Madrid concern the possibility of deploying the armed forces on national territory in the event of an attack, which would need prior authorisation by Parliament in Germany. It is important to note, however, that **this procedure poorly matches the speed of reaction necessary to limit or avoid the damage of a cyber-attack**: parliamentary timeframes, in cases that require rapid and tailored actions, could mean the state’s inability to protect its primary interests and thus hinder national defence.

London, Paris and Washington, by contrast, have a different understanding of the possibilities deriving from an active use of cyber defence. For the three capitals, cyber defence and deterrence are about ensuring not only reaction capabilities in the event of a cyber-attack, but also the possibility of a preventive action against potential adversaries, be they state or non-state actors. Following this logic, for instance, the UK carried out a cyber-attack to the detriment of ISIS in 2016.

Despite these differences, it is possible to outline shared **necessities** among the five countries **take into consideration**, which can be summed up as follows: • **Necessity to have a shared regulatory and doctrinal framework at the NATO,** EU and international level; • **Better integration** of the cyber element in national **and** allied command structures; • **More structured and strategic collaboration** with enterprises and research entities; • Specialised training of military personnel devoted to protection from the cyber threat; and • Increased awareness about the use of cyberspace among state officials, critical infrastructure managers and the population in general.

### I/L – OCOs = Deterrence

OCO’s = deterrence + traditional deterrence theory doesn’t assume OCOs

Oolup 22 – Master’s degree from the University of Tartu (Laura Oolup; " CYBER AS A DETERRENT: UTILIZING OFFENSIVE CYBER CAPABILITIES IN NATO’S DETERRENCE POSTURE "; Modern War Institute; https://core.ac.uk/download/pdf/223009731.pdf; 1-25-2022, Accessed 6-24-2022)//ILake-AZ

In this context, classical deterrence theory in regards of utilizing offensive cyber capabilities as a deterrent, should be improved by considering the secretive nature of offensive cyber capabilities and not requiring their exposure the same way as it is expected from using conventional means as deterrent. In this context, it should be more emphasized that the capability and willingness of relaying different types of cyber effects is there. This can be done through exercises but also through previously conducted offensive cyber operations in other domains.

Another feature that the classical deterrence theories do not address - but need to in order to explain how the offensive cyber capabilities can be used as means of deterrence - is taking into account the time constraint. The latter in the sense that deploying those cyber weapons which have the potential to generate greater strategic effects by targeting the functionality of critical infrastructure for instance, tends to be a long-term process. In order to instantly retaliate the enemy with this kind of operation, the deterrer needs to be in the adversary’s systems beforehand. Notably, as it was described in the theoretical section above, developing a sophisticated cyber weapon that could inflict damage on the industrial control system for instance, involves numerous time-consuming steps. The question that needs to be considered in this regard is how to hold the enemy at risk by threatening to harm the critical infrastructure through offensive cyber means in case it should decide to attack. Subsequently, if it requires the presence-based approach, then how to communicate that to the adversary to ensure the credibility of the threat, but without increasing instability between the actors?

However, in general, the mainstream deterrence theories seem to remain applicable to utilizing offensive cyber capabilities as means of deterrence. Because despite the different means to be used, it is still necessary to reflect to the potential enemy which kind of retaliatory capabilities one has and thereby which costs the enemy can expect in case it decides to attack. Therefore, the following recommendations can be given to NATO on how it could bolster its deterrence posture through the utilization of offensive cyber capabilities as means of deterrence.

First, NATO should take a step further and not limit itself considering the offensive cyber capabilities only as measures to deter the enemy from carrying out malicious activity in cyberspace. The strategic value of offensive cyber capabilities has been presented in this paper and thereby NATO should seek for options to include offensive cyber capabilities as means of cross-domain deterrence. This should accordingly be reflected in its strategy documents. However, for effective deterrence the identified credibility issues need to be mitigated.

NATO and its member states – particularly those that have offered their capabilities for the NATO’s use – need to achieve a common terminology and understanding of the offensive cyber capabilities and offensive cyber operations. Analysing the public documents from this angle, it was identified that the degree of effects Allies considered to be generated through the offensive cyber operations did differ. These different perceptions need to be aligned to make sure the enemy perceives that the Alliance has unified position on how the offensive cyber capabilities could be deployed and what kind of cyber effect it is willing to relay.

Third recommendation would be to have a clearer message on which kind of costs the enemy could expect from the deterrer’s offensive cyber capabilities. The actions alone are not enough. Words complement the actions and enable to prevent misperceptions and thereby mitigate the potential security dilemma that may occur. As noted in the theoretical part, relaying kinetic effects has greater strategic value, especially by targeting the critical infrastructure that the military also relies on. In this case – as it was also illuminated on the existing deterrence theory – it could be necessary to have access in the enemy’s systems before the crisis should erupt. Because NATO has emphasized its defensive posture also while talking about the offensive cyber capabilities, then it is particularly important to create the right narrative to avoid increasing the instability, contributing to security dilemma, and enabling the enemy to have a misperception on this. Finding the right balance here is probably the most difficult task. Thus, having an improved version of deterrence theory that can explain and guide how to make the cyber threat credible without increasing the instability, would be extremely valuable.

However, logic effects should not be left aside. Depending on the target, this could be the way to go as well. Concerning Russia – the subject of NATO’s deterrence – should be vulnerable to logic effects that intend to affect the stability of internal politics. This is presumed based on Rivera’s work on to which kind of cyberattacks countries are vulnerable to based on their power position and social cohesion (Rivera 2015:9-11). However, this should be further examined in the future on what would be strategically the most valuable targets to hold at risk as part of the deterrent threat related to Russia.

To sum up, NATO has the potential to bolster its deterrence by considering the offensive cyber capabilities as means of deterrence. It can be partly achieved by starting with meeting the conditions classical deterrence theories have set, like having a clear and unified message about the cyber capabilities as retaliatory measures. Yet, to ensure the total effectiveness, the classical deterrence theory needs to be improved by acknowledging the secretive nature of offensive cyber capabilities and answering questions on how to hold the enemy at risk by threatening to harm its critical infrastructure through offensive cyber means and if presence-based approach is required, how to communicate that to the adversary without increasing instability between the actors.

NATO intel-sharing is key to deter increasingly aggressive Russian cyberattacks

Lewis and Warner 22 – James Andrew Lewis is the Senior Vice President and the Director of the Technology and Public Policy Program at the Center for Strategic and International Studies, Senator Mark Warner is the senior United States senator from Virginia, first elected in 2008. He is a member of the Democratic Party, vice chair of the Senate Democratic Caucus, and chair of the Senate Intelligence Committee ("Cyber in the Ukraine Invasion"; No Publication; https://www.csis.org/analysis/cyber-ukraine-invasion; 3-14-2022, Accessed 6-24-2022)//ILake-AZ

I think it has really shown in an information-driven world if we can share intelligence with the public and with our allies in a more real-time basis, it puts us back in the game in terms of information warfare. I think over the last number of years, frankly, Russia has been a much better – has been much better at using information warfare or, particularly, disinformation. We all saw the Russian involvement in 2016 in our elections. We’ve continued to see Russia use social media in a much, much more aggressive way. The fact that we were able to get this information out into the bloodstream, you know demonstrating and taking away any ability for Putin to claim that there was any Ukrainian provocation that started this war, it really has left Putin exposed as being the absolute culprit in starting this war. There’s no credible claim otherwise. So that, I think, is important.

And also, the willingness to share with our allies. Obviously, we share a lot of times with our Five Eye allies. But this one, the information sharing with the balance of NATO and in some cases even beyond NATO, it’s not by chance that we ended up, I believe, with 142 votes in the U.N. General Assembly a week ago. A lot of that was because the American intelligence we were sharing with a lot of folks. I hope this will be a precursor to a much more ongoing, active intelligence network. And, candidly, again, the power of information sharing ought to be a stronger part of our, you know, military, diplomatic, and overall statecraft.

Dr. Lewis: Thank you. I think that’s really a neat point that intel sharing is something that lets us get an advantage in the intel – in the information conflict. So useful. I’m going to ask for a crystal ball moment. I almost saved this for last. You can dodge it if you want. But some of us have been following the CHIPS Act for however long it’s been in play – is it a decade now? I don’t know. But – (laughs) – that’s not fair. But has this changed the dynamics on the Hill vis-à-vis the sense that we are now in a much more immediate conflict with Russia, and I would say with China? How has it changed the dynamic?

### I/L – AT OCO’s Bad

Little academic support that offensive cyber operations cause escalation

Lonergan and Montgomery 22 – Dr. Erica Lonergan is an assistant professor in the Army Cyber Institute at West Point. She is also a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University. Erica previously served as a senior director on the Cyberspace Solarium Commission. Retired Rear Admiral Mark Montgomery, US Navy, is the senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies. Mark previously served as the executive director of the Cyberspace Solarium Commission. ("Pressing Questions: Offensive Cyber Operations and NATO Strategy"; Modern War Institute; https://mwi.usma.edu/pressing-questions-offensive-cyber-operations-and-nato-strategy/; 1-25-2022, Accessed 6-24-2022)//ILake-AZ

Finally, there is an obvious risk that moving toward a more offensive posture in cyberspace will increase the likelihood of escalation. While these concerns should not be ignored, academic research has found little support for the argument that cyber operations cause escalation. That said, the alliance should consider how to strengthen existing confidence-building measures, particularly with Russia, to enable more effective communication and transparency about cyber operations. The expert consultations between Russia and the United States that both governments agreed to in June 2021, for example, or recent diplomatic dialogue between Russia and NATO members over the Ukraine crisis, are important to strengthen processes for crisis management and reduce the risk of instability—including that which may stem from cyber operations.

NATO has slowly begun to address the use of offensive cyber operations, and has generally limited itself to the use of these tools in traditional military campaigns. The ongoing crisis with Russia on Ukraine’s border is exposing the risk in this approach. NATO needs to figure out a way forward fast.

Research shows escalation through cyber ops is unrealistic

**Lonergan & Montgomery 22** (Mark Montgomery is the Executive Director of the Cyberspace Solarium Commission. Erica D. Lonergan is an Assistant Professor in the Army Cyber Institute. She is also a Research Scholar in the Saltzman Institute of War and Peace Studies at Columbia University.) 1/25/22, accessed 6/24/22, “Pressing Questions: Offensive Cyber Operations and NATO Strategy”, <https://mwi.usma.edu/pressing-questions-offensive-cyber-operations-and-nato-strategy/#:~:text=At%20the%202018%20Brussels%20summit,Provided%20Voluntarily%20by%20Allies%20process.> (JB)

Finally, there is an obvious risk that moving toward a more offensive posture in cyberspace will increase the likelihood of [escalation](https://academic.oup.com/ia/article/97/3/703/6205395?login=true). While these concerns should not be ignored, academic [research](https://www.jstor.org/stable/26760131?seq=1#metadata_info_tab_contents) has found [**little**](https://academic.oup.com/cybersecurity/article/5/1/tyz007/5575971)[**support**](https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf) **for the argument that cyber operations cause escalation**. That said, the alliance should consider how to strengthen existing [confidence-building measures](https://www.jstor.org/stable/26481908?seq=1#metadata_info_tab_contents), particularly with Russia, to enable more effective communication and transparency about cyber operations. The expert consultations between Russia and the United States that both governments agreed to in [June 2021](https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/), for example, or recent [diplomatic](https://www.nytimes.com/live/2022/01/10/world/russia-us-ukraine-talks) [dialogue](https://www.nato.int/cps/en/natohq/news_190924.htm) between Russia and NATO members over the Ukraine crisis, are important to strengthen processes for crisis management and reduce the risk of instability—including that which may stem from cyber operations.

NATO has slowly begun to address the use of offensive cyber operations, and has generally limited itself to the use of these tools in traditional military campaigns. The ongoing crisis with Russia on Ukraine’s border is exposing the risk in this approach. **NATO needs to figure out a way forward fast.**

### I/L – US Key

[US](https://core.ac.uk/download/pdf/223009731.pdf) info-sharing is key – it’s the forefront of NATO cyber capabilities and spurs follow-on

Oolup citing Stoltenberg 22 – Laura Oolup holds a Master’s degree from the University of Tartu, Jens Stoltenberg is the Secretary General of NATO ("CYBER AS A DETERRENT: UTILIZING OFFENSIVE CYBER CAPABILITIES IN NATO’S DETERRENCE POSTURE "; Modern War Institute; https://core.ac.uk/download/pdf/223009731.pdf; 1-25-2022, Accessed 6-24-2022)//ILake-AZ

The US has been widely acknowledged as the global cyber power which is at the forefront with the offensive cyber capabilities. Therefore, the US is extremely important asset for NATO to have credibility and capability imposing retaliatory threat in cyberspace. The US has not been clear in words either which capabilities exactly it possesses, but the actions give a taste of it. The SCADA-attack against the Iranian nuclear facility in Natanz that caused kinetic effects is a significant reflection of it (Zetter 2014). What can be noted here is that the offensive cyber capabilities have been presented through their deployment.

If we also take a look at what Stoltenberg said in regards of the sovereign cyber capabilities certain Allies have given for the use of NATO, he does not give a clear answer to how the capabilities will be used as part of NATO’s missions and operations. However, he does refer to the capability and will to use it in regards of disrupting networks, in other words attacking the availability of data.

“We have been able to disrupt the cyber networks of Daesh to reduce their ability to recruit, to fund, to communicate. And these capabilities have been used by NATO Allies against Daesh and these are the same kind of capabilities we now are creating the framework to integrate into NATO missions and operations” (Stoltenberg 2018).

#### US leadership key to norm-building in cybersecurity—otherwise risk of pushback dooms cyber norms

Sanakli 20 (Angelo Sanakli, Angelo Sanakli is a Master’s Candidate in Security Policy Studies at the Elliott School of International Affairs at The George Washington University. His focus is on cybersecurity and international law, “America Should Engage Like-Minded Partners for a Safer Cyberspace,” The International Affairs Review, April 30 2020, <https://www.iar-gwu.org/blog/2020/04/30/america-should-engage-like-minded-partners-for-a-safer-cyberspace)-> lh

The last set of norms came in 2015 during a previous GGE. It set out that nations should not carry out cyber acts that seek to intentionally damage other nations’ critical infrastructure, such as power grids, water supplies, and financial services. The GGE process came to an abrupt end in 2017 owing to considerable push back from China, Russia, and Cuba. They opposed majority positions on the right to self-defense and the application of international humanitarian law, which regulates the humanitarian aspects of armed conflict. Conflicting interests on rules on, or related to, “free internet” and “cyber sovereignty” will continue to play out in both GGE and OEWG talks. Future push-back will only continue to stifle progress on norm-building. So what does this mean for the United States?

The United States needs to engage like-minded partners. They not only share like interests but play a vital role in projecting American interest abroad. Take for example how the North Atlantic Treaty Organization (NATO) broadened its collective defense commitment to include provisions for “cyber attacks” in 2014, or how the United States and Japan similarly broadened their mutual defense commitment in 2019. Here’s what the United States and like-minded partners should do next:

Reinforce existing norms: Like-minded partners should introduce enforcement procedures for nations that don’t abide by existing norms. They should affirm that there are consequences for bad behavior in cyberspace. Some possible examples of enforcement include facilitating robust information-sharing to thwart other nations’ wrongful cyber acts and developing defensive and offensive joint cyber operations. Nations that don’t follow the rules must know that they will be held accountable.

Develop new norms: Like-minded partners should also develop new norms, especially where OEWG or GGE consensus is unlikely. Some possible examples of norm-building include the right to respond to wrongful cyber acts in self-defense and the application of international humanitarian law in armed conflicts involving cyberspace. The progress on norms must be wrapped into both OEWG and GGE talks to push consensus in the right direction.

Norm-building on cyberspace remains controversial. Some will say that working with like-minded partners undermines United Nations processes. Yet existing norms are a clear indication that these processes protect the United States’ interests and make cyberspace safer for all nations. The OEWG or GGE talks will not reach consensus anytime soon, therefore the United States should press ahead with like-minded partners all the sooner.

The United States needs to step up and lead. It needs to engage like-minded partners. It needs to reinforce existing norms and develop new ones to affirm that there are consequences for bad behavior in cyberspace. The United States can’t risk the possibility of adversaries at the forefront of norm-building. This is an opportunity for American leadership to make cyberspace safer for all nations.

### I/L – Intel Sharing Key

#### NATO intelligence sharing key to allied response

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

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

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

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

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

When should states publicly attribute cyberattacks? Effective public attribution requires a clear understanding of the attributed cyber operation and the cyber-threat actor, but also the broader geopolitical environment, allied positions and activities, and the legal context. The public attribution framework put forward by Max Smeets and Florian Egloff in March 2021[27](https://www.gmfus.org/news/natos-role-global-cyber-security#footnote27_pukyrym)

distinguishes four factors that act as enablers or constraints in public attribution. These factors are intelligence, incident severity, geopolitical context, and post-attribution actions. The combination of these four components enables consistent decision-making about whether to publicly disseminate information about an adversary’s actions, privately tell the adversary, or restrict knowledge of the intrusion to the government and potentially other partners.

Collecting and processing intelligence—information about foreign countries and their agents—provides a technical basis for attribution. How could allies improve intelligence sharing to conduct more rapid attribution and enable a response to adversary cyber activity? During the Nordic-Baltic foreign ministers meeting in Tallinn in September 2020, a 90-minute tabletop exercise was organized[28](https://www.gmfus.org/news/natos-role-global-cyber-security#footnote28_cpch8u5)

to test the ministers’ ability to respond to and attribute an escalating cyberattack. They answered multiple-choice questions on communication of and possible diplomatic countermeasures to the attack. The ministers learned through first-hand experience that a timely exchange of technical intelligence can be key in attributing any cyberattack. “The shared view [of the countries involved]—especially when it comes to complicated issues—is crucial,” said Urmas Reinsalu, Foreign Minister of Estonia.[29](https://www.gmfus.org/news/natos-role-global-cyber-security#footnote29_topliia)

Attribution is only as good as the information that allies are willing to share. NATO’s value can be in becoming the preferred platform for sharing cyber information. General Paul Nakasone, who heads US Cyber Command, told the House Armed Services subcommittee on intelligence that “in 35 years” he has never seen a better sharing of accurate, timely, and actionable intelligence than what has transpired with Ukraine.[30](https://www.gmfus.org/news/natos-role-global-cyber-security#footnote30_qki9qsu)

**Sharing information and intelligence with allies “builds coalitions” and can “shine a light on disinformation” campaigns**, like the one Russia used to lay the groundwork for their invasion of Ukraine.

As the second course of action, **NATO should** use the current crisis to accelerate the progress with setting up NATO’s own cyber command and **sharpen allied responses** to malicious cyber actions. Overall, **this would give more credibility to its cyber defense.** In February 2019, allies endorsed a set of tools to respond to cumulative cyber activities, but not much has happened to take it forward. It is now time to build upon this set and develop concrete steps at the political, military, and technical levels to model alliance behavior according to the threat landscape. This means a sharper focus on future responses to high- and low-end cyberattacks along with concrete deterrence actions and tools for individual sectors and target types. Much of this is based on the high-end cyber capabilities of select individual allies called “volunteer sovereign cyber effects,” where cyber-capable nations deliver voluntarily offensive cyber effects on a target designated by an operational-level commander. The NATO Cyber Command would be responsible for matching military needs with the willingness and capabilities of the nations potentially able to deliver such effects.[31](https://www.gmfus.org/news/natos-role-global-cyber-security#footnote31_9likw2h)

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

### **I/L – Defending Forward Key**

#### That requires defending forward

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

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

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

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

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

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

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

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

### I/L – Deterrence

#### That unlocks a joint offensive cyber capability that deters conflict and increases operational strength---it facilitates knowledge transfer, improves attack coordination, and streamlines decision-making.

University of Exeter 20. “Should NATO Adopt a Joint Offensive Cyber Capability?” September 2020. <https://socialsciences.exeter.ac.uk/media/universityofexeter/strategyandsecurityinstitute/pdfs/mstrat/James_Prideaux.pdf>. //AN

With this established, it is possible to set out this chapter’s main argument: that a joint offensive cyber capability would enhance the Alliance’s cyber-deterrent posture. There are three reasons for this. It would: improve intra-alliance knowledge transfer of cyber-intelligence gathering and cyber-sabotage techniques; help coordinate attacks and mitigate fratricide; accelerate decision-making and streamline response scenario planning.

First, NATO’s cyber-deterrence would be more credible because a joint cyber capability would facilitate knowledge transfer between member states. For deterrence to be successful, NATO has to convince aggressors that it can retaliate against the right aggressor in a manner that imposes unacceptable costs. However, state and non-state actors, like the Fancy Bear cyber-espionage group likely associated with the Russian security services, know that the disaggregation of member states’ cyber assets makes this harder to achieve.89 The primary reason for this separation of effort is that intelligence on adversaries’ cyber vulnerabilities is closely guarded by national intelligence agencies.90 This intelligence is absolutely critical for effective cyber attacks, since it is necessary to understand the targeted systems in great detail.91 The CyOC will not go far enough in fostering intelligence sharing, even though it aims to ‘integrate cyber capabilities into NATO planning and operations’.92 It is certainly a step forward, but of those states that have offered their cyber effects to NATO, France and America have clearly stated they will retain full control of their operations and capabilities.93 This lack of joint operational authority poses a significant challenge, as it appears the centre will serve to coordinate rather than oversee operations.94 It will prove very hard to achieve even this when members’ capabilities vary greatly in their maturity and development. Whereas Germany is said to have thousands of ‘information and cyber officers’, other European states have hardly any.95 Overall, NATO in its current state is not optimised for deterrence-by-punishment and the CyOC will do little to improve this.

Instead, pooling members’ cyber-intelligence and cyber-sabotage expertise would encourage intra-alliance knowledge transfer. Knowledge transfer in organisations is the process through which one unit, like a department or division, is affected by the experience of another.96 Empirical evidence suggests that interconnected organisations like franchises and chains hold comparative advantages over their autonomous counterparts, due to the ability to transfer knowledge between their constituent elements.97

This would apply to NATO in two ways. First, organisational integration of cyber-intelligence would facilitate knowledge transfer, as demonstrated by the preparations behind Stuxnet.98 To design such a complex computer worm, the US National Security Agency (NSA) collaborated with Israel’s counterpart, Unit 8200, largely because it had deep intelligence about operations at Iran’s Natanz facility.99 This was vital for the attack’s success, because the individual control systems they targeted had unique configurations, making them harder to penetrate.100

Second, merging cyber-sabotage capabilities would similarly aid knowledge transfer. There are two types of knowledge required for cyber-sabotage operations. One type is explicit and can be transferred in a systematic manner, such as knowledge of how a SCADA system works or how to write code in a certain programming language.101 The other, more significant type is tacit knowledge, which is difficult to transfer to another person by verbalising or writing it down.102 This could include a hacker’s accumulated experience or knowledge of a cyber command’s implicit operational processes.103 Tacit knowledge can be shared, but this is done by performance and learning by example.104 A joint offensive cyber capability would provide an excellent opportunity for this to happen.105 Both forms of knowledge transfer would be especially useful for ‘upskilling’ those NATO members that lack the advanced technical expertise in America, Britain, France and Germany. In practice, this would make acquiring cyberattack tools and training personnel easier and cheaper.106 The importance of training technical personnel should not be underestimated, because all members are short of them but most lack the resources to attract them.107 Pooling capabilities is one way of alleviating this pressure. In turn, the cumulative benefits of knowledge transfer would likely make it easier to launch retaliatory attacks against the right aggressor and impose unacceptable costs more successfully. Overall, this would improve the credibility of a deterrence-by- punishment posture.

Furthermore, a joint capability would improve NATO’s offensive cyber C2, improving attack coordination and mitigating fratricide. This is because NATO’s ‘volunteer’ system and its CyOC mark a striking departure from the way it usually handles C2of members’ assets.108 The NATO Force Structure dictates that conventional forces like ships and tanks come under the full operational control of an assigned NATO commander.109 However, according to a retired USAF Colonel leading the implementation of NATO’s 2017 cyber policy, the C2 problems inherent in the volunteer system make it ‘far from ideal’.110 This is because NATO commanders do not know the details of capabilities available to them, such as their legal consequences, impeding the decision-making process.111 Commanders also want to know how using cyberweapons might conflict with other operations; without this they are left ‘flying blind’.112 Failing to coordinate operations can have far-reaching consequences. For instance, intelligence agencies’ reconnaissance of target networks needs to be coordinated with cyber-sabotage operations, so they do not interfere with each other.113 Disaggregated C2 can even result in fratricide on other allies’ networks, because the distinction between internal and external security threats is much harder to ascertain in cyberspace than in the other four domains.114 The CyOC is a step towards resolving this, but until a NATO commander has control over members’ capabilities, these problems will not be fully resolved.

Additionally, a unified offensive cyber C2 structure would aid scenario planning and speed up decision-making. This is important, because NATO needs to streamline its current decision-making process in the cyber domain.115 A single command would help members agree on appropriate forms of retaliation in cyberspace in different scenarios, bolstering the credibility of deterrence-by-punishment even further. Without a clear command structure, it is very difficult for the 30 NATO allies – who have different threat perceptions and suffer from a lack of cohesion – to agree on effective response scenarios in contingency planning.116 As a case in point, Estonia is willing to strike back when attacked online, given its memory of the 2007 attack and its proximity to Russia.117 However, Estonian officials do not know whether other allies will support them, validating some scholars’ arguments that NATO needs to find common ground in cyber contingency planning.118 The secrecy that shrouds allies’ capabilities and the uncertainty surrounding cyber scenario planning might explain why offensive cyber effects do not feature in NATO’s mission planning process.119 This is not to say that NATO needs to publicly agree on a ‘red line’ in cyberspace that could trigger an Article 5 response. If anything, NATO’s current strategic ambiguity is key for deterring attacks that fall just below a defined threshold.120 However, unifying cyber C2 would help them carry out scenario planning behind closed doors, improving the Alliance’s readiness. Speeding up the decision-making process is crucial given how long it can take to attribute and then launch a retaliatory attack.121 Overall, streamlined scenario planning and decision- making, augmented by improved coordination of cyberattacks, would strengthen the credibility of deterrence-by-punishment. Although aggressors like Fancy Bear would not know when a certain threshold has been crossed, it would tilt their risk-benefit calculus knowing an attack could trigger a faster, well-coordinated retaliatory attack.

### !! – Russian Cyberattacks

Unprecedented Russian cyberattacks are rapidly escalating now and cascade globally – nuclear war

Umbach 22 – Professor, researcher, consultant, European government advisor and prolific author, with expertise in energy security and cybersecurity (Frank Umbach; "Russia’s cyber fog in the Ukraine war"; https://www.gisreportsonline.com/r/russia-cyber/; 5-10-2022, Accessed 6-24-2022)//ILake-AZ

Russia’s state-supported cyberattacks increased both before and during its invasion of Ukraine. The moves are part of Moscow’s broader attempt to disrupt services and create intimidation and confusion. Up until now, however, the Kremlin has not launched a devastating cyberwar against NATO countries, despite numerous warnings in recent months.

Western experts are still uncertain whether fears of American cyber retaliation and the existence of a “Mutual Assured Cyber Destruction” (“cyber-MAD”) are the reason why such attacks have not materialized. But any further Western sanctions (such as the European Union’s declared oil embargo on Russia) will increase the risk of devastating Russian cyberattacks.

Shared targets

On May 10, 2022, the European Union, United Kingdom and the United States officially attributed a February 24 cyberattack to Russia. One hour before the invasion of Ukraine, hackers had targeted the Viasat-operated KA-SAT satellite network to disrupt command and control of the Ukrainian military and government communications.

The disrupted internet access caused collateral damage to commercial and residential internet services. Thousands of modems across Central Europe lost their satellite connection. In Germany, 5,800 Enercon wind turbines could no longer be remotely monitored by their operators.

In 2015, Russia conducted its first deliberate cyberattack on Ukraine’s energy infrastructure and grid system.

Since the invasion, Russian attacks have become more frequent and destructive. They are coordinated with the Kremlin’s military actions as part of its hybrid warfare against both Ukraine and the West. Its state-supported hacker groups began preparing for the conflict as early as March 2021, according to new reports on Russia’s relentless cyberattacks as part of its hybrid warfare against Ukraine. These cyber operations require careful planning, targeting and development, which requires months if not years.

In recent years, both the U.S. and EU have intensified their collaboration with Ukraine on cybersecurity. This is because Ukraine has become a testing ground for Russia’s advanced cyberattacks on critical infrastructure, and the West can learn much from Russian cyber strikes against Ukraine.

[[FIGURE OMITTED]]

In 2015, Russia conducted its first deliberate cyberattack on Ukraine’s energy infrastructure and grid system. In 2017, the Kremlin-backed NotPetya virus, designed to disrupt financial, energy and government sectors in Ukraine, spread internationally and cost companies around the world over $10 billion in damages.

For the EU, strengthening the cybersecurity of Ukraine’s critical infrastructure has become increasingly important since the Ukrainian electricity grid is being integrated into the EU’s common electricity market and network (ENTSO-E).

The rising vulnerabilities of Western societies and economies have been highlighted in 2020 after the hack of a leading U.S. security tech company and its software (SolarWinds). It gave the Russian hacker group “Cozy Bear” (also called “Nobelium” or APT-29) access to thousands of companies’ data, as well as critical infrastructure in various countries. The targets of this hacker group are believed to reflect the Kremlin’s geopolitical interests and strategic priorities. Cozy Bear has increased its attacks against Ukraine from a mere six in 2021 to more than 1,200 this year, with particular focus on the Ukrainian government and its state agencies.

There are also lessons to be learned from the ransomware cyberattack on the 8,000-kilometer U.S. Colonial oil pipeline. In May 2021, hackers infiltrated the company’s information technology infrastructure and were able to disable the pipeline’s operation. The hack affected the oil supply for both private consumers and U.S. Armed Forces, leading to panic buying. The attackers stole nearly 100 gigabits of data and requested a ransom of 75 Bitcoin ($4.4 million at the time) to return access to the company’s billing system. The company eventually paid the ransom to the cyber hacker group DarkSide, despite the government’s efforts to prevent this. In response, the Biden administration passed the Strengthening American Cybersecurity Act (SACA) last March. It requires federal agencies as well as owners and operators of critical infrastructure to report cyberattacks within 72 hours and ransomware payments within 24 hours. But how to better mitigate threats and enhance resilience collectively across industries and sectors is not addressed in the SACA.

Mutual escalation

Since the war in Ukraine began, Russia’s state-backed cyberattacks against Western critical infrastructure have increased – by as much as 72 percent in the U.K. Alongside ever more Western sanctions and the increasing supply of heavy weaponry, NATO countries fear that Russia could escalate its nascent cyberwar with sophisticated strikes against critical infrastructure. NATO governments and the European Central Bank have repeatedly warned that the West should be prepared for this eventuality.

The Five Eyes intelligence-sharing network among the U.S., the UK, Canada, Australia and New Zealand stated in April that Russia was planning massive cyberattacks against Western countries supporting Ukraine. A dozen hacking groups were designated as threats, since they are part of, or close to, Russian intelligence and military institutions. They have the ability to anonymously compromise IT networks, steal large amounts of data, deploy destructive malware and bring down networks.

Last October, Microsoft warned in its 2021 Digital Defense Report that Russia was the state that posed the greatest cyber threat. Russian hackers are considered much more prolific than those from China, Iran and North Korea. In 2020, 58 percent of all state-backed cyberattacks identified by Microsoft came from Russia. Cozy Bear accounted for more than 92 percent of all detected Russian activity. Microsoft also warned that its attacks targeting enterprise VPN software have become up to 32 percent more successful. Attacks are mainly carried out as espionage and intelligence campaigns against government agencies and think tanks. The top target countries are the U.S., Ukraine, and the UK.

During its 2014 annexation of Crimea, Russia learned that it is much more difficult to conduct a surgical cyber strike than an indiscriminate one.

In March, the White House issued a strongly worded warning that Russia is planning major cyberattacks against the U.S. in retaliation for its harsh economic sanctions. In April, a U.S. federal advisory warned that hackers with ties to foreign governments are targeting specific industrial processes and their information and control systems, including the supervisory control and data acquisition devices to disrupt, sabotage and physically destruct them.

Last June, U.S. President Joe Biden, embarrassed by the SolarWinds hack and facing political pressure to retaliate against Russia, issued a warning to President Vladimir Putin. At the first bilateral cybersecurity summit since the Kremlin’s annexation of Crimea in 2014, Mr. Biden stated that 16 areas of critical infrastructure, including energy, health and water, should be “off-limits to attack” by cyberattacks or other means.

He also urged the Kremlin to take action against criminals conducting ransomware attacks. But bilateral cybersecurity cooperation has not made any significant progress since last summer. Illicit ransomware activities by criminal groups appear to have continued unabated. The trend goes hand in hand with the booming cryptocurrency industry, which provides anonymous digital assets that can be used for money laundering.

‘Cyber-MAD’ and cyber deterrence

Alongside diplomatic efforts to de-escalate cyber tensions between the West and Russia during the last few years, Western allies have warned Russia of “massive consequences” for its largest banks and trading companies in the case of escalating cyberwarfare against NATO and EU countries.

Despite Russia’s undeniable offensive cyber capabilities, the Kremlin has not initiated any larger devastating cyberwar against the West since its military invasion began – despite unprecedented sanctions.

One explanation could be that both the U.S. and NATO have stated that a highly damaging cyberattack on any member of the alliance could trigger Article 5 of the treaty, which guarantees mutual defense. This could indicate that some form of “cyber MAD” still functions between the U.S. and Russia. Many cyber experts have warned that the West cannot afford to bet on that as a deterrent. However, defining a more assertive cyber retaliation strategy must also consider the possibility of an escalatory spiral that could even result in Russia resorting to use nuclear weapons, even perhaps preemptively.

During its 2014 annexation of Crimea, Russia learned that it is much more difficult to conduct a surgical cyber strike than an indiscriminate one. If the Kremlin decides to directly attack major Western infrastructure, it will face retaliation. But the situation could also escalate because Russia might not always be able to control its own cyber operations on selected targets, potentially leading to unwanted escalation and collateral damages far beyond what was initially intended.

[[FIGURE OMITTED]]

Since the beginning of the war, Russia itself has become the target of numerous international pro-Ukraine cyber groups and hackers, shattering illusions of Moscow’s cyber superiority. Cyberattacks on the Russian government and military institutions have increased significantly. The active Anonymous group has stolen hundreds of millions of documents from governmental and industrial websites, including the Ministry of Defense. Others have blocked or slowed freight trains carrying Russian military equipment or tampered with the automatic ticket system for passengers.

Ukraine itself has built an “army” of IT volunteers (like Network Battalion 65) to protect the country against Russian hackers, but also to launch counter operations against Russian cyber threats. The Ukrainian cybersecurity company Hacken claims that 10,000 hackers from 150 countries have volunteered to disrupt Russian media sites and promote pro-Ukrainian messages across Russian social media.

But these international and private Ukrainian hacker groups have acted without any kind of coordination, in contrast to Russia’s state-supported cyber groups controlled by the foreign intelligence agency (SVR) or the military intelligence agency (GRU). Hence, the impact of these international cyberattacks against Russia has yet not been significant enough to shift the Kremlin’s cost-benefit calculation of its invasion of Ukraine.

Scenarios

Russia’s red lines and escalation strategy could further change in the weeks and months ahead. How the military, political and economic aspects evolve, and war aims change will influence how the Kremlin decides to use its cyber capabilities in the conflict.

Beyond the Russian-Ukrainian war, if adversarial threats increase, so too will the vulnerabilities, as the world increasingly relies on digital technology. In 2021, a record-breaking number of cyberattacks took place – a 50 percent increase from the previous year according to the cybersecurity firm Check Point Research. New forecasts suggest that 2022 could be even worse. Cyber threats to civilian and military critical infrastructure are likely to multiply and grow even more consequential as the digital and physical worlds become increasingly intertwined. While awareness of the need for cyber resilience has grown in the West, it is too little to prevent disastrous cyberattacks on critical infrastructure

Russian cyber attacks incoming

Corbishley 22 – Journalist covering global financial, economic, and political developments. (Nick Corbishley; "The Russia-NATO Cyber War Is Escalating Fast"; naked capitalism; https://www.nakedcapitalism.com/2022/04/are-we-in-the-first-ever-global-cyber-war.html; 6-24-2022, Accessed 6-24-2022)//ILake-AZ

Fears are rising that the boundaries of the cyber war between Russia and NATO could soon spread beyond Europe.

Eight cybersecurity authorities from the so-called “Five Eye” nations (United States, United Kingdom, Australia, Canada and New Zealand) released a joint statement on Thursday warning that more malicious cyber activity is on the way as Russia’s invasion of Ukraine continues to undermine geopolitical stability.

Before we look at the statement in any depth, an important five-pronged caveat is needed:

Both the US and the UK are among the primary antagonists in NATO’s ongoing war with Russia;

They both have significant offensive cyber war capabilities of their own;

US intelligence agencies, at Obama’s behest, have drawn up a list of potential overseas targets for cyber attacks;

Both countries have surreptitiously conducted vast surveillance programs, targeting not only their own populations but also citizens and government leaders of other countries;

The world right now is in the grip of the biggest information war of this century.

As such, any information coming out of the Five Eyes’ intelligence services should be treated with a healthy dose of skepticism. That having been said, here are the first three paragraphs of the missive:

The cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom are releasing this joint Cybersecurity Advisory. The intent of this joint CSA is to warn organizations that Russia’s invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and U.S. allies and partners.

Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks (see the March 21, 2022, Statement by U.S. President Biden for more information). Recent Russian state-sponsored cyber operations have included distributed denial-of-service (DDoS) attacks, and older operations have included deployment of destructive malware against Ukrainian government and critical infrastructure organizations.

Additionally, some cybercrime groups have recently publicly pledged support for the Russian government. These Russian-aligned cybercrime groups have threatened to conduct cyber operations in retaliation for perceived cyber offensives against the Russian government or the Russian people.

The document also emphasizes the frontline role likely to be played by Russian state actors, including the Russian Federal Security Service (FSB), the Russian Foreign Intelligence Service (SVR), Russian General Staff Main Intelligence Directorate (GRU), GRU’s Main Center for Special Technologies (GTsST) and the Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM) of the Russian Ministry of Defense. Clearly, Russia has the capability to launch a barrage of cyber attacks against the west; the question is: does it want to?

The authors of the document urge critical infrastructure organizations to take immediate steps to protect against cyberattacks. Those steps, they say, should include patching known exploited vulnerabilities, updating software, enforcing multi-factor authentication, securing and monitoring remote desktop protocol (RDP) and other “potentially risky” services, and providing end-user security awareness and training. As The Register, a British technology news website, notes, if any of these recommendations come as a surprise to critical infrastructure operators, “we’re screwed”.

The warning from the “Five Eye” nations comes just days after NATO began (as Bloomberg puts it) “the largest and most complex ‘live-fire’ cyber defense exercises” ever conducted. More than 2,000 people from 32 nations were expected to participate in the war game, which began on Tuesday in Tallinn, Estonia. They include representatives of five to 10 large global financial institutions, including Santander and Mastercard.

This is all happening as fears rise that the boundaries of the cyber war between Russia and NATO could soon spread beyond Europe, where attacks have been registered not only in Ukraine and Russia but also Poland and Finland. On March 21, President Joe Biden warned American businesses to prepare themselves for cyberattacks. Russia is likely to deploy cyber attacks as a form of retaliation against US sanctions, Biden said, adding that Russia has “a very sophisticated cyber capability,” which Putin “hasn’t used… yet” but which forms “part of his playbook.”

Cyber War Reaches Latin America?

Over the past week, two Latin American countries, Costa Rica and Puerto Rico, have suffered major cyber attacks targeting key national infrastructure. In Costa Rica a wave of attacks on Wednesday temporarily disabled websites belonging to the Ministry of Finance, the Ministry of Science, Innovation, Technology and Telecommunication, the Costa Rica Social Security Fund, the National Meteorological Institute (IMN) and the Costa Rican Radiographic Institute (Racsa).

Following the attack the Ministry of Science’s Director of Digital Governance, Jorge Mora, noted that the digitization of governmental activities creates risks as well as benefits. As for who was responsible, Mora said a US$10 million ransom demand had been posted on the dark web by the Conti Group, a pro-Russian ransomware gang that has threatened to deploy retaliatory measures if cyberattacks are launched against Russia. The Costa Rican government has ruled out paying a ransom, which prompted Conti Group to issue one last ultimatum: pay up or all the data gets released.

Costa Rica is a curious choice of target given the country, like Mexico, follows a policy of neutrality regarding foreign wars. In fact, Costa Rica has not had an army for 73 years. That said, the Costa Rican government is one of a small number of Latin American countries to have agreed to apply US and EU sanctions against Russia within its financial system. It has also suspended broadcasts of Russian state-backed media outlet RT.

Puerto Rico, being a so-called unincorporated territory of the United States, is a more obvious choice of target. In the past few days the country’s electronic toll collection system was brought down by a cyber attack. Local media reported Tuesday (April 19) that the attacks had begun over the weekend and had affected a mobile application, the collection systems at toll plazas, and a website. The website was up and running again by Tuesday but users were still reporting service irregularities as of this writing.

Puerto Rico’s Interior Secretary Noelia García said the hackers have demanded a ransom to restore the system, which the government says it will not do. García also insisted that users’ encrypted data such as credit card details are safe. According to Ngai Oliveras, the Puerto Rican government’s chief of security, the FBI is investigating the attack, which it is believed could be linked to the war in Ukraine.

This is not the first major cyber attack to target key public infrastructure in Puerto Rico in recent months. In January, the website of Puerto Rico’s senate as well as its internet provider and telephone systems were temporarily taken out. In October 2021, the capital’s electricity provider fell victim to a DDoS attack that resulted in a power outage affecting more than a million people. In a DDoS attack hackers inundate a website with so many bots connecting to it all at once, they render it inaccessible. Servers are not breached, data is not stolen but it can still cause lots of disruption.

The Digital Side of Russia-NATO War

Both sides of the NATO-Russia conflict took the battle to the cyber sphere from day one. In the case of Russia, it has been attacking Ukrainian targets since mid-January, weeks before the war even began. At the very onset of its invasion of Ukraine, “U.S. intelligence and military cyber warriors were advocating the use of American cyberweapons on a scale never before contemplated.” That was according to a February 24 report out of NBC titled “Biden Has Been Presented with Options for Massive Cyberattacks Against Russia.”

In an interview with MSNBC two days earlier, Hilary Clinton praised hacker group Anonymous’ for launching coordinated cyber attacks on Russian targets.

“There were reports overnight that Anonymous, a group of hackers, took down Russian TV. I think that people who love freedom, who understand that out way of life depends upon supporting those who believe in freedom as well, could be engaged in cyber support for those in the streets of Russia. We did some of that during the Arab Spring when I was secretary of state. I think we could also be attacking a lot of the government institutions, and you know the Oligarchs and their way of life through cyber attacks.”

The hacktivist group DDoSecrets, which specializes in hacking and then publishing compromising data, has also been busy since the war began. According to Micah Lee, an operational security analyst at The Intercept, the group has so far amassed seven Russian datasets from March and a further 20 from April. Among its targets are Roskomnadzor, an agency that monitors and censors mass media; Transneft, the world’s largest oil pipeline company; Rosatom, the state nuclear energy agency; the Russian Orthodox Church’s charitable wing and the Russian Central Bank.

On the other side of the conflict, cyber attacks have played a constant, if somewhat muted, role in Russia’s invasion. The targets in Ukraine have included government websites; the mobile apps and ATMs of the country’s largest banks; and the websites of non-profit organizations, tech companies, the Ukrainian military and Security Service (SBU).

“We are now witnessing the first real cyberwar,” Natalia Tkachuk, the head of Ukraine’s Information Security and Cybersecurity Service, told The Record, a cyber security news publication belonging to Recorded Future, a Massachusetts-based cybersecurity firm:

[M]any cyber attacks on government institutions and critical infrastructure are coordinated and planned by the Russians in order to cause maximum damage to Ukraine. Most of the attacks are now aimed at government agencies, energy, telecommunications and banking sectors. In most cases, the main purpose of the attacks is to destroy information using various data wiper malware.

We can’t say that there is necessarily an increase in the number of the attacks, rather we can note the increased coordination of efforts in the preparation of attacks on a particular sector. Such targeted and dangerous attacks come in waves, amid the static noise caused by a large number of overall cyber incidents and small attacks.

Fake News and Bank Runs

Concerns are also rising about potential attacks on financial institutions, particularly in Europe. On April 1, the European Banking Authority issued a warning about the risk of fake news triggering a run on European banks. Per Reuters:

“As market sentiment remains highly volatile and driven by news flow, banks’ liquidity levels can become vulnerable due to spread of inaccurate information,” the European Banking Authority said in its latest “risk dashboard”, which focused on exposures to Russia and Ukraine.

“Such campaigns that spread inaccurate information may result in deposit outflows from targeted banks,” EBA said.

EBA said exposures of banks in the bloc to Russia are too low to threaten financial stability, but economic fallout from the war in Ukraine and cyber attacks could hit the profitability of lenders.

EU banks had exposures totalling 76 billion euros ($84 billion) to Russia and 11 billion euros to Ukraine in the fourth quarter of 2021, mainly among Austrian, French and Italian lenders.

“Based on the EBA’s initial assessment, direct exposures to Russia, Belarus and Ukraine are limited, but second-round effects may be more material from a financial stability perspective,” it said.

Second-round effects include direct economic fallout of the war such as the fiscal impact, the impact of sanctions, elevated risks from cyber attacks, and the longer-term impact on supply chains in the global economy, EBA said.

The EBA’s warning bears a striking resemblance to a scenario featured in a 10-country simulation of a major cyberattack organized by the Israeli government in December 2021. As Reuters reported at the time, the simulated cyber attack, dubbed “Collective Strength”, took place over 10 days, “with sensitive data emerging on the Dark Web along with fake news reports that ultimately caused chaos in global markets and a run on banks.”

Participants in the Collective Strength simulation included treasury officials from Israel, the US, the UK, Austria, Switzerland, Germany, Italy, the Netherlands, the United Arab Emirates and Thailand, as well as representatives of the IMF, the World Bank and the Bank of International Settlements, the central bank of central banks. The participants discussed a range of policies for responding to the simulated crisis, including a coordinated bank holiday, debt repayment grace periods, SWAP/REPO agreements and coordinated delinking from major currencies.

The simulation took place after a string of cyber attacks last year caused serious disruption to banks and other financial institutions in Pakistan, Ecuador, New Zealand and Venezuela. Interestingly, Venezuela’s government laid the blame for the IT outage suffered by Banco de Venezuela, the country’s largest bank, on the US government, which Venezuela’s vice president Delcy Rodríguez accused of launching an “intense and aggressive” cyber attack against the bank’s IT system.

Cyber Attacks Were on the Rise Long Before Russia’s Invasion of Ukraine

Cyber attacks have been a growing problem for a number of years as more and more aspects of human communication, work and business operations have migrated online, particularly following the pandemic-induced lockdowns of 2020. Ransomware-related data breaches have doubled in the US for the past two years, according to the Identity Theft Resource Center’s 16th Annual Data Breach Report. Supply chain attacks, like DarkSide’s ransomware attack on Colonial Pipeline, are also on the rise.

There are many reasons for this. One is that large companies that fall victim to ransom attacks tend to pay up. And the ransoms tend to be big. Colonial Pipeline paid a $4.4 million ransom payment to regain access to its files.

The rising threat is also being driven by the increasing technological sophistication and capability of hackers. At the same time, banks and companies’ IT systems have grown more vulnerable due to the explosion in use of electronic financial services during the pandemic as well as the rise in remote working by employees, as reader Vlade commented on a previous article:

The problem with the home front is that most people are treating home IT as “just put it there”, and not thinking about security until it’s way too late. Using open wifi, not changing default passwords or admin users etc. etc. – but TBH, I have seen the same behaviour within large corpos too.

Still by far the easiest hacking attack is via a mole (i.e. human element), and that’s very hard to prevent. And, as they are right now, since the companies are looking at their employees as interchangeable cogs in a machine, recruiting moles is likely getting easier and easier.

This may well have been the case with the recent cyber attack against Colonial pipeline, which took down the largest fuel pipeline in the country, leading to fuel shortages along the East Coast, and was pulled off with a single compromised password.

US Infrastructure At Risk?

As Russia gets bogged down in its war with Ukraine (and, of course, NATO & friends) and its sanctions-ravaged economy spirals deeper and deeper into depression, an increasingly desperate Vladimir Putin may resort to digital warfare against US targets. That is the scenario being depicted by some mainstream media outlets. A recent CBS News report, citing the same US intelligence officials that helped produce the Five Eyes missive, warns that cyber attacks against US infrastructure are growing increasingly likely.

“We have to assume that there’s going to be a breach,” said Jen Easterly, US Director of the Cybersecurity and Infrastructure Security Agency (CISA), a US federal agency that operates under Department of Homeland Security oversight. “There’s going to be an incident.”

Caveat #2: US intelligence agencies are not exactly the most reliable sources of information. Intelligence officials already told a big porky when they recently warned that Russia might be preparing to use chemical agents in Ukraine. As it turns out, they had no evidence Russia had brought any chemical weapons near Ukraine; they were apparently just trying to deter Russia from using the banned munitions. This is part and parcel of Washington/NATO’s disinformation war against Russia, as even NBC News recently admitted:

It’s one of a string of examples of the Biden administration’s breaking with recent precedent by deploying declassified intelligence as part of an information war against Russia. The administration has done so even when the intelligence wasn’t rock solid, officials said, to keep Russian President Vladimir Putin off balance.

In other words, they lied, just as they lied about Iraq’s weapons of mass destruction. As Caitlin Johnstone notes in an article for Consortium News, they may contend that they lied for a noble reason but they still lied: “They knowingly circulated information they had no reason to believe was true, and that lie was amplified by all the most influential media outlets in the western world.”

Now, we are being told by the intelligence agencies of not only the US but also its fellow Five Eye partners that a Russian cyber attack against critical infrastructure is all but inevitable. But as I noted at the beginning of this article, they are not exactly trusted sources.

### !! – China

OCOs are key to address incoming Chinese threats – NATO key

Odgaard 22 – (Liselotte Odgaard; "NATO’s China Role: Defending Cyber and Outer Space"; Taylor & Francis; https://www.tandfonline.com/doi/full/10.1080/0163660X.2022.2059145; 2-24-2022, Accessed 6-24-2022)//ILake-AZ

NATO’s Role in the Global Commons

NATO can only be as effective as its member states allow it to be. NATO reflects the state of transatlantic relations: are US and European security outlooks sufficiently compatible such that the alliance is able to address threats from China collectively? This question is reflected in how well they manage to define common challenges and establish mechanisms that allow them to address these challenges together. NATO was a natural center of security focus for Washington when Europe was the main arena for US-Soviet deterrence. Today, the Indo-Pacific competes for US attention and resources as competition with China has moved to the center stage of US security and defense priorities.

The strategic shift in US priorities does not mean that Europe cannot continue to remain a significant influence on global security dynamics. The EU has demonstrated its continued relevance in the security realm, not merely by relying on its role as a major trade bloc, but also by reforming the interplay between member states and EU institutions to avoid being paralyzed by consensus requirements, which apply in most areas outside the trade sector. This is done by providing platforms for member states to start initiatives. If successful in attracting support within the union, the initiatives are consolidated by supportive mechanisms and programs.43

NATO is not the EU and hence should not duplicate its methods. The EU is driven by the urge to secure the continued influence of its member states on major global issues. NATO’s raison d’être is to facilitate transatlantic cooperation in the military sector to counter common threats and challenges. Coordination is complex at a time when US and European security outlooks are drifting apart in terms of threat perceptions and priorities. At the same time, fears of entrapment stifle NATO’s efforts to update its relevance, principally because key members such as France and Germany are not interested in NATO taking on China as a threat.

Nevertheless, NATO’s agreement to define China as a challenge promises opportunities for positioning the alliance in a key role in transatlantic relations. Because cyber and space encompass threats from other adversaries such as Russia and Iran, these domains are a good place to start taking on China as they do not require that China be singled out as a threat. By taking on the responsibility for coordinating US and European definitions of cyber and outer space threats in the military sector, integrating these domains in all organizational and operational NATO structures, devising mechanisms for the member states to address cyber and outer space threats, and by facilitating intelligence exchange and management of the vulnerabilities produced by civil-military interaction and overlapping interfaces between the cyber and space sectors, NATO can demonstrate its continued relevance for transatlantic security in an era where threats are increasingly global and transcend geographical boundaries. There’s no time like the present.

**NATO key to tackle china/russia**

Odgaard 22 – (Liselotte Odgaard; "NATO’s China Role: Defending Cyber and Outer Space"; Taylor & Francis; https://www.tandfonline.com/doi/full/10.1080/0163660X.2022.2059145; 2-24-2022, Accessed 6-24-2022)//ILake-AZ

NATO’s vague recognition in 2021 that China constitutes a challenge to the transatlantic alliance reflects an institution that has failed to take on the security threats emanating from Beijing. Russia’s invasion of Ukraine on February 24, 2022 highlights the reasons why this omission is problematic. The war in Ukraine has reignited transatlantic unity of purpose in addressing threats from Moscow toward European security. The existential shock that Europe is facing now that a Russian regime has shown itself willing to go to war against European countries carries with it the risk that China will be forgotten when NATO discusses its future priorities. During the war, China is walking a tightrope between maintaining its commitment to sovereignty and territorial integrity and keeping up cooperation with Russia. The future strength of the Chinese-Russian partnership is likely to be determined by the continued usefulness of Moscow in China’s efforts to carve out more space for a Sinocentric international order based on authoritarian regimes. Meanwhile, China will continue to engender threats to the US and Europe in all domains and across geographical regions.

With the summit statement of the North Atlantic Council released June 14, 2021, NATO extended a commitment to “engage China with a view to defending the security interests of the Alliance,” since “China’s stated ambitions and assertive behavior present systemic challenges to the rules-based international order and to areas relevant to Alliance security.”1 China’s coercive policies, nuclear arsenal, military modernization, military cooperation with Russia, lack of transparency, and use of disinformation are listed as main areas of concern for the alliance. NATO takes the China challenge seriously but has yet to devise a strategy to address it.

NATO takes the China challenge seriously but has yet to devise a strategy to address it

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

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

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

On February 11, 2022, during the runup to the Russian-Ukrainian war, the Biden administration published its Indo-Pacific strategy as US Secretary of State Anthony Blinken was in the midst of a Pacific trip to Australia, Fiji, and Hawaii.7 This US prioritization signaled that despite Moscow’s war in Europe, Washington remains committed to strengthening its presence in the Indo-Pacific and competing with China. If the US drops the ball on the Indo-Pacific, Washington is concerned that China might use force against Taiwan.8 Consequently, the key question for the US is how many resources can be tied up in Europe without losing sight of the long-term goal: deterrence of China. As US strategic competition with China increases while NATO is sitting on the fence, failure to develop a transatlantic defense policy that addresses China will leave Europe vulnerable to China’s ability to exploit the weak links in European defense arrangements, which are newly fragmented by the Russian invasion of Ukraine.9

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

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

NATO’s involvement is essential to establish an effective response to China

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

NATO intel-sharing and offensive cyber unification deters Chinese and Russian cyber threats

Machiels 19 – Public Policy & Security Diplomacy Analyst and International Humanitarian Law Researcher (Maaike Machiels; "Active Cyber Defence and NATO"; Atlantic Forum; https://www.atlantic-forum.com/atlantica/active-cyber-defence-and-nato-natos-innovative-offensive-strategy-towards-russia-and-china; 11-01-2019, Accessed 6-24-2022)//ILake-AZ

Apart from the diplomatic approach with China, NATO should ensure its Allies maintain confident relations with one another. As mentioned above, resources differ between member states, leaving the majority dependent on a third state’s cyber intelligence. To ensure its own military power and resilience against China, NATO should facilitate the sharing of sensitive information amongst its Allies.

While fostering a unified offensive cyber defence strategy, NATO should refrain from its Allies’ national prerogatives, namely the decision of whether or not their reaction to a certain cyber attack is legitimate and thus authorized by the UN Charter. Admittedly, international law is not sufficiently developed to regulate counter offenses in detail, but most fundamental texts—whether designed for warfare or peacetime—should be respected.

Not only should NATO take responsibility, but so also should its Allies, who are encouraged to re-evaluate their national digital dependency, especially in relation to 5G networks. States should investigate their continuity mechanisms and draft scenarios with alternative solutions to sole dependence on Huawei.[xxxvii] On an even more pressing note, and before any policy or general principles can be drafted, member states should urgently develop a common risk assessment of Huawei’s mobile networks on global trade and military security. A successful resilience and offense strategy should be built on a common strategy fuelled by a certain consensus on values, measurements, and beliefs.

In conclusion, a considerable number of top-down policies remain to be drafted: strategies demand to be amended on NATO’s side, and Allies’ stances will have to be reconciled in order to tackle future cyber threats from Russia and China. Recent security meetings and conferences, namely the Munich Security Conference, demonstrate an awareness and incitement to address today’s needs in cyber space. NATO and its Allies wish to centre themselves around the democratic defence of human dignity while striving for global peace and upholding respect for the rule of law, thereby reaching consensus on the destination of NATO’s role in cyber space. The journey ahead—or the years leading to 2023—will prove whether or not this destination is feasible.

### !! - Nuke War

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

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

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

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

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

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

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

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

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

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

### !! – Hybrid War

#### Hybrid War happening now and will escalate

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

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

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

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

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

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

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

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

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

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

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

### !! - Meltdown

#### Threat of meltdown from cyberattacks is high and increasing

Dr. Page Stoutland 18, Consultant of Scientific and Technical Affairs to the Nuclear Threat Initiative, B.S. from St. Olaf College, Ph.D in Chemistry from University of California Berkeley, “Cyberattacks on Nuclear Power Plants”, The Nuclear Threat Initiative, 3/19/2018, https://www.nti.org/atomic-pulse/cyberattacks-nuclear-power-plants-how-worried-should-we-be/ Accessed 24 June 22

The New York Times reported last week on a U.S. government report accusing Russia of conducting a series of cyberattacks aimed at U.S. and European nuclear power plants and water and electric systems from 2015 through 2017. In addition to attacks on water and electric plants, publicly available evidence suggests that Russia infiltrated the business systems of the Burlington, Kan., Wolf Creek nuclear plant but not the plant’s control systems. It was not clear whether the goal of the attack was to conduct reconnaissance or, more seriously, some type of sabotage.

Needless to say, any type of attack on a nuclear plant is very concerning. An attack that allows hackers to manipulate the systems that control a nuclear reactor, while very difficult, could have very serious consequences, including potentially nuclear reactor core damage and off-site release of radiation.

This is not the first time that nuclear facilities have been attacked. The most well-known example is the Stuxnet attack on Iran’s uranium enrichment facility, generally attributed to the U.S. and Israel (for a summary of attacks on nuclear facilities, click here.

Very recently, a new piece of dangerous malware, TRISIS, which specifically targets the industrial controllers used for safety critical applications, including in nuclear plants, has been found in the Middle East.

So how worried should we be?

The good news is that the safety and security of nuclear facilities is taken very seriously. In the United States, cyber security at nuclear facilities is receiving increased attention from regulators, plant operators and technical experts. In addition, as the United States has an aging nuclear infrastructure, many of the plants are still operating mostly with analog controls and/or safety systems, meaning they are less vulnerable to cyberattacks.

Unfortunately, this attention to the cyber threat does not exist everywhere. A 2016 NTI study found that nearly half of the countries with relevant nuclear facilities had no regulations for cyber security at those facilities.

**Looking forward, there are a number of** concerning signs.

As recent attacks have confirmed, cyberattacks are getting increasingly sophisticated. Complex attacks are no longer just the purview of nations but can now be conducted by smaller groups. Furthermore, systems which may have been analog at one time are increasingly digital and increasingly complex. The growing Internet-of-Things will present additional challenges.

Responding to this growing threat is not easy. Airgaps, originally designed to counter untargeted attacks, are not effective against a determined adversary. Existing safety systems may not be effective against cyberattacks that can lead to failures that would never occur naturally. Furthermore, threats do not just arise from the internet—defenders must consider supply chain risks and the potential for insider threat.

NTI is increasingly focused on this area. NTI’s 2016 study concluded in the release of a report, Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities,that summarized the key pillars of a new strategy, urging operators to address fundamental issues such as system complexity and promoting the importance of an active defense. The report also highlighted the importance of developing transformational approaches (perhaps new, non-programmable solutions) that would be immune to cyberattacks. In addition to the need for a more robust strategy, the current shortfalls in global technical capacity must be addressed, perhaps by improving means to provide international assistance.

The cyber threat to nuclear facilities is serious, but the challenge going forward is evident. Threats and vulnerabilities will continue to mount. Today’s strategy is not sufficiently robust or scalable, and a high level of cyber security may never be compatible with current nuclear plant business models. Governments, regulators, facility operators, vendors, and experts need to accelerate our efforts to develop new approaches that can scale to the threats of the future.

#### Cyberattacks on nuclear power plants are devastating

Jeremy **Straub 19**, Assistant Professor of Computer Science, North Dakota State University, Ph.D. in Scientific Computing, M.S., M.B.A., and two B.S degrees, “A Cyberattack Could Wreak Destruction Comparable to a Nuclear Weapon,” The Conversation, 8/16/2019, http://theconversation.com/a-cyberattack-could-wreak-destruction-comparable-to-a-nuclear-weapon-112173, Accessed 24 June 22

People around the world may be worried about nuclear tensions rising, but I think they’re missing the fact that a major cyberattack could be just as damaging – and hackers are already laying the groundwork.

With the U.S. and Russia pulling out of a key nuclear weapons pact – and beginning to develop new nuclear weapons – plus Iran tensions and North Korea again test-launching missiles, the global threat to civilization is high. Some fear a new nuclear arms race.

That threat is serious – but another could be as serious, and is less visible to the public. So far, most of the well-known hacking incidents, even those with foreign government backing, have done little more than steal data. Unfortunately, there are signs that hackers have placed malicious software inside U.S. power and water systems, where it’s lying in wait, ready to be triggered. The U.S. military has also reportedly penetrated the computers that control Russian electrical systems.

Many intrusions already

As someone who studies cybersecurity and information warfare, I’m concerned that a cyberattack with widespread impact, an intrusion in one area that spreads to others or a combination of lots of smaller attacks, could cause significant damage, including mass injury and death rivaling the death toll of a nuclear weapon.

Unlike a nuclear weapon, which would vaporize people within 100 feet and kill almost everyone within a half-mile, the death toll from most cyberattacks would be slower. People might die from a lack of food, power or gas for heat or from car crashes resulting from a corrupted traffic light system. This could happen over a wide area, resulting in mass injury and even deaths.

This might sound alarmist, but look at what has been happening in recent years, in the U.S. and around the world.

In early 2016, hackers took control of a U.S. treatment plant for drinking water, and changed the chemical mixture used to purify the water. If changes had been made – and gone unnoticed – this could have led to poisonings, an unusable water supply and a lack of water.

In 2016 and 2017, hackers shut down major sections of the power grid in Ukraine. This attack was milder than it could have been, as no equipment was destroyed during it, despite the ability to do so. Officials think it was designed to send a message. In 2018, unknown cybercriminals gained access throughout the United Kingdom’s electricity system; in 2019 a similar incursion may have penetrated the U.S. grid.

In August 2017, a Saudi Arabian petrochemical plant was hit by hackers who tried to blow up equipment by taking control of the same types of electronics used in industrial facilities of all kinds throughout the world. Just a few months later, hackers shut down monitoring systems for oil and gas pipelines across the U.S. This primarily caused logistical problems – but it showed how an insecure contractor’s systems could potentially cause problems for primary ones.

The FBI has even warned that hackers are targeting nuclear facilities. A compromised nuclear facility could result in the discharge of radioactive material, chemicals or even possibly a reactor meltdown. A cyberattack could cause an event similar to the incident in Chernobyl. That explosion, caused by inadvertent error, resulted in 50 deaths and evacuation of 120,000 and has left parts of the region uninhabitable for thousands of years into the future.

Mutual assured destruction

My concern is not intended to downplay the devastating and immediate effects of a nuclear attack. Rather, it’s to point out that some of the international protections against nuclear conflicts don’t exist for cyberattacks. For instance, the idea of “mutual assured destruction” suggests that no country should launch a nuclear weapon at another nuclear-armed nation: The launch would likely be detected, and the target nation would launch its own weapons in response, destroying both nations.

Cyberattackers have fewer inhibitions. For one thing, it’s much easier to disguise the source of a digital incursion than it is to hide where a missile blasted off from. Further, cyberwarfare can start small, targeting even a single phone or laptop. Larger attacks might target businesses, such as banks or hotels, or a government agency. But those aren’t enough to escalate a conflict to the nuclear scale.

Nuclear grade cyberattacks

There are three basic scenarios for how a nuclear grade cyberattack might develop. It could start modestly, with one country’s intelligence service stealing, deleting or compromising another nation’s military data. Successive rounds of retaliation could expand the scope of the attacks and the severity of the damage to civilian life.

In another situation, a nation or a terrorist organization could unleash a massively destructive cyberattack – targeting several electricity utilities, water treatment facilities or industrial plants at once, or in combination with each other to compound the damage.

Perhaps the most concerning possibility, though, is that it might happen by mistake. On several occasions, human and mechanical errors very nearly destroyed the world during the Cold War; something analogous could happen in the software and hardware of the digital realm.

Defending against disaster

Just as there is no way to completely protect against a nuclear attack, there are only ways to make devastating cyberattacks less likely.

The first is that governments, businesses and regular people need to secure their systems to prevent outside intruders from finding their way in, and then exploiting their connections and access to dive deeper.

Critical systems, like those at public utilities, transportation companies and firms that use hazardous chemicals, need to be much more secure. One analysis found that only about one-fifth of companies that use computers to control industrial machinery in the U.S. even monitor their equipment to detect potential attacks – and that in 40% of the attacks they did catch, the intruder had been accessing the system for more than a year. Another survey found that nearly three-quarters of energy companies had experienced some sort of network intrusion in the previous year.

But all those systems can’t be protected without skilled cybersecurity staffs to handle the work. At present, nearly a quarter of all cybersecurity jobs in the U.S. are vacant, with more positions opening up than there are people to fill them. One recruiter has expressed concern that even some of the jobs that are filled are held by people who aren’t qualified to do them. The solution is more training and education, to teach people the skills they need to do cybersecurity work, and to keep existing workers up to date on the latest threats and defense strategies.

If the world is to hold off major cyberattacks – including some with the potential to be as damaging as a nuclear strike – it will be up to each person, each company, each government agency to work on its own and together to secure the vital systems on which people’s lives depend.

## Adv 2 - Cohesion

### UQ – AT Squo Solves [Deterrence by Denial]

#### There is no alternative---traditional deterrence fails---black market zero-day exploits, weak inspection, and missing ilaw.

University of Exeter 20. “Should NATO Adopt a Joint Offensive Cyber Capability?” September 2020. <https://socialsciences.exeter.ac.uk/media/universityofexeter/strategyandsecurityinstitute/pdfs/mstrat/James_Prideaux.pdf>. //AN

Joint Offensive Cyber Capabilities and Cyber Deterrence-by-Punishment

It is necessary to explain the limitations of NATO’s current deterrence-by-denial policy to contextualise cyber deterrence-by-punishment. After all, one may ask: why not just bolster NATO’s cyber defences? While defensive measures are absolutely essential for stopping attacks that have already launched, they are severely limited at deterring potential attacks. This probably explains why NATO does not mention ‘cyber deterrence-by-denial’ in its policy documents, but rather cyber- deterrence more broadly.74 The main problem with deterrence-by-denial is that cyberattacks are very low cost for an aggressor, both in terms of the effort expended to launch an attack and the cost of penalties.75 The existence of a huge black market offering everything from zero-day exploits to off-the-shelf services to conduct DDoS attacks facilitates the ease with which cyberattack technology can be acquired.76 Meanwhile, the lack of an inspection regime and the infancy of international legal frameworks reduces the risk of penalties.77 This gives aggressors little incentive to stop attacking, even in the face of strong defences.

Meanwhile, defence in cyberspace is porous in nature.78 Every system has vulnerabilities and exploiting them is only a matter of time, means and determination.79 This permeability is a serious problem, because defenders must convince aggressors that an attack will have little to no effect for deterrence-by-denial to be effective.80 NATO’s deterrence-by-denial posture certainly makes attacks harder to conduct, but this has not deterred the hundreds of significant attacks it faces monthly. Clearly, a discussion over cyber deterrence-by- punishment is warranted.

The cyber deterrence-by-punishment that offensive weapons afford serves to bolster and complement deterrence-by-denial. This is because it threatens the imposition of costs where, in the absence of retaliation, there would be hardly any.

### UQ – Now Key

#### Allied cohesion over cyber norms key now—else NATO credibility and deterrence crumbles

Lonergan and Moller 4/27 (ERICA D. LONERGAN and SARA B. MOLLER, Erica D. Lonergan is an assistant professor in the Army Cyber Institute and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University. Sara B. Moller is a former Eisenhower Fellow at the NATO Defense College and will be joining the Center for Security Studies at Georgetown University later this year, “NATO’s Credibility Is on the Line with its Cyber Defense Pledge. That’s a Bad Idea,” POLITICO, 4/27/2022, <https://www.politico.com/news/magazine/2022/04/27/nato-credibility-cyber-defense-pledge-russia-ukraine-00027829>) -lh

With little chance of improved NATO-Russian relations any time soon, time is of the essence to get this right. The allies should begin the hard political legwork now to ensure members get on the same page before NATO’s June summit, if not sooner. Achieving consensus on significant cyber issues has previously taken time. NATO’s attribution of the Microsoft Exchange hack last summer to China was an important step for the alliance and sent a strong signal to our adversaries. But it took months to reach agreement on the statement; the hack was uncovered in March 2021 and the NATO statement was not made public until July. In the current crisis, the alliance will not have the luxury of waiting four (or more) months to agree on a response. To avoid incurring damaging costs to NATO’s credibility and its deterrent powers, the allies should refine their cyber policy, now.

### I/L – AT Defense [Attribution]

#### Attribution is possible now through using past data, attacker’s mistakes, and political context, but if anything, a joint OCO bolsters it through freeing up available resources.

University of Exeter 20. “Should NATO Adopt a Joint Offensive Cyber Capability?” September 2020. <https://socialsciences.exeter.ac.uk/media/universityofexeter/strategyandsecurityinstitute/pdfs/mstrat/James_Prideaux.pdf>. //AN

The main critique of deterrence-by-punishment is that it is hard to attribute cyberattacks. This reduces the credibility of deterrence because it is too difficult to tell which systems to retaliate against.122 Nevertheless, though attribution is costly and time-consuming, it is possible.123 On a technical level, malware’s source code and programming style can be mapped against previous incidents.124 In Iran, these forensics revealed similarities between Stuxnet and another virus developed by the NSA called Flame, intensifying accusations against US involvement in both tools.125

Furthermore, anonymity in cyberspace is not as pervasive as critics make out, because attackers do make mistakes. For instance, the Chinese hacker group APT1 is recognisable for its sloppy re-use of social engineering tactics and specific infrastructure.126 Additionally, attribution is facilitated by examining the history and politics surrounding an attack; in the case of Stuxnet, the tense relations between America, Israel and Iran narrowed down the list of likely sources.127 What’s more, Russia is increasingly likely to use its state security services to conduct attacks, instead of more anonymous but lower skilled non-state hackers.128 This suggests that attacks from NATO’s main adversary in cyberspace may become more traceable.

Most importantly, a joint offensive cyber capability would benefit NATO precisely because attribution is time consuming and costly. The quality of attribution is a function of available resources – the more there are, the more accurately one can attribute an attack.129 Although pooling NATO’s capabilities would not increase the quantity of resources available, it would improve resource allocation and thus allow NATO to ‘do more with the same’.130 In several countries, the growth of offensive cyber has already allowed for greater specialisation in cyber operations. US Cyber Command (USCYBERCOM) now has 133 teams, making it easier to dedicate teams to specific tasks.131 This division of labour, enabled by pooling capabilities, would hopefully allow NATO to devote specialised units to cyber forensics. This would likely increase their output, facilitating timely and accurate attribution.

### I/L – Intrusions

#### US intrusions into allied networks increasingly deteriorate relations and provide adversaries with new avenues to exploit.

Max Smeets 19. Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich, Director of the European Cyber Conflict Research Initiative, and Author of “No Shortcuts: Why States Struggle to Develop a Military Cyber-Force.” “Cyber Command’s Strategy Risks Friction With Allies”. Lawfare. 5-28-2019. https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies. //AN

Much has been written about the fundamental changes in U.S. cyber strategy. U.S. Cyber Command’s vision of “persistent engagement” and the Department of Defense’s new strategy of “defend forward” have, in particular, led to numerous critical remarks about the risks of escalation between the U.S. and its main adversaries in cyberspace.

These debates are worth continuing, including about what the change in strategy means for establishing norms in cyberspace. But commentators have so far ignored a key dimension: The strategy’s main implications may not reside in how it changes the dynamics between the U.S. and its adversaries but, instead, in how it affects broader alliance relationships, especially beyond the Five Eyes (Australia, Canada, the U.K., the U.S. and New Zealand). U.S. Cyber Command’s mission to cause friction in adversaries’ freedom of maneuver in cyberspace may end up causing significant friction in allies’ trust and confidence—and adversaries may be able to exploit that.

Operating “Seamlessly, Globally, and Continuously”

Cyber Command’s new strategy seeks to operate “seamlessly, globally, and continuously.” It states that “[s]uperiority through persistence seizes and maintains the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver.” According to the strategy document, Cyber Command intends to do this “as close as possible to adversaries and their operations,” connecting persistent engagement to the Pentagon’s principle of “defending forward.”

In an article for Joint Force Quarterly (JFQ), NSA Director and Cyber Command head Gen. Paul Nakasone writes: “We must instead maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries.”

When Nakasone says the U.S. must get “as close as possible to adversaries and their operations,” he implies that the U.S. seeks to achieve effects that are outside of its own networks and beyond the networks of its adversaries. This vast area is not ungoverned space. It includes, for example, routers in Nairobi, servers in Denmark or operating infrastructure in any other country around the world.

Blue Space, Gray Space and Red Space

In the JFQ article, Nakasone also states that “if we are only defending in ‘blue space’ we have failed.” This use of terminology as well as talk about “operating close to the adversary” evades one issue: It is unclear whether Cyber Command only seeks to cause friction in “red space” or if it seeks to compete in “gray space” as well. These terms are often confused and not well-understood. (The terms “gray zone”—areas where it’s unclear whether the government has legal authority to act—and “gray space” are also frequently confused.) In fact, the issue was raised for “further exploration” at Cyber Command’s 2018 symposium, specifically understanding the “relevance of concepts like area of responsibility and red-blue-gray space to the cyberspace domain.”

Joint Publication 3-12 (JP 3-12) on cyberspace operations, prepared under the direction of the chairman of the Joint Chiefs of Staff, explains the terminology:

The term “blue cyberspace” denotes areas in cyberspace protected by the US, its mission partners, and other areas DOD may be ordered to protect. Although DOD has standing orders to protect only the Department of Defense information network (DODIN), cyberspace forces prepare on order, and when requested by other authorities, to defend or secure other United States Government (USG) or other cyberspace, as well as cyberspace related to critical infrastructure and key resources (CI/KR) of the US and PNs [partner nations]. The term “red cyberspace” refers to those portions of cyberspace owned or controlled by an adversary or enemy. In this case, “controlled” means more than simply “having a presence on,” since threats may have clandestine access to elements of global cyberspace where their presence is undetected and without apparent impact to the operation of the system. Here, controlled means the ability to direct the operations of a link or node of cyberspace, to the exclusion of others. All cyberspace that does not meet the description of either “blue” or “red” is referred to as “gray” cyberspace.

Gray space is defined based on the nodes adversaries control. This means the vast area between U.S. government-owned networks and adversaries is not considered to be gray space. Instead, if for instance the GRU (Russia’s military intelligence agency) controls a node in the Netherlands, it is considered to be red space based on JP 3-12. And it’s worth mentioning that the notion of control is open to interpretation by states.

This means that if Cyber Command seeks to operate only in “red space,” its activities will still have global reach (globally). It also suggests that red space grows as adversaries expand their operational activity. Most importantly, this implies that if Cyber Command seeks to achieve “effects” in gray space, this will involve operating infrastructure that adversaries do not control—which is to say those systems or networks on which adversaries merely have a presence or are not active at all.

What’s New Under the Sun?

What’s really new here? The United States has long operated in networks “close to the adversary.” As Ben Buchanan’s book, “The Cybersecurity Dilemma,” demonstrates, the U.S. has long acted as an “observer” in gray space, gathering intelligence of adversarial activity in those others’ networks. In fact, information has become public concerning a case in which the Five Eyes collected intelligence about an espionage platform (dubbed “Snowglobe” by the Canadian Intelligence Agency CSEC and “Animal Farm” by Kaspersky Lab) of an allied country, France, likely operating in adversarial networks in the Middle East. In other words, the practice of fourth-party collection is nothing new. And the U.S. has also long acted in foreign nonadversarial networks as a “passerby,” transiting through gray space networks to access an adversarial network.

But the new Cyber Command and Defense Department strategy changes the nature of the U.S. military’s behavior within those systems and networks. Under the new strategy, Cyber Command wants to be an active disrupter on those networks. It wants to achieve effects.

The only known precedent is Cyber Command operators wiping Islamic State propaganda material off a server located in Germany. The German government was notified in some fashion but not asked for advance consent, causing much frustration.

This will likely lead to a systematic scaling up: Cyber Command now also seeks to be an active disrupter on those networks “globally, continuously and seamlessly”—not regionally and sporadically.

The Danger of Operating Seamlessly in Allied Networks

Operating instantly makes sense considering the potential operational tempo of adversaries: You can’t have protracted diplomatic discussions for two months with an ally about whether or not to take down some command and control infrastructure of an adversary hosted in the allied country. You don’t have days, let alone months. As a participant mentioned at the recent Chatham House Rule 2019 Cyber Command Symposium on strategy: “Opportunities within this domain are fleeting.”

Operating seamlessly could also make sense if an ally does not mind the U.S. coming into its networks to address the malicious activity. In this vein, the U.S. can continue to build partnerships with countries that do not have the capacity to defend against cyber attacks on their own.

But, what if an allied country is not keen on having the U.S. military in its networks, actively, seamlessly, and continuously disrupting an adversary’s cyber operations? As the German case shows, this scenario will likely come up a lot more in the near future.

In other words, in seeking to successfully create friction in cyberspace for adversaries, Cyber Command may also seek to act within allied networks, even if the ally does not approve. It might even be successful in its mission, causing friction in adversaries’ operations before they cause serious harm to the U.S. But this strategy runs a real risk of undermining allies’ trust and confidence in ways that are subtle and not easily observable. This ought not to be overlooked, especially since this element may itself be exploited by adversaries.

Adversaries don’t randomly choose which intermediate nodes to direct their operations through. If Russia has the choice to go through a network that would raise some serious diplomatic friction between the U.S. and a U.S. ally, or operate through a network that would cause no diplomatic friction for the U.S., what would it prefer? It would make sense for adversaries to operate through the networks of exactly those countries with which the U.S. has a strong relationship but that do not want the U.S. to operate within their networks causing any effects.

Russia is already good at exploiting divisions between the U.S. and its allies. Cyber Command’s new strategy might give it another avenue to do so.

### I/L – AT OCOs Bad

#### Individual OCOs are bad–but a joint capability would increase NATO ability to control retaliation.

University of Exeter 20. “Should NATO Adopt a Joint Offensive Cyber Capability?” September 2020. <https://socialsciences.exeter.ac.uk/media/universityofexeter/strategyandsecurityinstitute/pdfs/mstrat/James_Prideaux.pdf>. //AN

A third criticism is that retaliatory cyberattacks can easily cause collateral damage and are dangerously escalatory. Since the distinction between internal and external networks is often blurred, attacks directed at a defender’s network may spill over into external networks.138 Adopting a persistent engagement approach will also pose increasing risks for escalation.139 This is aggravated by the absence of international agreements determining unacceptable behaviour in cyberspace.140 This dissertation does not dispute these criticisms; on the contrary, they strengthen the case for a joint-NATO offensive cyber capability. This is because one of the main solutions to these problems is increased control of cyber operations.141 A joint capability would increase NATO members’ control, because it would facilitate agreement on how to integrate offensive cyber effects into a Flexible Deterrent Options (FDO) package.142 FDOs are meant to allow for a gradual increase of pressure in response to threats, limiting the chance of uncontrolled escalation.143 Chapter 5 outlines how offensive cyber could be integrated into an FDO package in more detail. Leaving members to adhere to their own FDOs undermines the unity of NATO’s response to an attack. Similarly, the extra control that centralised C2 offers would allow NATO to reduce the risk of cyberattacks causing collateral damage.144 Though this risk cannot be eliminated entirely, joint C2 and standardised offensive cyber doctrine could add extra controls that seem unlikely to appear at the CyOC. For instance, doctrine could dictate that large attacks should only be launched against military networks; air defence systems are unlikely to be on the same network as hospitals, mitigating the chance of collateral damage.

### I/L - Deterrence

#### A joint OCO unlocks cyber-deterrence:

#### 1. It upskills all NATO members with cyber-intelligence and expertise.

University of Exeter 20. “Should NATO Adopt a Joint Offensive Cyber Capability?” September 2020. <https://socialsciences.exeter.ac.uk/media/universityofexeter/strategyandsecurityinstitute/pdfs/mstrat/James_Prideaux.pdf>. //AN

First, NATO’s cyber-deterrence would be more credible because a joint cyber capability would facilitate knowledge transfer between member states. For deterrence to be successful, NATO has to convince aggressors that it can retaliate against the right aggressor in a manner that imposes unacceptable costs. However, state and non-state actors, like the Fancy Bear cyber-espionage group likely associated with the Russian security services, know that the disaggregation of member states’ cyber assets makes this harder to achieve.89 The primary reason for this separation of effort is that intelligence on adversaries’ cyber vulnerabilities is closely guarded by national intelligence agencies.90 This intelligence is absolutely critical for effective cyber attacks, since it is necessary to understand the targeted systems in great detail.91 The CyOC will not go far enough in fostering intelligence sharing, even though it aims to ‘integrate cyber capabilities into NATO planning and operations’.92 It is certainly a step forward, but of those states that have offered their cyber effects to NATO, France and America have clearly stated they will retain full control of their operations and capabilities.93 This lack of joint operational authority poses a significant challenge, as it appears the centre will serve to coordinate rather than oversee operations.94 It will prove very hard to achieve even this when members’ capabilities vary greatly in their maturity and development. Whereas Germany is said to have thousands of ‘information and cyber officers’, other European states have hardly any.95 Overall, NATO in its current state is not optimised for deterrence-by-punishment and the CyOC will do little to improve this.

Instead, pooling members’ cyber-intelligence and cyber-sabotage expertise would encourage intra-alliance knowledge transfer. Knowledge transfer in organisations is the process through which one unit, like a department or division, is affected by the experience of another.96 Empirical evidence suggests that interconnected organisations like franchises and chains hold comparative advantages over their autonomous counterparts, due to the ability to transfer knowledge between their constituent elements.97

This would apply to NATO in two ways. First, organisational integration of cyber-intelligence would facilitate knowledge transfer, as demonstrated by the preparations behind Stuxnet.98 To design such a complex computer worm, the US National Security Agency (NSA) collaborated with Israel’s counterpart, Unit 8200, largely because it had deep intelligence about operations at Iran’s Natanz facility.99 This was vital for the attack’s success, because the individual control systems they targeted had unique configurations, making them harder to penetrate.100

Second, merging cyber-sabotage capabilities would similarly aid knowledge transfer. There are two types of knowledge required for cyber-sabotage operations. One type is explicit and can be transferred in a systematic manner, such as knowledge of how a SCADA system works or how to write code in a certain programming language.101 The other, more significant type is tacit knowledge, which is difficult to transfer to another person by verbalising or writing it down.102 This could include a hacker’s accumulated experience or knowledge of a cyber command’s implicit operational processes.103 Tacit knowledge can be shared, but this is done by performance and learning by example.104 A joint offensive cyber capability would provide an excellent opportunity for this to happen.105 Both forms of knowledge transfer would be especially useful for ‘upskilling’ those NATO members that lack the advanced technical expertise in America, Britain, France and Germany. In practice, this would make acquiring cyberattack tools and training personnel easier and cheaper.106 The importance of training technical personnel should not be underestimated, because all members are short of them but most lack the resources to attract them.107 Pooling capabilities is one way of alleviating this pressure. In turn, the cumulative benefits of knowledge transfer would likely make it easier to launch retaliatory attacks against the right aggressor and impose unacceptable costs more successfully. Overall, this would improve the credibility of a deterrence-by- punishment posture.

#### 2. It improves attack coordination.

University of Exeter 20. “Should NATO Adopt a Joint Offensive Cyber Capability?” September 2020. <https://socialsciences.exeter.ac.uk/media/universityofexeter/strategyandsecurityinstitute/pdfs/mstrat/James_Prideaux.pdf>. //AN

Furthermore, a joint capability would improve NATO’s offensive cyber C2, improving attack coordination and mitigating fratricide. This is because NATO’s ‘volunteer’ system and its CyOC mark a striking departure from the way it usually handles C2of members’ assets.108 The NATO Force Structure dictates that conventional forces like ships and tanks come under the full operational control of an assigned NATO commander.109 However, according to a retired USAF Colonel leading the implementation of NATO’s 2017 cyber policy, the C2 problems inherent in the volunteer system make it ‘far from ideal’.110 This is because NATO commanders do not know the details of capabilities available to them, such as their legal consequences, impeding the decision-making process.111 Commanders also want to know how using cyberweapons might conflict with other operations; without this they are left ‘flying blind’.112 Failing to coordinate operations can have far-reaching consequences. For instance, intelligence agencies’ reconnaissance of target networks needs to be coordinated with cyber-sabotage operations, so they do not interfere with each other.113 Disaggregated C2 can even result in fratricide on other allies’ networks, because the distinction between internal and external security threats is much harder to ascertain in cyberspace than in the other four domains.114 The CyOC is a step towards resolving this, but until a NATO commander has control over members’ capabilities, these problems will not be fully resolved.

#### 3. It streamlines decision-making.

University of Exeter 20. “Should NATO Adopt a Joint Offensive Cyber Capability?” September 2020. <https://socialsciences.exeter.ac.uk/media/universityofexeter/strategyandsecurityinstitute/pdfs/mstrat/James_Prideaux.pdf>. //AN

Additionally, a unified offensive cyber C2 structure would aid scenario planning and speed up decision-making. This is important, because NATO needs to streamline its current decision-making process in the cyber domain.115 A single command would help members agree on appropriate forms of retaliation in cyberspace in different scenarios, bolstering the credibility of deterrence-by-punishment even further. Without a clear command structure, it is very difficult for the 30 NATO allies – who have different threat perceptions and suffer from a lack of cohesion – to agree on effective response scenarios in contingency planning.116 As a case in point, Estonia is willing to strike back when attacked online, given its memory of the 2007 attack and its proximity to Russia.117 However, Estonian officials do not know whether other allies will support them, validating some scholars’ arguments that NATO needs to find common ground in cyber contingency planning.118 The secrecy that shrouds allies’ capabilities and the uncertainty surrounding cyber scenario planning might explain why offensive cyber effects do not feature in NATO’s mission planning process.119 This is not to say that NATO needs to publicly agree on a ‘red line’ in cyberspace that could trigger an Article 5 response. If anything, NATO’s current strategic ambiguity is key for deterring attacks that fall just below a defined threshold.120 However, unifying cyber C2 would help them carry out scenario planning behind closed doors, improving the Alliance’s readiness. Speeding up the decision-making process is crucial given how long it can take to attribute and then launch a retaliatory attack.121 Overall, streamlined scenario planning and decision- making, augmented by improved coordination of cyberattacks, would strengthen the credibility of deterrence-by-punishment. Although aggressors like Fancy Bear would not know when a certain threshold has been crossed, it would tilt their risk-benefit calculus knowing an attack could trigger a faster, well-coordinated retaliatory attack.

#### 4. It fortifies collective defence and conventional warfare.

University of Exeter 20. “Should NATO Adopt a Joint Offensive Cyber Capability?” September 2020. <https://socialsciences.exeter.ac.uk/media/universityofexeter/strategyandsecurityinstitute/pdfs/mstrat/James_Prideaux.pdf>. //AN

The benefits of a joint offensive cyber capability for conventional collective defence are far easier to discern than cyber-deterrence. NATO could use it for tactical operations to support combat operations and shape the battlefield.149 The most obvious scenario this could be used in is if NATO were attacked by Russia, the only state whose conventional forces pose a threat. Offensive cyber capabilities would be an important force multiplier in the event of a Russian attack on the Baltic states, where local force ratios would favour the attacker.150 Battlefield NATO commanders could use cyber effects to disrupt Russian C2 networks or the software on advanced weapons, like surface-to-air missiles or fighter aircraft.151 Anti-access/ area denial operations (A2/AD) like these seek to deny attackers the ability to bring their assets into a contested region and prevent them from operating freely within it.152 Offensive cyber capabilities have already been used in this way to great effect. In 2007, the Israeli Air Force allegedly used the Suter computer program to conduct an airstrike against a nuclear reactor in Northern Syria.153 This fed Syria’s air defence systems a false-sky picture, allowing Israeli fighter jets to successfully bomb the reactor without being detected.154 In many ways, cyber effects will become a basic necessity in conventional warfare. No modern air force would enter combat without electronic warfare (EW) capabilities; as cyber and EW merge into a single activity, air operations will require cyber support.155 Overall, since cyberweapons can be so effective on the battlefield, they would clearly aid NATO’s warfighting ability.

A joint capability would be the best way to fulfill this role. The CyOC is hoping to coordinate battlefield effects in a similar way.156 However, the secrecy of members’ capabilities and the persistence of sovereign operational authority will make it harder for SACEUR to quickly decide whether and how to use cyberweapons. This would be detrimental in a hot war scenario, the rapid pace of which demands decisions to be made ‘at the speed of relevance’.157 Additionally, offensive cyberweapons depend heavily on force integration to be effective on the battlefield.158 The greater the integration between conventional and cyber operations, the greater the multiplier effect achieved – as proved by Israel’s highly coordinated airstrike.159 However, it seems the current volunteer system is lacking in this regard. A senior NATO official has acknowledged the Alliance needs to get better at aligning its cyber assets with its Enhanced Forward Presence (EFP) in the Baltics as part of an A2/AD strategy.160 This means it needs to improve coordination with the EFP’s graduated response plans and practise battlefield cyberattacks in a more realistic way during exercises.161 To this end, the improved C2, knowledge transfer and resource allocation that a joint cyber capability offers would augment not just cyber-deterrence but collective defence too.

### I/L – Cohesion Key

#### NATO cohesion key to development of technologies and mitigating future cyber risks

Bellasio and Silfversten 20 (Jacobo Bellasio and Erik Silfversten, Bellasio is the Senior Analyst Defence, Security and Infrastructure RAND Europe, Silfversten is the Co-Director Centre for Futures and Foresight Studies RAND Europe, “The Impact of New and Emerging Technologies on the Cyber Threat Landscape and Their Implications for NATO,” Cyber Threats and NATO 2030: Horizon Scanning and Analysis, 2020, https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030\_Horizon-Scanning-and-Analysis.pdf)- lh

C. Strengthening Trust and Interoperability Across the Alliance The coming decade will be of pivotal importance to NATO as a period characterised by a continuously evolving technology landscape with potentially disruptive effects in the cyber domain and beyond. In an era of uncertainty, constrained resources and political tension, cooperation and trust will be fundamental enablers of an agile, technology-driven and digital NATO. Only through joint efforts will NATO truly be able to harness the potential of the emerging technologies discussed in this chapter and successfully mitigate the risks and threats they may pose in the future. The need for trust therefore extends to both trust in technology and trust in the Alliance and its member states.

Similar to how the effects of emerging technologies should not be treated in isolation, NATO’s response to emerging technologies must be one of joint efforts and interoperability. Technical, legal, financial and organisational barriers to the implementation of emerging technologies are more likely to be overcome through joint capability and force development efforts, which will, by extension, also help build trust and facilitate interoperability. Several of the emerging technology areas discussed in this paper would place significant data, infrastructure and interoperability requirements on NATO, which may be particularly difficult to overcome given the current state of data heterogeneity and sometimes incompatible digital infrastructure across the Alliance. Several emerging technologies would also require interoperability in relation to shared vocabularies of technical terms, norms, standards and organisational practices, as well as human interoperability and joint training and exercising. For example, AI has been highlighted as a potential area of concern where a lack of interoperability and common definitions paired with technological mismatches could erode Alliance cohesion (Dufour, 2018).

Joint efforts are, therefore, likely to help overcome these challenges and barriers to NATO harnessing emerging technologies in the next decade. While the 30-member Alliance may be at a competitive disadvantage compared to single state or non-state adversaries in relation to interoperability barriers, NATO’s collective strength may also serve as an enabler for technological superiority. Joint planning, requirement setting, and development may enable individual member states to pursue specialisation in aspects of particular emergent technology areas, thereby allowing other countries to pursue other specialisations and, by extension, increasing the overall capability within the Alliance.

#### Alliance cohesion over cybersecurity key to prevent exploitation of internal disagreements

Author?? 21 (author, “The V4 towards a new NATO Strategic Concept and the EU Strategic Compass,” 2021, https://www.europeum.org/data/articles/the-v4-towards-a-new-nato-strategic-concept.pdf)-lh

This issue, over which there are no major disagreements among V4 states, comprises cybersecurity and the development of the alliance’s resilience in cyberspace. All member states agree that this new operational domain has become vital in all types of conflicts, and therefore must be a key area of cooperation amongst NATO members. Our experts also noted that cyber resilience is an area where cohesion can be achieved at the lowest cost. This does not diminish the importance of the topic at hand; rather, it shows us that there are still key challenges which have to be overcome in the near future. Despite the fact that it is not a physical area of operations, cyberspace cannot be separated from the aforementioned geopolitical tensions. It is also connected with the question of the alliance’s stance towards Russia and China; both of these countries have robust capabilities in cyberspace, which they are keen to utilise in the developing great power competition. This factor is also relevant on a lower level, connected to other disruptive and hostile powers such as Iran or North Korea, as well as non-state actors such as international terrorist organisations. The V4 countries naturally have lower levels of readiness in cyberspace than the great powers do; however, it is entirely possible for small and medium-sized powers to enhance their resilience against cyberattacks. For example, Estonia reacted (with the support of NATO) to Russian cyber aggression, and developed robust defensive infrastructure and practices, which should be emulated by other countries.

Due to its limited size, resources, demography, and industrial capacity, Estonia could not aspire to such a power position in terms of conventional warfare. International cooperation in cyber resilience is also a force multiplier, and no country can or should rely solely on itself. Thus, it is in the interests of security and political stability to have more pronounced cooperation in this field. The V4 can be a champion in this area: Poland is a great example of the rapid development of the cyber industry, deeply anchored in the transatlantic alliance.

The security environment in the 21st century is fundamentally different to any time in the past. The geopolitics of today is not about the possession of territory and material resources, but about the interdependence of economies and companies, as well as the incorporation of new technologies, such as 5G networks and AI, often developed either in the US or China. In such an environment, NATO should incorporate defence capabilities into the fields of cyberspace, countering fake news, human trafficking, and weaponising migration. NATO must be prepared for future challenges; however, this is a much harder task to accomplish in the V4 region than it is in Western Europe. This can and should be seen as an opportunity. While the V4 countries have neither the population bases nor the resources to compete with global leading players, the knowledge-based economies of tomorrow create a solid chance even for small and medium-sized states to catch up with wealthier and bigger states.

1.1.6. Resilience In order to tackle these challenges, NATO members have to be resilient, but there is also a need for a terminological debate on the merits and meaning of resilience. We need to differentiate between the classical understanding of resilience as civil preparedness relating to crisis response and management; democratic resilience relating to institutions, values and commitments; and cyber resilience. While cyber resilience and civil preparedness are low-hanging fruits from a cooperation perspective, democratic resilience will be a subject of heated political discussion.

In the coming years, NATO will begin to see more and more so-called “homeland deployments”. These will be mainly in response to climate change and caused by extreme weather events such as floods, wildfires and heavy storms. With the increasing intensity of such events, civilian agencies responsible for crisis response and management will not have sufficient capabilities, leading to the need for deployment of armed forces. On a mass scale, we witnessed such a scenario in 2020, where armed forces were deployed to support the countering of the COVID-19 pandemic. Central topics in Alliance discussions on how to adapt to these coming challenges should include enhancing the interoperability of armed forces with civilian agencies in crisis situations, reviewing the adequacy of national legal frameworks, and refocusing CIMIC efforts from peacebuilding missions abroad to “home front” deployments. Of course, all this is directly connected to the need for enhanced resilience building and civil preparedness.

The NATO 2030 report by the Secretary General outlined some necessary reforms in terms of political decision-making processes; it suggested changes to the fundamental underpinnings of NATO and, therefore, alliance cohesion itself. The report, written among others by Wess Mitchell, is a thought-provoking document. However, it is highly unlikely that the decision-making process will truly undergo a fundamental procedural change, nor is it clearly in the Alliance’s interest to reform this aspect. NATO’s current decision-making process reflects decades of tradition and political will. It maintains and underpins internal cohesion, to the benefit of all NATO allies. The V4 countries share the positive sentiment that the current consensus-based process is within the group’s best interest. Leaving consensusdecision-making behind in any area promotes a perception of decreased cohesion to our adversaries and a potential angle where internal disagreements might be exploited to undermine the alliance. This is a risk factor that all NATO allies – particularly the V4 member states, which are reliant on NATO’s traditional threat response capabilities – want to avoid.

#### Cohesion over cyber norm-development reduces risk of cyberattack escalation

Davis 19 (Susan Davis, “NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE,” NATO Parliamentary Assembly, 8/13/2019, https://www.nato-pa.int/download-file?filename=sites/default/files/2019-09/148%20STC%20Davis%20-%20NATO%20IN%20THE%20CYBER%20AGE%20-%20fall%20revision%20-%20clean%2011.9.19.pdf)-lh

Policy circles within the Alliance and beyond continue to debate how cyber attacks affect stability during crises and armed conflict. Which types of cyber attacks would be de-escalatory, escalatory, or neutral? Would the answer differ depending on when, during a crisis or an armed conflict, they would be launched? And are there significant differences between various states on these answers? States most likely do not see a cyber attack as a viable option for a pre-emptive first strike. However, in a crisis or pre-war situation, they could perceive a significant “cost of going second” (Davis, 2014). In such situations, one side “may well be frightened of what would happen if the other side attacks and may be convinced that going first will be advantageous” (Davis, 2014). This could lead to high escalatory risks in a crisis. Another key problem is the difficulty of determining the intent of a cyber intrusion (Lindsay, 2015). When a defender detects a breach, he may not know whether the intruder wants to spy on him, conduct forward defence, gain a foothold for future defensive measures, or prepare for an imminent or future cyber attack (Slayton, 2017). It is extremely difficult to gauge intent in cyber space, and, in such cases, states tend to assume the worst (Hennessey, 2017). As a result, this can lead to misperception and an escalatory spiral (Slayton, 2017). In sum, escalation dynamics deserve considerably more attention. For now, however, the Alliance should seek to reduce escalatory risks through clear diplomatic messaging and engagement; a high level of transparency on cyber policies; examining escalation dynamics in exercises; as well as support to norm-development and confidence building measures.

III. NATO CYBER POLICY 23. At the political level, the Alliance continues to adapt its cyber security, defence, and deterrence policies through regularly updated action plans with concrete objectives and timelines. This section outlines NATO’s: - overarching strategies to counter cyber attacks; - cyber capability development; - the integration of cyber capabilities into NATO planning; - concrete cooperation in NATO; and - NATO’s cyber partnerships.

A. NATO’S OVERALL CYBER STRATEGY 24. As armed forces around the world, including in potential adversary states, build up their cyber capabilities, NATO and its member states must devise strategies and policies to counter the threat of serious state-directed cyber attacks. Overall, NATO is leaning heavily on the same general strategies it uses to counter other attacks: dissuasion by denial and deterrence by punishment. However, Allies should continue to support work on international norms and engage in serious discussions if and how strategies such as persistent engagement, as outlined above, can supplement overall NATO strategy.

1. Norms in Cyber Space 25. Due to the specific characteristics of malicious cyber code, arms control, disarmament, and non-proliferation measures very likely remain beyond reach for now, most importantly because verification seems impossible. However, the further development of norms in cyber space could become an important pillar of support against such attacks. NATO continues to argue that international law applies to cyber space, including international humanitarian law and the United Nations Charter. This is also in line with the declaration of the 2013 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE, 2013). The Alliance has declared its support for “work on voluntary international norms of responsible state behaviour and confidence-building measures regarding cyberspace” (NATO, 2016b). Allies furthermore made clear that they “stand to benefit from a norms-based, predictable, and secure cyberspace” (NATO, 2018a). However, it is unrealistic to expect that NATO, as an Alliance of 29 sovereign nations, could become the primary driving force for the further development of norms. Instead, individual Allies must continue to drive this effort in the international community and encourage other member states to do the same.

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

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

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

#### **Lack of cohesion on cyber spills over – emboldens adversaries**

**Kramer 20** – Franklin Kramer is a member of the board at the Atlantic Council and the Former Assistant Secretary of Defense for International Security Affairs. “NATO needs continuous responses in cyberspace”. Published December 9, 2020. <https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/> //DG

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

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

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

President-elect Biden and his team have pledged to renew US leadership in cooperation with Allies and partners. That agenda should start at NATO, and a key focus should be on cybersecurity. In early NATO meetings, the Biden administration should champion a cybersecurity continuous-response campaign, built around three key actions.

First, NATO should require the development and implementation of resilient cybersecurity architectures for itself, its members’ forces, and its key critical infrastructures. **A resilient cybersecurity architecture involves an integrated set of capabilities that work as a system to reduce the disruptive effects of adversaries** in cyber. Key elements of a resilient architecture should include use of private sector cloud technology; zero-trust architecture for effective access management; development of secure hardware capabilities; and machine-learning and artificial-intelligence-augmented cyber defenses. This architecture also needs to be flexible to incorporate emerging technologies as they are developed.

NATO itself cannot develop such architectures. It can, however, underscore their necessity and require its members to do so, using the NATO Defense Planning Process (NDPP), acquisition procedures, standards and targets, and innovation from Allied Command Transformation to support a comprehensive research and development effort. In establishing requirements for these resilient architectures, NATO must recognize that one size will not fit all. Not only will requirements differ among military, government, and critical infrastructures operators, but, as has been shown in the development of autonomous vehicles and space capabilities, there are a variety of different approaches that may prove effective. In fact, having diversity within these capabilities will increase resilience by complicating adversaries’ abilities to infiltrate and attack them.

Second, NATO, in coordination with its nations, should undertake active cyber defense. Even the best exclusionary capabilities in a cybersecurity resilient architecture can fail due to technical loopholes or human error. As a result, the Alliance needs “active cyber defenses” that can create resilience even when an attacker has breached cyber protections. These capabilities affect only those networks in which operators and owners have installed them and are not for offensive purposes. As the US National Security Agency explains, key elements of active defense capacities include “real-time communications,…sensors that report data on the current state of the network, sense-making analytics to understand the current state, automated decision-making to decide how to react to current state information, and capabilities to act on those decisions to defend the network.” NATO should include such active defense capabilities as a requirement of an overall resilient cybersecurity architecture.

As a key element of active cyber defense, NATO must be capable of hunting for adversaries within cyber systems critical to defense. The Alliance should develop highly capable expert hunt teams to review system activities, detect anomalies, and defeat intruders, for example by deleting malware and closing unnecessary ports. NATO can significantly enhance Allies’ active defense efforts by establishing an NDPP requirement for national cybersecurity hunt teams, along with command arrangements for those teams in both hybrid and Article 5 contingencies. It should also establish several NATO Standing Cybersecurity Hunt Teams that would operate with the consent and active partnership of national governments and critical infrastructure network operators. As Microsoft has explained the role of hunt teams, Standing Cybersecurity Hunt Teams, acting in conjunction with national capabilities, can contest the continuous cyber campaigns of Russia and China. According to the US Department of Homeland Security, such hunt teams can conduct deep technical analyses of live networks to identify “previously unobserved threats.” Standing Cybersecurity Hunt Teams, with a focus on active defense, would expand on the capabilities of NATO’s current Cyber Rapid Reaction teams which are limited in numbers and operate reactively.

While the cybersecurity of infrastructure and government systems is a national responsibility, **a breach of cybersecurity** at the national level **can have collective consequences.** Standing Cybersecurity Hunt Teams can be a capability, as well as connective tissue, to identify and mitigate cyber threats across national boundaries and enhance NATO’s collective defense. Standing Cybersecurity Hunt Teams would be able to utilize information and experience gained from contesting Russian and Chinese cyber-attacks against one ally in the defense of others. A Standing Cybersecurity Hunt Team can also serve in a capacity-building role to help allied nations develop their own cyber capabilities, for example, in conjunction with the NATO Cooperative Cyber Defense Center of Excellence.

Third, **NATO should coordinate** a strategy of persistent engagement **to reduce Russian and Chinese activities to undercut the Alliance** in cyberspace. The concept of persistent engagement was developed by US Cyber Command, but the rationale likewise applies to NATO, deriving from the need to combat the continuous campaigns of cyberattacks coming from Russia and China. Persistent engagement involves tracking adversaries, understanding their goals, analyzing the tools used for attacks, and taking actions to degrade their capabilities to blunt ongoing, or prevent future, attacks. **The Alliance needs a persistent engagement cyber strategy as a key element of its deterrence and defense.**

Customary international law, including the law of countermeasures, pleas of necessity, and other cyber norms, provides the international legal basis for a strategy of persistent engagement. Because NATO Allies have already been attacked and are continuously being targeted by these adversaries, **offensive actions to counter** such activities **are justified**, as long as they are conducted proportionately. While persistent engagement arguably could increase instability in cyberspace, **Alliance inaction is far more dangerous.** **If Russia and China perceive no consequences to their malign actions** in cyberspace, **they will only continue and even intensify them.**

#### Cyber cohesion key to preventing future military attacks

Namias 22 – Dominic Namias is a legislative fellow at the US House of Representatives. “U.S. Warfare Within the Fifth Domain: Deterring Russian Cyber Aggression” Published 2022. <https://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=1267&context=hsgconference> //DG

NATO has been generally successful in implementing the private sector of their various nations into the cyber defense field and serves as an example of the private cybersecurity industry aiding the public sector. Through NCI Agency, the information technology, communications and cyber defense arm of NATO, billions of dollars have been invested in private companies from NATO countries to train and equip professionals in the public field to defend against attacks. This is an example of successful strategy that has also been used by the U.S. Department of Defense. These investments show a common strategy among NATO member states which has been extremely successful. **Through sharing strategies and information, the U.S. and NATO can learn from one another the best means** to deter cyber aggression.

Working with NATO Counterparts

NATO was founded in 1949 with the full intention to “safeguard the freedom, common heritage and civilization of their peoples, founded on the principles of democracy, individual liberty and the rule of law...to promote stability and well-being in the North Atlantic area.”23 The 12 founding countries have since grown to 30 nations all with the same goal of furthering security and prosperity in the North Atlantic region. According to NATO, the alliance was formed to meet three objectives: “[to deter] Soviet expansionism, [forbid] the revival of nationalist militarism in Europe through a strong North American presence on the continent and [encourage] European political integration.” 24 The expansion of NATO has driven the alliance closer to its main aggressor, Russia, with the addition of four former Warsaw Pact members (Czech Republic, Hungary, Poland and Romania) and three former-Soviet states (Estonia, Latvia and Lithuania). This has broadened NATO’s responsibilities and increased the threat from Russian interference in NATO activities.

NATO has focused heavily on cybersecurity since 2014 and as recently as January 2022 re-emphasized their commitment to security in the fifth domain: To keep pace with the rapidly changing threat landscape and maintain robust cyber defenses, NATO adopted an enhanced policy and action plan, which were endorsed by Allies at the Wales Summit in September 2014. An updated action plan was endorsed by Allies in February 2017. The 2014 policy established that cyber defense is part of the Alliance’s core task of collective defense, confirmed that international law applies in cyberspace, set out the further development of NATO’s and Allies’ capabilities, and intensified NATO’s cooperation with industry.25 NATO has recently alluded to a policy of physical military action against any cyberattacks on member states: Appearing at the Atlantic Council’s headquarters in Washington ahead of NATO’s summit in Brussels, Stoltenberg said NATO did not distinguish between cyber intrusions and other forms of attacks. He noted that cyber aggression could trigger a military response through “other means.” “In a way, it doesn’t matter whether it’s a kinetic attack or a cyberattack, we will assess as allies whether it meets the thresholds for triggering Article 5. It sends a message that we regard cyberattacks as seriously as any other attack.”26

This has yet to be implemented based solely on an aggression against a member state, but the 2021–2022 Russo-Ukrainian crisis can be traced back to Russian cyberaggression against the Ukrainian central government. The response by the United States and NATO allies is the correct approach to a cyberattack from within the Russian Federation. According to intel from the Ukrainian Government, hackers from within the Russian Federation shut down major government websites on January 14, 2022, “The websites of the country’s cabinet, seven ministries, the treasury, the National Emergency Service, and the state services website, where Ukrainians’ electronic passports and vaccination certificates are stored, were temporarily unavailable on Friday as a result of the hack.” 2

Russia coincided this aggressive action by building a significant military force on Ukraine’s eastern border, furthering the idea of simultaneous kinetic and cyber aggression. NATO and the U.S. responded accordingly by deploying troops to eastern Europe to defend the NATO alliance and Ukraine from invasion: “Denmark, Spain, France and the Netherlands were all planning or considering sending troops, planes or ships to eastern Europe, NATO said. Ukraine shares borders with four NATO countries: Poland, Slovakia, Hungary and Romania.”28

**The** 2021-2022 Russo-**Ukrainian crisis is revealing** of Russia’s ultimate strategy in two ways. Firstly, **it is now clear that a cyberattack will more than likely precede a kinetic attack**, especially when there is little resistance to that aggression. Secondly, there will be more aggressive action coming out of the Russian Federation and **NATO and the U.S. are not properly prepared on the cyber-defense front**. The evidence for the latter point has been addressed earlier with the examples of successful cyberattacks against the United States such as the Colonial Pipeline and JBS infrastructure attacks as well as the Notpetya attack.

NATO has been primarily concerned with building up cybersecurity in member states. The next step, led by the United States, is to go on the offensive and accurately identify the sources of these cyber aggressions. On several occasions, Russia has been able to hide behind the idea that the cyber-attackers are not state-affiliated and fiend responsibility of aggressions from within the Federation: Three successive U.S. administrations have failed to develop any form of doctrine to adequately address increasingly problematic cyberattacks from unattributable sources that plague U.S. businesses and can even endanger lives. Instead, the private sector has been left to deal with ever more destructive and dangerous ransomware attacks unassisted, and Russia continues to do nothing about cyberattacks originating from Russian territory.29

This is an epidemic that can be cured by shifting from a conservative policy regarding the cyberworld and towards a more proactive position. If the United States were able to identify actors with precision, further measures could be taken to prevent attacks on the U.S. infrastructure and on the private sector. In addition, being able to identify these actors would allow the United States and its allies to expose the perpetrators worldwide through media with solid evidence, damaging the perpetrator state’s reputation with the international community. Once the United States can present solid evidence against cyber criminals, **the United States and NATO allies can** **take conjoint actions** voluntarily against the perpetrator state/entity. This can be done **through intelligence sharing**, public statements of support for actions taken following an attack, and participation in the charges taken against the perpetrator state/entity. This strategy is reliant upon the ability of the United States and its allies to accurately identify perpetrators with a proactive joint campaign.

### I/L – NATO Key

#### Lack of NATO leadership in cybersecurity policy and legal norms leaves the Alliance stuck in a reactive limbo

Fidler 13 (David P. Fidler, Indiana University Maurer School of Law, “NATO, Cyber Def , Cyber Defense, and International Law,” Articles by Maurer Faculty, 2013, <https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2673&context=facpub>) - lh

In its sixty-four year history, NATO has been at the center of national security challenges faced by members of the Alliance, whether the challenge involved confronting Soviet military power in Europe, expanding its collective defense strategy in the postCold War period, responding to humanitarian crises, or participating in efforts to address international terrorism. NATO’s cyber defense strategy means that the Alliance has started to deal with yet another security threat, spurred in particular by the Estonia cyber crisis. However, despite the progress NATO has made with its operational capabilities through NCIRC and its decision-making processes on cyber defense issues, NATO is not, at present, at the center of cybersecurity thinking taking place within the policy circles in NATO members, especially the United States. The more NATO lags behind in cybersecurity policy and law, the more the Alliance will be stuck in a reactive mode—a situation that will reduce NATO’s ability to be a more constructive platform for cybersecurity both within the Alliance and between NATO and non-NATO countries. NATO could proactively play a more significant role in global cybersecurity but only if NATO members empower NATO to lead rather than just trail behind.

#### International cooperation key to responding to cyberthreats

Talihärm 13 (Anna-Maria Talihärm, Senior Analyst of the Legal and Policy Branch, NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), “Towards Cyberpeace: Managing Cyberwar Through International Cooperation” UN, vol. L, no. 2, August 2013, <https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation>) -lh

Malicious cyberactivities have been affecting individuals, private entities, government institutions and non-governmental organizations for years. We have witnessed large-scale cyber-incidents such as in Estonia in 2007, with numerous sophisticated targeted attacks, hacktivism and countless instances of identity theft and malware. Due to the unpredictable nature of cyberthreats, an incident that may appear in the beginning as an act of hacktivism or financially motivated cybercrime may rapidly escalate into something much more serious and reach the threshold of national security, even cyberwar.

Despite the lack of consensus on exactly what constitutes cyberwarfare or cyberterrorism, governments need to ensure that their infrastructure is well protected against different types of cyberthreats and that their legal and policy frameworks would allow to effectively prevent, deter, defend and mitigate possible cyberattacks. Not being able to agree on common definitions of central terms such as “cyberattack” and “cyberwar” should not prevent states from expressing the urgency of preparing their nations for possible cyberincidents.

INTERNATIONAL COOPERATION

The logic of international cooperation and collaboration lies on why, when, and how to collaborate, and generally takes place in order to follow one’s interests or to manage common aversions.1 In the context of cybersecurity, the need for international cooperation between states, international and regional organizations and other entities is emphasized by the borderless and increasingly sophisticated nature of cyberthreats. Principally, any actor, whether it is a country or a non-governmental organization, following its objectives in cybersecurity requires cooperation from a wide range of international partners. In fact, much of the international collaboration will occur outside specific national frameworks, emphasizing the Whole of System approach that stresses the need to take into account all relevant stakeholders.2

Thus, from a national perspective, advancements in cybersecurity depend to a large extent on the political will of different actors. Areas such as information and intelligence sharing and mutual assistance may become essential in responding to a cybercrisis, but the effectiveness of such cooperation depends greatly upon strategically aligned policy goals and bilateral and multilateral relations. In many domains, such as international criminal cooperation, there are several preconditions that need to be in place in the cooperating countries, such as substantive national law as well as procedural law and international agreements, before the dialogue on the possibility of any sort of international cooperation can grow into further discussions on the efficiency of such cooperation.

INTERNATIONAL ORGANIZATIONS ACTIVE IN CYBERSECURITY

National policies, international agreements as well as other initiatives addressing cybersecurity that are being proposed and launched by different international, regional and national actors may vary considerably in their scope, aim and success, but they all underline the international dimension of cyberspace.

For example, the United Nations First Committee has been actively examining the Developments in the Field of Information and Telecommunications in the Context of International Security for years. The African Union has published the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa. The European Union (EU) has recently published a Joint Communication on the Cyber Security Strategy of the European Union, which is the first attempt for a comprehensive EU policy document in this domain to reflect the common view on cybersecurity of all its 27 member states.

Even though in recent years the wider debate has intensified on the development of possible norms of behaviour or a set of confidence-building measures in the cybersecurity domain, it should not be forgotten that most of the pressing issues and challenges in areas related to cybersecurity have roots in the adoption and review of national legislation and the implementation of multilaterally agreed principles.

PRINCIPLE DEVELOPMENTS

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is a North Atlantic Treaty Organization (NATO) accredited international military organization that focuses on a range of aspects related to cybersecurity, such as education, analyses, consultation, lessons learned, research and development. Even though the Centre does not belong to the direct command line of NATO, its mission is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyberdefence.

Determined that international cooperation is key to the successful mitigation of cyberthreats worldwide, the Centre invests not only in broader collaboration with NATO and EU entities but, more specifically, focuses on improving practical cooperation within and among its sponsoring nations by hosting a real time network defence exercise known as Locked Shields. It also participates in many other similar simulations, thereby allowing the participants to put national coordination and cooperation frameworks to practise, and to learn and test the skills needed to fend off a real attack.

Regarding the legal and policy aspects of cybersecurity, NATO CCD COE has identified two main trends. Firstly, a growing number of countries are adopting national cybersecurity strategies and the majority of these documents confirm the role of cybersecurity as a national security priority. To further analyse such a development and the concept of national cybersecurity strategies, the Centre has conducted a comparative study called the National Cyber Security Framework Manual. The research asserts that a comprehensive cybersecurity strategy needs to take into account a number of national stakeholders with various responsibilities in ensuring national cybersecurity. The national stakeholders include critical infrastructure providers, law enforcement agencies, international organizations, computer emergency response teams and entities ensuring internal and external security. Importantly, instead of viewing cybersecurity as a combination of segregated areas or isolated stakeholders, the activities of different subdomains and areas of competence should be coordinated. Secondly, there are ongoing discussions about the applicability of international law to cyberactivities. Whereas it is widely accepted that cyberspace needs to be protected like air, sea and land, and is clearly defined by NATO Strategic Concept as a threat that can possibly reach a threshold setting threatening national and Euro-Atlantic prosperity, security and stability, there are only a few international agreements that would directly address behaviour in cyberspace.

Agreeing on a common stance even in matters regarding well-established norms of customary international law, such as the prohibition of the use of force codified in the United Nations Charter, Article 2(4), together with the two exceptions of self-defence and a resolution by the Security Council, in the context of their applicability to the cyberdomain remains a challenging task for the involved parties.

Therefore, amid the complex legal issues surrounding these debates, in 2009 NATO CCD COE invited an independent International Group of Experts to examine whether existing international law applies to issues regarding cybersecurity and, if so, to what extent. The result of this three-year project, the Tallinn Manual on the International Law Applicable to Cyber Warfare, focuses on the jus ad bellum, the international law governing the resort to force by states as an instrument of their national policy, and the jus in bello, the international law regulating the conduct of armed conflict. The experts taking part in the project concluded that, in principle, jus ad bellum and jus in bello do apply in the cyber context but this may be altered by state practice. This and other opinions expressed in the Tallinn Manual should not be considered as an official declaration of any state or organization, but rather as the interpretation of the group of individual international experts acting solely in their personal capacity. The Manual does not, however, address cyberactivities that occur below the threshold of a use of force, and for that purpose NATO CCD COE has launched a follow-on three-year project entitled Tallinn 2.0.

In order to prepare nations for possible cyberincidents and ensure a solid ground for international cooperation, both comprehensive national cybersecurity strategies and a common understanding on the applicability of the international law are required.

Even though it has been argued that multilateral treaties are the most practical vehicles for harmonizing national legal systems and aligning the interpretation of existing international law, discussions about moving towards such an agreement on a global level appear to be at a very early stage. Given the current normative ambiguity surrounding international law in the context of cybersecurity, international cooperation between different actors is deemed to be the cornerstone of effective responses to cyberthreats.

### I/L – AT A/C

#### No alt causes – NATO’s greatest threat is cyber & failure to create consensus on that is what turns into collapse

**Lonergan and Montgomery 22** -- Dr. Erica Lonergan is an assistant professor in the Army Cyber Institute at West Point and Rear Admiral Mark Montgomery is the senior director of the Center on Cyber and Technology Innovation. “PRESSING QUESTIONS: OFFENSIVE CYBER OPERATIONS AND NATO STRATEGY” Published January 25, 2022. <https://mwi.usma.edu/pressing-questions-offensive-cyber-operations-and-nato-strategy/> //DG

NATO’s shift to incorporating offensive cyber operations into existing strategy and policy has focused on integrating offensive effects into conventional military plans and operations in the context of a conflict. While **NATO’s** updated **strategy** is a positive development, its limited focus on conflict scenarios for employing cyber power **fails to accurately account for the cyber threat environment NATO faces**—particularly the mismatch between the alliance’s clear distinction between wartime and peacetime and the approach of adversaries like Russia, who adopt a competition-conflict continuum. Additionally, the focus on employing offensive cyber during a high-end conventional fight is also not consistent with how several NATO members are already engaged in gray zone offensive cyber operations.

**The primary threat to NATO allies** in the cyber domain **is** not **from** high-end, decisive cyberattacks. Instead, cyber threats more frequently and effectively manifest as gray zone tactics designed to have a corrosive effect without rising to the level of warfare. There are numerous examples of this type of threat. For instance, in July 2021, NATO publicly condemned **a range of malicious cyber behavior**, including the Microsoft Exchange hack (which NATO attributed to China) and ransomware attacks targeting critical infrastructure. **Russia has leveraged cyber and disinformation operations** to interfere in democratic elections in the United States in 2016, 2018, and 2020; France in 2017; and Germany in 2017 and 2021—to name just a few examples. Russia also conducted distributed denial-of-service cyberattacks against government websites in Montenegro during the lead-up to, and following, Montenegro’s ascension to NATO in 2017. And when NATO forces were positioned in the Baltics beginning in 2017 as part of NATO’s enhanced forward presence, two threat actors, GhostWriter and Secondary Infektion, conducted a range of disinformation campaigns.

Additionally, the reality is that several NATO members are already speaking publicly about offensive cyber operations below the level of warfare and their statements and actions have an effect on the entire alliance. In particular, **NATO member nations have not reached a political consensus about the role of offensive cyber operations**. In 2018, the US Department of Defense and US Cyber Command issued new strategy and policy documents that articulated a role for the military in conducting offensive cyber operations below the level of armed conflict outside of US-controlled cyberspace (part of the “defend forward” strategy), and there has been some reporting about US offensive cyber operations. For instance, in 2018 the United States disrupted the Russian-linked Internet Research Agency from interfering in the midterm elections. And, more recently, in December 2021 General Paul Nakasone, commander of US Cyber Command, publicly acknowledged that the military played a role in disrupting ransomware groups targeting critical infrastructure. The United States has also worked with other NATO allies, such as Estonia and Montenegro, to conduct “hunt forward” cyber operations on allied and partner networks to uncover and disrupt malicious cyber activity.

Other NATO allies have also been more transparent about offensive cyber operations. In 2020, the United Kingdom announced a significant investment in its National Cyber Force, its organizational arm for offensive cyber operations, and its 2022 National Cyber Strategy emphasized the role of offensive cyber operations. In November 2021, General Nakasone and the director of Government Communications Headquarters—the UK government’s principal signals intelligence agency—stated jointly that the two governments were collaborating to “impose consequences” in cyberspace to disrupt adversary operations. The Netherlands has also publicly alluded to conducting offensive cyber operations.

Next Steps: Addressing Challenges and Mitigating Risks

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

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

#### NATO is key to establishing global cybersecurity norms

Lété 21 -- Bruno Lété currently serves as a senior fellow at The German Marshall Fund of the United States. He focuses primarily on NATO, transatlantic defense cooperation, developments in Eastern Europe and the Black Sea region, and cybersecurity. “Policy Brief: The Paris Call and Activating Global Norms” Published March 2021. <https://www.gmfus.org/sites/default/files/Lete%2520-%2520Paris%2520Call_0.pdf> // DG

The United Nations is unique because it convenes the full spectrum of global views and interests. But there are other international organizations and smaller groupings of countries that can be engaged by the Paris Call community to indirectly influence the UN processes and to **advance the debate of norm creation and implementation**. These gather diverse key players, their structures are more flexible, they possess a credible level of expertise, they often have more experience working with non-state actors, and they carry enough weight to negotiate on an equal footing with big countries like China or at the UN level. Projects can be developed in smaller bodies and then more easily transferred to the UN. The EU, ASEAN, the Organization for Economic Co-operation and Development, or the Organization for Security and Co-operation in Europe are experienced in working with multiple stakeholders and are a good place to engage in policy experimentation and vetting. **NATO** could **offer a good platform to introduce** new **ideas around a transatlantic zone of cyber stability.**

The Paris Call community should also look at relevant geographic clusters. This would make it easier to identify local attitudes and policy goals, and to create projects of common interests. Initiatives could, for example**, feature regions with exemplary cyber behavior as a role model or connect cluster of countries with other clusters and assist them in implementing norms of responsible cyber behavior.** The **goal would be to build an ever-increasing number of geographic pockets of cyber stability.** A good example of this is how the Baltic states cooperate on cyber-hygiene initiatives in the public sector and exchange best practices. There have also been efforts between the EU and the United States to strengthen cooperation on the global norms debate, despite the U.S. government not having signed the Paris Call yet. In other words, to act globally the Paris Call also must think regionally.

## AT – Politics DA

### 2AC – PTX Thumper

\*\* also good card that oco’s = defensive intent

#### No DA’s – NATO already agreed to integrate OCO’s

Pomerleau 19 – Reporter for C4ISRNET, covering information warfare and cyberspace. (Mark Pomerleau; "NATO to integrate offensive cyber capabilities of individual members"; C4ISRNet; https://www.c4isrnet.com/international/2019/05/28/nato-to-integrate-offensive-cyber-capabilities-of-individual-members/; 5-28-2019, Accessed 6-24-2022)//ILake-AZ

A relative latecomer to the cyber game, NATO is beginning to “operationalize” cyber capabilities into its overall structure by integrating those tools of member nations, said the alliance’s secretary general.

“We are tackling increasingly complex cyberthreats faster and more efficiently. And we are more aware of the threats, more resilient to incidents,” Jens Stoltenberg said May 23 at the Cyber Defense Pledge Conference in London. “We also need to consider how we can deter attacks in cyberspace.”

Top NATO officials have long maintained that the 29-nation alliance is defensive in nature with a mission of deterrence, implying that the body itself doesn’t engage in offensive maneuvers, including in cyberspace.

As such, Stoltenberg noted that part of deterring cyberattacks is attribution.

“Cyber attackers must know that they will be exposed,” he said, citing a thwarted attempt by Russian intelligence operatives to hack the Organisation for the Prohibition of Chemical Weapons in the Hague in October.

Conversely, Stoltenberg said, NATO must be ready to use cyber capabilities to fight enemies.

NATO has walked a fine line as a defensive organization, relying on the individual capabilities of member states. As an example, Stoltenberg pointed to allies conducting cyber operations against the Islamic State group in Iraq and Syria.

“By using national cyber effects, or offensive cyber, they suppressed ISIS propaganda, degraded their ability to coordinate attacks and disrupted their recruitment of foreign fighters,” he said. “We have agreed to integrate national cyber capabilities or offensive cyber into alliance operations and missions. All of this has made NATO more effective in cyberspace.”

Several experts have said members states that are both willing and capable of offensive operations number about a half dozen. Without a NATO-owned offensive capability, officials have noted that contesting adversaries in cyberspace is no simple endeavor.

“This is true for the air, the land, the maritime domain, and it has to become true — I’m careful on that — for the cyber domain or cyberspace as a domain of operations,” he said at a November 2018 conference. “This is what really we have to find out, and I address this is a difficult part because NATO is defensive and is a defensive alliance.”

And adversaries must be wary that cyberattacks could engender responses in other domains, said Stoltenberg.

“For deterrence to have full effect, potential attackers must know that we are not limited to respond in cyberspace when we are attacked in cyberspace. We can and we will use the full range of capabilities at our disposal,” he said, reiterating that a cyberattack on a member state could trigger the famed Article 5, in which an attack on one member is considered an attack on all members.

For 70 years, NATO has kept our people safe in the physical world. Now NATO needs to do the same in the cyber world,” he added. “We have seen that now in cyberspace we had a remarkable increase in our capabilities to defend our networks to stand together, to integrate offensive cyber intermissions and operations, and we have done that over the last years.”

However, NATO is not responsible for defending individual member nations in cyberspace; members agreed in 2016 to boost their respective cyber defense capabilities.

But in July 2018, NATO created a Cyber Operations Center. It opened in August 2018 with a three-pronged mission:

Provide situational awareness in cyberspace.

Plan allied cyberspace operations.

Manage the execution of operations.

The center’s deputy director, U.S. Air Force Col. Don Lewis, wrote that it serves as the theater component for cyberspace similar to how geographic commands cover specific physical domains. The center executes operational-level and strategic missions to provide commanders with domain advice, planning support and capability integration.

Just as in the physical space, but in some cases more pertinent in the cyber domain, deconfliction of efforts is critical to ensure friendly forces aren’t interfering with each other and compromising the mission. The center seeks to play a part in that role.

“But still," he noted, "it’s a national responsibly, fielding and offensive effect[s].”

### 2AC – No Link [Covert]

#### NATO does legal coordination through secret MOUs

Andrés B. Muñoz Mosquera 16, Legal Advisor, Director, at NATO Supreme Headquarters Allied Power, Europe - Allied Command Operations, October 2016, “Memorandum Of Understanding (MOU): A Philosophical and Empirical Approach (Part II),” NATO Legal Gazette, Issue #37, p. 34-38

The NATO Legal Deskbook briefly characterises MOUs as follows: “The form of MOU is frequently used to record informal arrangements between States on matters which are inappropriate for inclusion in treaties or where the form is more convenient than a treaty (e.g. **for** **confidentiality**). They may be drawn up as a single document using non-treaty terms, signed on behalf of two or more governments, or consist of an exchange of notes or letters recording an understanding reached between two governments, or a government and an international organization. MOUs usually do not require ratification. However depending on the content and the agreement between the Parties on the nature of the document, MOUs can be subject of a certain level of domestic ratification…NATO, in general, concludes MOUs in numerous occasions. MOUs are a very flexible and adaptable instrument to record the will of entities with legal personality to achieve practical results that do not amount to treaty obligations.”

How are MOUs practiced? There are several ‘schools’ of practice that nations and international organisations have developed, with different references to this practice in the British-law influential area5, continental European states and the United States.6 Aust highlights that in all of these areas, MOUs are considered ‘agreements without legally-binding force’ and refers to the European Commission document PESC/SEC 899 of 9 August 1996 to support his argument. Aust also admits that in certain circumstances nonbinding becomes binding.7 However, practice shows that states have different approaches depending on their political approach to the topic or topics addressed in specific MOUs.8

At this point, it is relevant to note the process for creating MOUs at NATO, a ‘classic’ international organisation practicing intergovernmentalism. At NATO, during the decision making process, members may reaffirm their sovereignty9, several times, by supporting or opposing the existence of an MOU in their collective realm. One wonders if in the process of creating MOU organisations or simple MOU initiatives there is any other international organisation in the world that gives its members so many opportunities to express their ‘super-will’10 with respect to scope and purpose, as well as to the provisions of MOUs, which are intended to implement the obligations under the foundational treaty. These treaty obligations are updated by an established practice that operates through the decisions taken, in general per the practice of consensus, by its highest decision making bodies. It is necessary to note that this consensual commitment does not only have a collective nature, as consensus reflects ineludibly the individual commitment of each of the NATO members on any specific decision taken by the Council for creating a concept supported by an MOU. In the Council’s decision, states do not particularly address the non-binding status of the MOUs. In fact, the non-binding status discussion rarely happens before the MOU text negotiations start and, normally, ends at national level exclusively mandated by political approaches or national legislation. This acts as almost pro-forma language applied dependent on a states’ individual practice and perspective, irrespective of the actual points negotiated in the MOU.

Consequently, are MOUs non-binding documents by default? How valid is the written commitment of the participants? Could the ‘bindingness’ 11 created in a non-binding environment lead to legal effects? This battery of ‘tricky’ questions, partially addressed ut supra, takes us outward to square one and convinces us that the law of parsimony fed by anterior facts and posterior behaviour surrounding the life of an MOU has to be taken into account seriously when determining its legal effects.

In this regard, MOUs are chosen for cross-border relations because there has been a previous political commitment or the basic principles of framework treaties have been implemented. The form of negotiations does not vary from that of a treaty, and in general, although there is a tendency to use lax or soft wording vis-à-vis treaties, the treaty negotiation strategies are clearly displayed. MOU texts, contrary to popular belief, have little flexibility for review once agreed upon. As such, MOU drafters incorporate predictable ‘mobile’ elements through annexes to MOUs, which negotiators assume can be opened by lower level managers, though it always requires a ‘political’ mandate either directly or indirectly.12 MOU practice shows that it is not common to incorporate reservations (statements of interpretation). However, these have recently found their way into MOUs carrying heavy and long-term financial commitments within their provisions

Compared to treaties, MOUs have, in general, shorter internal coordination processes for approval, and **few states pass them through parliament or their commissions**. Moreover, since most MOUs have some financial clauses related to budget and taxes, many negotiators regularly announce that their parliaments or specialised commissions need to give their approval before the state in question can consider the text of the MOU agreed upon.

Another example of how MOUs trigger complicated internal coordination processes is seen in the Host Nation Support Arrangements13 negotiated with states not party to the North Atlantic Treaty and other NATO treaties. The fact of not counting on those treaties initiates a parallel process of negotiations for concluding treaties14 on status of forces and international military headquarters. These treaties commonly address an array of matters that range from entering and staying in foreign territory, taxes and customs, wearing uniforms, holding weapons, policing compounds, claim waivers, freedom of movement, concurrent jurisdiction, etc. In addition, another significant factor is that due to confidentiality, **MOUs are published only at the level of for official use only, as most of them are classified.**

We must also say that MOUs often serve multiple purposes and are drafted to create a **cooperation** framework. This may require establishing understandings via joint procedures, or creating a sophisticated network of structures and procedures that would require detaching states’ resources abroad, **which in turn increases their level of commitment** and, inextricably, their expectations vis-à-vis the other participants.

Finally, we cannot conclude this section without referring to MOUs as implanting rules. Cross-border relations have, since ancient history, required minimum sets of principles that, in accordance with Dworkin, have the nature of standards that carry more weight in form of precise rules.15 This reality has been documented, for more than five thousand years, and ‘[a]ll groups of nations in regular contact had in practice adopted certain rules defining the conduct which could usually be expected among their members.’16

The principle of good faith is linked to that of estoppel, which leads us to address briefly the consequence of conflicts within MOUs.17 Since MOUs enjoy ‘all’ of the elements and principles that treaties do, we may warily open the Pandora’s Box of state responsibility, which cannot be addressed in this article. But is it true that state responsibility applies for MOUs, and is there any legal effect? MOU participants reach a consensual engagement reflected in the MOU provisions, which obliges those participants to communicate unilateral acts that can have legal effects. If those acts, fruits of a consensual engagement, are committed contrary to good faith by any participant, they are considered unfriendly acts and will, in certain cases, **be void.** Therefore, they will be subject, at the least, to retorsion, which is nothing other than a non-amicable act of retaliation within the bounds of proportionality, and based on good faith, common sense, and reasonableness.18 But what about justice and MOUs?

#### NATO’s info security is air tight---secrets will never leak

Alasdair **Roberts 3**, University of Massachusetts Amherst - School of Public Policy, 5/15/3, “Entangling Alliances: NATO's Security Policy and the Entrenchment of State Secrecy,” <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1307692>, p. 350-355.

Penalties for unauthorized disclosure. The security policy adopted by the Council in March 1955 made clear that "disciplinary action" was to be taken "against any individual who is responsible for the compromise of NATO classified information."' 12 No comparable provision was included in earlier policies. However, a series of substantial leaks in 1952 and 1953 demonstrated the need for firmer rules, and resulted in increased pressure on member states to adopt criminal penalties for unauthorized release of NATO information.' 1

Frustration with leaks peaked after a meeting of the Council in April 1953.1 14 The main aim of the meeting was the resolution of the sensitive issue of how much each nation would contribute toward a £250 million defense infrastructure program. The New York Times published details of the proposed plan two weeks before the meeting.1 15 A week later, the Times, London's Daily Telegraph, and the Associated Press simultaneously published details of NATO's plans for production of fighter aircraft. Matters deteriorated during the meeting when Le Monde reproduced the agenda and provided a running summary of the talks, while the Times summarized American and British background reports on relations with the Soviet Union.' 16 Major press services transmitted the final communique hours before the NATO secretariat formally released it. Later, the Times excerpted a secret paper on Soviet-Chinese relations discussed at the meeting. ' ' 7

In May 1953, Secretary General Ismay told the Council that leaks such as these posed a "grave threat" to NATO's effectiveness. The NATO Council directed the Security Committee to study "the extent to which each member government could take legal action in respect of leakages of NATO classified information . .. [and] report to the Council as soon as possible with regard to any practical steps that could be taken to ensure that leakages of NATO classified information would not occur in future."'" 8

The Security Committee made a ten-month study of state secrets laws and reported to Council in March 1954. Only three countries-France, Italy, and Turkey-had clear criminal penalties for the unauthorized disclosure of NATO classified information. (In fact, France recently had modified its law to address this issue, perhaps in response to the leaks controversy.' 19) Many countries were found to have state secrets laws that were deficient or ambiguously worded. Two of these countries, Belgium and the Netherlands, reported that they were contemplating amendments to address problems with their state secrets laws. The Security Committee recommended that governments consider "suitable supplementary legislation" to ensure that **there would be criminal sanctions for leaking NATO information.'** 20 The Council endorsed the recommendation.' 2'

In August 1954, the Standing Group considered the problem of leaks. Its draft overhaul of the NATO security policy included a new section dedicated to the problem of "leakages of information to the press."' 2 2 It proposed that national security authorities should have the duty to immediately investigate leaks and take "disciplinary action" against leakers. The Standing Group later added another proposal, giving the NATO Security Bureau the authority to coordinate with national authorities on leak investigations. 12 3 Comparable rules are found in the final version of the policy adopted by the Council in March 1955.

The subject did not rest there. The chairman of the Security Committee, apparently dismayed by governments' response to the Committee's 1954 recommendation on reform of national laws, returned to the subject in a January 1956 meeting. "To make the position quite clear," the chairman said, governments were to answer five questions about their state secrets laws:

1) Is a NATO secret considered to be a "State secret"? (2) Can any person guilty of disclosing a "State secret" be prosecuted whether he be a member of the Government, an official or a private citizen? (3) Is the charge the same for a person who intentionally discloses a secret and for one who does so by negligence? (4) Can a person who discloses a "State secret" or a NATO secret be prosecuted in a country when the offence has been committed outside that country? (5) Can a country prosecute a foreigner who has disclosed a NATO secret on its territory? 124

Most countries answered that their national legislation provided adequate protection. Denmark responded that its law had been modified in April 1955 to address these issues, while Belgium said that statutory changes had been introduced in April 1956. The Greek government also reported that "necessary steps to revise legislation to cover all possible cases" were being taken.12

Ironically, in the United States, sanctions for unauthorized disclosure of classified information remained weak. Congress refused to enact criminal penalties except in narrowly defined circumstances, such as the disclosure of atomic information or deliberate disclosure to foreign agents. 1 26 The American representative to NATO conceded the inadequacy of these measures in his report to the Security Committee. 127 In March 1955, the Department of Justice told Congress that it had broader penalties under "active consideration." ' 28 A bipartisan commission on government security established in August 1955 recommended wider criminal sanctions, 1 29 but Congress again failed to act.

III. EVIDENCE OF CONTINUING INFLUENCE

The tension between domestic policies on access to information and intergovernmental obligations continues to be evident among NATO's older member states. One critical conflict concerns the treatment of information received from other governments, or intergovernmental organizations such as NATO, under domestic access-to-information laws. Adopted after the establishment of the NATO security regime, these laws have been drafted to accommodate the principle of originator control that is entrenched in NATO SOI policy. Governments have resisted calls for loosening this rule in national access-to-information laws, but have rarely acknowledged that national policy is constrained by intergovernmental commitments. Consequently, many domestic policy actors continue under the misapprehension that the content of national policy can be decided in national fora.

Canada. Debate over Canada's Access to Information Act (ATIA) illustrates the problem. The law obliges the Canadian government to deny any request for access to information provided in confidence by other states or international organizations of states unless the originator consents to its release. ' 30 In 1987, a parliamentary committee recommended that the law be amended to give the government discretion to release such information when disclosure seemed unlikely to cause harm. 131 Canada's Information Commissioner later gave qualified support to the proposal. 132 The Canadian government has consistently resisted these proposals. In 1987, it argued that weakening the originator control rule would impair "[tihe willingness of other governments to continue to share their information." ' 33 More recently, it has said that any reform would "set Canada apart from its key allies."13 4 This may be an indirect way of making clear the fundamental problem: that reform of this part of the ATIA would create a conflict between national law and Canada's obligations under the North Atlantic Treaty. Canada cannot explicitly acknowledge the potential conflict, because this would constitute a non-consensual disclosure of the substance of NATO's security policy. As a result, many Canadians continue to believe that reform is a matter that can be settled on the merits by domestic actors.

United Kingdom. The same misapprehension may prevail in other jurisdictions. In 1999, the British government was criticized for incorporating the originator control rule in its draft Freedom of Information Act. 135 The Campaign for Freedom of Information, a non-governmental organization, described this as an "indiscriminate" exemption that would allow the withholding of "harmless information." 13 6 Parliamentarians attempted to have the provision amended, but the government opposed these proposals on the grounds that they would violate a universally recognized norm of confidentiality. 137 It failed to explain that the government was constrained by more than convention: such an amendment would create a conflict between statutory and intergovernmental obligations. Similar complaints were made against a comparable provision in the new Scottish Freedom of Information Act.' 38 However, the Scottish government was explicitly constrained by the agreement governing the delegation of power to Scotland from the United Kingdom, which required Scotland to respect the terms of C-M(55)15(Final). 13

United States. In the United States, debate about the degree of protection to be given to information provided by foreign governments was stirred by the 1998 case of Weatherhead v. United States. 1 40 At the center of that case was the question of whether the judiciary should be permitted to consider the reasonableness of the U.S. government's decision to withhold a communication from the British government. Advocates for transparency argued in favor of the court's power to intervene, saying that it was indefensible in an open society to support a policy of absolute secrecy for inter-governmental communications, and that foreign governments could not reasonably expect total secrecy. 141

The case did not involve NATO communications, however, the transparency advocates' case was probably overstated. As the NATO policy shows, there are clearly domains where other governments do have a reasonable expectation of complete secrecy, based on the existence of an SO agreement. Furthermore, the capacity of the judiciary to intervene and impose the right balance on questions of disclosure is exaggerated. **The effect of NATO's SOI policy is to deny domestic actors,** including the courts, **the opportunity to make their own decisions about the disclosure of information within a certain policy domain. 14 2**

#### Secrecy solves the politics link

Ashley S. **Deeks 17**, Associate Professor, University of Virginia Law School, “A (QUALIFIED) DEFENSE OF SECRET AGREEMENTS,” Arizona State Law Journal, <https://arizonastatelawjournal.org/wp-content/uploads/2017/09/Deeks_Pub.pdf>, p. 725-727.

B. U.S. Political Arrangements

Just as states conclude politically binding (but legally non-binding) commitments in the public context that are intended to set parameters for their interactions, so too do **states conclude politically binding commitments in secret**. Further, there is reason to think that states adhere to these politically binding secret commitments with some regularity.

1. Secret Political Arrangements in U.S. Law

Section A identified a group of agreements that meet the definition of “treaty” found in the VCLT. But there are almost certainly many more secret arrangements that states do not intend to be governed by international law.35 In common parlance, these are political arrangements that happen to be secret. Some of these arrangements, which set out rules or modes of operation to be followed in one or more interactions between or among states, are surprisingly detailed. **A paradigmatic example would be a secret memorandum of understanding (MOU) between the U.S. Defense Department and a foreign military agency to guide specific types of intelligence interactions.**36 Other examples include arrangements between the CIA and its foreign counterparts and oral or tacit arrangements between the United States and foreign states, the legal status of which may be ambiguous. Pakistan’s reported consent to the U.S. use of armed drones to target individual members of al Qaeda in the Federally Administered Tribal Areas may reflect such a secret tacit arrangement.37 Some of these secret arrangements explicitly state that the parties do not intend them to create legally binding obligations.38

Compared to secret agreements (at least those to which the United States is a party), secret arrangements often are seen and approved by fewer people because **the Executive has no statutory obligation to transmit them to Congress.**39 The Case Act establishes a mechanism by which the Department of State (DOS) should be informed of these arrangements, so that the DOS can determine whether the arrangement is or is not an international agreement.40 However, it is not clear that each agency actually shares every one of its arrangements with the DOS. Some arrangements may be highly classified, which might make the initiating agency reluctant to share the arrangement’s contents. Alternatively, agencies may have worked out a modus vivendi with the DOS, whereby the DOS determines that certain categories of arrangements do not represent international agreements and thus effectively blesses another agency’s conclusion of such arrangements without DOS involvement.

The fact that only a limited number of people and a limited category of people are aware of these arrangements means several things. First, the arrangements constitute what Professor David Pozen has referred to as “deep secrets.”41 That is, these arrangements are often “unknown unknowns,” where the **public is generally unaware that the arrangements even exist**.42 (In contrast, an agreement is a shallow secret when the public knows that a particular secret agreement exists, but does not know the content of the agreement.) Less is known about these arrangements because **there are fewer players in a position within either government to leak them to the press or the public.** Second, the arrangements almost surely contain narrower national undertakings than do secret agreements (of which Congress and the DOS, as well as the originating agency, at a minimum, are aware). If only a single agency—or a limited set of actors within an agency—knows of the arrangement, its implementation by definition cannot require the involvement of large numbers of government officials.

Compared to secret agreements, it is even more difficult to estimate the number of secret arrangements between the United States and other states. This is because many of them are negotiated by intelligence agencies, which tend to be the best secret-keepers within governments. Jeffrey Richelson and Desmond Ball assert that over 1,000 intelligence arrangements exist among the five states that are parties to the Five Eyes agreement (the United States, United Kingdom, Canada, Australia, and New Zealand).43 Richelson describes some of them, including arrangements regarding defense intelligence analysis,44 ocean surveillance,45 and satellite imagery exchanges.46 Secret arrangements also exist between various U.S. and Israeli intelligence agencies.47 The U.S. CIA reportedly has established connections with more than 400 foreign agencies, which almost certainly entails concluding secret arrangements with some of those agencies.48 Likewise, the CIA’s Canadian equivalent has more than 250 intelligence-sharing arrangements with foreign intelligence entities.49 These arrangements may take the form of memoranda of understanding or even oral agreements between intelligence officials.50 Defense agencies also seem to conclude a wide variety of secret cooperative arrangements.51

### 2AC – No Link [Fopo]

#### Foreign policy doesn’t matter on the political stage

Dr. James M. **Lindsay 20**, Senior Vice President, Director of Studies, and Maurice R. Greenberg Chair at the Council on Foreign Relations, MA, MPhil, and PhD from Yale University, AB in Economics and Political Science from the University of Michigan, “Campaign Foreign Policy Roundup: Foreign Policy Is AWOL”, Council on Foreign Relations, 9/11/2020, <https://www.cfr.org/blog/campaign-foreign-policy-roundup-foreign-policy-awol>

Today on the nineteenth anniversary of September 11 it is **notable how little of the 2020 presidential campaign has been about foreign policy.** It’s not just terrorism that has receded from the headlines. The same could be said about China, Russia, Iran, and a whole host of other issues.

To an extent, the fact that foreign policy has been AWOL on the campaign trail isn’t surprising. Domestic issues typically dominate presidential campaigns, and COVID-19 is perhaps the mother of all domestic issues. It has upended the economy, disrupted daily life, and exacerbated existing racial and social inequalities. Even so, it was only a few months ago that some experts were speculating that COVID-19 would catapult U.S. policy toward China to the forefront of the campaign and give Donald Trump a cudgel with which to beat Joe Biden. So far that hasn’t happened.

This state of affairs seems to fit the public mood. A Pew survey of registered voters conducted this summer found that 57 percent of registered voters said that foreign policy was “very important” to them when voting. That sounds like an impressive figure, but 79 percent of respondents flagged the economy as “very important” and 68 percent flagged health care. Voters accord even less importance to specific foreign policy issues. Pew reported that just 42 percent of respondents said climate change was important to their vote, and it didn’t even bother to ask about terrorism.

Events could still elevate foreign policy in importance. There is no shortage of simmering crises that could suddenly remind Americans of their stake in what happens abroad. But for now, as unusual as 2020 has been, it is shaping up as a pretty traditional election year in at least one respect.

### !! - AT Tech Leadership

#### Impact Turn: Antitrust Legislation hurts U.S. Tech Leadership, empirics prove

Robert D. **Atkinson 21**,Mr. Atkinson is president of the Information Technology and Innovation Foundation, Ph.D. in city and regional planning from the University of North Carolina Chapel Hill, masters in urban and regional planning from the University of Oregon, Robert D. Atkinson 21,“Opinion | Antitrust Can Hurt U.S. Competitiveness,” Wall Street Journal, 07/05/2021, www.wsj.com, <https://www.wsj.com/articles/antitrust-can-hurt-u-s-competitiveness-11625520340>, accessed 6/24/2022.

When it comes to technology and the economy, the U.S. is grappling with two contradictory goals: competing with China in advanced technology industries and ramping up antitrust enforcement against leading U.S. tech companies.

Antimonopoly advocates argue that we can have our cake and eat it too. Go ahead and break up big tech, they say; we can still compete with China. But there is a long history of U.S. antitrust actions against technology companies, and the results suggest regulators should exercise caution.

Consider the case of Western Electric, AT&T’s equipment subsidiary. By the early 1920s, it had factories in Austria, Belgium, Canada, China, Germany, France, Italy, Japan, the Netherlands, Russia and the U.K. But because AT&T relied on it exclusively for equipment, in 1925 the Justice Department threatened AT&T with breakup unless it divested Western Electric’s foreign assets, creating International Telephone & Telegraph and ultimately giving birth to robust foreign-owned competitors.

Antitrust regulators also pressured AT&T’s Bell Labs in the early 1950s to license its newly invented transistor technology. That spurred innovation because it helped emerging companies such as Texas Instruments and Fairchild. But because of government pressure, AT&T also licensed its technology, almost for free, to foreign companies. This eventually enabled Sony to take global leadership from the U.S. in consumer electronics, and it gave a major leg up to Europe’s Ericsson and Siemens.

The U.S. also used to be the global leader in television technology thanks to the Radio Corp. of America, the pathbreaker in color television. But in the 1950s the Justice Department required RCA to let other U.S. companies use its patents at no charge. RCA had long relied on licensing revenue, so it started making money where it could—in Japan. “RCA licenses made Japanese color television possible,” technology historian James Abegglen has written.

In 1972, the Federal Trade Commission brought a similar antitrust suit against Xerox, the world’s then-leading producer of copier technology thanks in part to its Silicon Valley-based innovation incubator Xerox PARC. Evidently unimpressed, the head of the FTC’s Bureau of Competition F.M. Scherer said he would be “dissatisfied if Xerox’s market share isn’t significantly diminished in several years.” To that end, the FTC forced Xerox to give up its blueprints and other discoveries, allowing an estimated 1,700 patents to make their way to Xerox competitors. Sure enough, Xerox lost half its market share—mostly to Japanese firms such as Canon, Toshiba and Sharp. Xerox’s only viable path to survival was to strengthen its alliance with Fuji, creating a new giant, Fuji Xerox.

Two years later in 1974, the Justice Department targeted AT&T again, forcing it to break up over the objections of Commerce Secretary Malcolm Baldridge that the suit jeopardized America’s leadership position. This was the death knell for Bell Labs, arguably the most innovative organization that has ever existed.

None of this is to say that antitrust authorities should be passive or turn a blind eye to anticompetitive behavior. But they should recognize that firms’ size can be an important factor in their ability to innovate. Rather than rely on market share as the alarm bell that signals the need for antitrust enforcement, regulators should focus more on firms’ conduct, and they should look first to behavioral remedies, not structural ones. Antitrust analysis should also consider that tech companies compete globally, not nationally, so cutting them down to size usually has significant economic consequences.

The Federal Communications Commission has provided a model for the behavioral approach by conducting a series of inquiries starting in 1970 to investigate the convergence of telephone and computing services and establish rules enabling competition among established and upstart players across sectors that are increasingly intertwined. U.S. courts also provided a model in judgments against Microsoft, which compelled it to let other companies more easily integrate their software into Windows.

As policy makers now consider competition issues related to today’s large technology firms, they would be well advised to learn from this history. With Chinese internet and tech companies waiting in the wings, aggressive antitrust actions against U.S. leaders run the risk of giving a new generation of foreign rivals the boost they need to dominate global markets, just as Japanese and European firms have benefited in the past.

### !! – AT Economy

#### Antitrust law restricts competition and the growth of the economy

Clyde Wayne **Crews &** Ryan **Young 19,** Clyde Wane Crews is vice president for policy and a senior fellow at the CEI, M.B.A. from William and Mary, B.S. from Lander College; Ryan Young is a senior fellow at the CEI, M.A. in Economics from George Mason University, B.A. in History from Lawrence University, “The Case against Antitrust Law”, Competitive Enterprise Institute, 4/16/2019, <https://cei.org/studies/the-case-against-antitrust-law/>, Accessed 24 June 22.

Antitrust regulation began as a populist reaction against big business and industrial concentration. Yet, it has proven ineffective at countering the perceive threat of bigness in business, while causing considerable harm to consumers, competition, and innovation. Moreover, many antitrust policies are based on faulty arguments that bear little relation to how real-world markets work. And throughout its history, U.S. antitrust law has created considerable uncertainty for businesses, as federal antitrust enforcers have tried different regulatory approaches over the last 130 years.

The “rule of reason” standard, which had no set criteria, became the standard for enforcing actions from fines to jail terms to firm breakups. During the New Deal, government policy turned in the opposite direction and actively encouraged cartel behavior. After a postwar change of heart, antitrust enforcement reached its peak in the 1950s and early 1960s. Around this time, economists’ arguments slowly earned mainstream acceptance in the legal profession. By the 1980s, a Chicago-style consumer welfare had become the dominant enforcement standard, and has remained so up to the present day. However, the combination of a populist presidential administration with a growing Neo-Brandeisian antitrust movement on the progressive side threaten to revert antitrust policy to something closer to an arbitrary rule of reason standard, which creates the potential for a sharp upswing in enforcement actions against large or politically disfavored firms.

While the Chicago school and the Neo-Brandeisians prefer different levels of antitrust enforcement, both believe that antitrust regulation is an effective tool for managing competitive market processes. In this, both are in error, for a number of reasons.

First, competition is a spectrum, not an on/off switch. That makes it difficult to set predictable standards that companies can work to avoid violating and plan around.

Second, regulators are prone to fall for the relevant market fallacy, in which a company appears to dominate a narrowly defined market but has little power in the larger market in which it actually competes.

Third, antitrust enforcement standards are so broad that they are useless as a guide to permissible behavior. Allowable behavior changes with the political winds. Cases, especially major ones, are sometimes prosecuted for publicity rather than merit.

Fourth, antitrust regulation creates rent-seeking opportunities for companies seeking favors from government to harm competitors. As a result, antitrust regulation, as actually practiced, has done far more to stifle competition than to protect it or promote it.

Finally, antitrust regulation takes a short-term approach to a long-term competitive process. The IBM case was in play for a dozen years before the government dropped the case. By that time, the technology at the heart of the case had changed and IBM’s competitive position had declined. A case against one of the FAANG companies would likely have similar competitive relevance by the time a major trial would be decided.

As noted, antitrust regulation harms competition, consumers, and innovation, and therefore should be repealed. Congress should repeal the Sherman Act of 1890, the Clayton Act of 1914, and the Federal Trade Commission Act of 1914, as amended, including the Celler-Kefauver Act of 1950 and the Hart-Scott-Rodino Act of 1976. A market-based approach to competition would enable more powerful market regulation to replace flawed government regulation. This would reduce regulatory uncertainty and its chilling effects on innovation, reduce rent-seeking, and do away with the need for intellectual rabbit holes such as defining relevant markets or permissible levels of firm size or market share.

Aggressive antitrust enforcement can create considerable economic uncertainty, which can have a chilling effect on long term investment and innovation in both products and in business practices that could benefit consumers. Consumers and competition would greatly benefit from the repeal of antitrust regulations regarding restraint of trade and monopolization, horizontal and vertical mergers, collusion such as price fixing and market division, predatory pricing, price discrimination, minimum resale prices, exclusive dealing, tying and bundling, strategic predatory behavior, and technological lock-in. As the economy becomes more high-tech, specialized, and global, antitrust policies formed in the smokestack era are becoming progressively less relevant.

## AT – T-Cybersecurity

### 2AC – OCOs = Defense

#### OCOs fall under “cyber defense” which is distinct from “cybersecurity”

Tammet 21 (Tanel Tammet, “Autonomous Cyber Capabilities under International Law,” NATO CCDCOE, ch 3, 2021, <https://ccdcoe.org/uploads/2021/05/Autonomous-Cyber-Capabilities-under-International-Law.pdf>) -lh

Since ‘cyber security’ and ‘cyber defence’ cover a wide range of goals and activities, their meanings are—inevitably—somewhat vague and mostly overlapping. However, by ‘cyber defence’ people typically mean a more pro-active stance than is conveyed by ‘cyber security’. For example, cyber intelligence and reconnaissance are often described as ‘cyber defence’ activities.

## misc

### IHL stuff—not complete

#### NATO resilience is the top priority—NATO in unique position to apply IHL to cybersecurity

Hughes 09 (Dr Rex Hughes, “Towards a Global Regime for Cyber Warfare,” The Virtual Battlefield: Perspectives on Cyber Warfare, 2009, <https://books.google.com/books?hl=en&lr=&id=BKDbN5eUhV0C&oi=fnd&pg=PA106&dq=us+leadership+on+ihl+and+cyber+norms&ots=v4H3plPodS&sig=WK49Llw6YJFyl3FhxQxlT3yqH4E#v=onepage&q&f=false>) -lh

Does cyber warfare fall under the international humanitarian law (IHL)? Jeffrey Kelsey holds that IHL ‘should evolve to encourage the use of cyber warfare in some situations and provide states better guidance in the conduct of these attacks’ [16]. He argues that for a decade or more the ‘potential threat and opportunity of cyber warfare’ have confronted military planners while the ‘international community has yet to reach consensus on the application of IHL’. This lack of consensus may be due to a variety of reasons, from holding that the ’current IHL framework can be applied to cyber warfare by analogy’ to the realization that vast growth and fluidity of technology would make potential international agreements obsolete [16]. Kelsey further maintains that ‘IHL applies to cyber warfare by analogy but contends that IHL must evolve to accommodate and, in some cases even encourage cyber warfare over conventional methods’ [16].

The movement in a cyber attack across a neutral state becomes more than a ‘mere communication signal’, for cyber weapons can cause damage to states as have more conventional weapons. A weapon the ‘size of a electron’ could be a violation of the territory of a neutral state according to the Hague Convention that ‘forbids the movement of weapons’ across a neutral state which risks being drawn into a wider cyber conflict when its Internet nodes are engaged by a belligerent [16]. What obligations would a neutral state have as a conduit for cyber attack and mischief? Kelsey argues against establishing new treaties and in favour of states and their military commanders to follow established legal principles in cyber combat [16]. The question remains: What standards should emerge for a cyber security regime under established peace and war legal principles? Since cyber warfare is still in its infancy, some would argue that regulating it is a difficult if not an impossible challenge. However, the so called catastrophic cyber attack is to be avoided, it would be foolish and impractical not to establish some type of international rules of the game as deterrence.

3. Towards a 21st Century Global Cyber Regime Thus far, the diplomatic community has had little to say about the governance of cyber warfare. Two exceptions of major importance include former diplomats with knowledge of ICT have in recent months discussed with this author the major international relations quandaries from cyber threats and attacks plus their own concerns about diplomatic-level solutions. These former envoys are retired senior US Amb. Thomas Pickering who served over four decades in major posting for the US Dept of State, and Amb. David Gross, U.S. Coordinator for International Communications and Information Policy 2001-08. The latter observes that diplomatic silence may be attributed largely to a generational gap and a lack of technical understanding by policy makers since the Internet and associated networks are fairly recent developments; therefore, cyber security concepts in international affairs are still a nascent on the part of the diplomatic community (Gross to the author: April 2009). With wide-ranging diplomatic and corporate experience, Amb. Pickering sees an even larger problem in that forming an international treaty involves major, prolonged steps and major questions: What is the problem to be solved? How will the problem evolve in the future? (Pickering to the author: July 2009). Since cyber warfare is being conducted and developed during a period of wide interstate trade and general economic accord or agreement, there is an opportunity to design a governing framework before an actual global catastrophic attack takes place. Today the questions remains: Can governments be motivated to take action now before it is too late?

Special regimes have been formed for far-ranging interests or activities, such as treaties governing the Arctic, Antarctic, canals, international rivers, and outer space. While somewhat vague or undetermined there appears to be a consensus that outer space begins where airspace ends [17]. Examples of the treaties governing outer space include those governing the International Space Station (1998), Registration of Objects Launched into Outer Space (1975), INTELSAT or International Telecommunications Satellite Organization (1986), INMARSAT or International Maritime Satellite Organization (1976), as well as the ITU or International Telecommunications Union (1932; 1947 as UN agency) [17]. You may ask, ‘Where does cyberspace begin?’ It would appear that cyberspace begins with the keystroke to log on to a cyber network, whether from a mega terminal, a PC, a game console, or a mobile telephone. Eventually, the ultimate venue for cyber warfare governance would be The Hague as the home of the world’s first Peace Conference and for over a century as the international centre of justice and arbitration, as well as warfare governance. The Hague hosts several international organisations, including the UN International Court of Justice, the Permanent Court of Arbitration, the NATO Consultation, Command and Control Agency (NC3A). As cyber warfare moves to the forefront of more government agendas, more questions arise as to how the Law of Armed Conflict and the Geneva Convention apply to cyberspace. Responses are likely to range on both sides of the fault line: those who see cyber warfare as fitting neatly under existing LOAC (as well as under the UN charter), and on the other side, those who see the need for an entirely new set of international laws and treaties to govern cyber warfare.

A Way Forward While it is unlikely that these two countervailing diplomatic/legal views will be reconciled anytime soon, the time is now to begin having this debate in a more serious, focused manner. Again, because cyber warfare is a complex and dynamic issue, these debates will need to be hosted in many different venues and viewed from many different perspectives. NATO is already playing an important role in this debate by hosting conferences such as this June 2009 Tallinn gathering bringing together the relevant players from both member states and global partners. For the foreseeable future, this NATO Center of Excellence can play a critical role in bringing together the best experts both to analyze and to debate the problems from a number of unique cultural and disciplinary perspectives.

As the world’s premiere military alliance, NATO is positioned to play a major role by facilitating significant interstate dialogue between civilian and military planners. Each year NATO hosts various fora where such engagements take place. The NATO Global Partnership Program provides a mechanism to reach out to other countries. NATO could also explore reaching out to other peace and security alliances, such as ASEAN Regional Forum (ARF) and the Shanghai Cooperation Organization (SCO), for the purpose of exploring confidence-building measures with that global hemisphere. Although presently cyber warfare/defense is largely an ungoverned affair, the UN leadership has already acknowledged the severity of the problem and the need for governance. UN secretary-general Ban Ki-moon earlier this year announced that the UN Advisory Board on Disarmament Matters is to include cyber weapons in its arms list [18]. In his prepared February remarks to this Advisory Board the Sec-Gen stated: This year you will be considering cyber warfare and its impact on international security. As you know, there have been many widely reported breaches of information systems in recent years. With both the public and private sectors growing increasingly dependent on electronic information, your work in this area is very timely. It will also complement the efforts of the panel of governmental experts that will be addressing information security later this year [19].

The UN’s International Telecommunications Union last year concluded its agreement with the International Multilateral Partnership Against Cyber-Terrorism (IMPACT) to conduct the ITU Global Cybersecurity Agenda (GCA) with headquarters in Cyberjaya, Kuala Lumpur. The GCA seeks international cooperation for governments, international law enforcement authorities, the private sector, international organisations, and civil society for the purpose of a secure cyberspace. Through five areas the GCA if focused on strengthening the legal framework, technical measures, organizational structure, capacity building, and international cooperation. [20] At its Cyberjaya headquarters inauguration the ITU-GCA was billed as ‘public-private initiative’ and a ‘framework for cooperation aimed at finding strategic solutions to boost confidence and security’ in a networked world [21].

Relevant committees beyond the UN should also begin to debate a proper a framework for cyber warfare while other international fora can and should play a role. Significant organisations such as the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Society (ISOC) are positioned to use their technical legitimacy and their soft power to press forward with best practices for member states to follow in securing their own sovereign cyberspace. World Trade Organization (WTO) signatories should develop an agreement for pledges from nations not to promote or solicit mercenaries, or attack a member state’s trade infrastructure. On the military side, the national leading military services should be encouraged to act with transparency where possible so as not to launch initiatives that unduly contribute to unnecessary cyber arms race between states.

One of the most difficult governance areas to reconcile will be in the area of police vs. military involvement in cyber security/defence. As the US-led global war on terror has shown, there is no clear line of authority when defending against threats where state involvement is murky at best. Due to the anonymous and secretive nature of cyber warfare, state involvement is often tricky for producing fool-proof forensics that can prove state involvement. While each country will ultimately need to sort through this problem in accordance to its national laws and constitutions, more global debate will be needed to clarify these issues.

Participants in Tallinn are witnesses to the positive leadership role assumed by Estonia and leading to the NATO CCD COE here at the scene of the first acknowledged, major interstate cyber conflict. There is potential for a cyber treaty to emerge should the North Atlantic Council embrace thoroughly the cyber warfare issue and engage the NATO Consultation, Control and Command Agency (NC3A) and the NATO Military Authorities (NMA). The Tallinn cyber convention questions and discussions are a start, but a protocol or treaty governing the conduct of cyber warfare needs serious consideration.

4. Conclusion While cyber warfare is not an entirely new area of modern warfare (at least as viewed within an Internet world), its current evolution poses many challenges to international peace and stability. The increasing quantity and quality of online attacks threaten many parts of civil society that depend on reliable networks and information systems. Growing evidence of state-sponsored cyber attacks is especially alarming and could spark a serious arms race in cyberspace. Understandably, a number of countries have announced plans for full spectrum military cyber commands. As history has demonstrated, while international law cannot stop states from going to war with one another, it can go a long ways towards regulating their conduct should hostilities boil over into actual war. Some may argue that because cyber warfare is still in its formative stages, it is premature to begin work on a global regime to regulate it. However, it can also be logically argued that absence of some rules of the game, states will not feel constrained to develop and deploy cyber weaponry if the consequences are not understood by both military and civilian planners. While it is difficult to estimate the true potential for a catastrophic attack to spill over to kinetic warfare between states, the notion that the threat exists at all is cause enough to begin constructing a regime or legal framework through which to conduct cyber warfare.

History presents another lesson in that even with the best intentions and resources, a global cyber security regime will not transpire in short order. It will take many years to form an effective international consensus that might translate into a revision of the Law of Armed Conflict as spelled out by the Geneva Conventions. The operative concept is regime. And, the time to establish a global cyber security regime is now. As a proper follow-up to the innovative inaugural Tallinn CCD COE conference of 2009, NATO can and should play an important role by bringing together in short order the relevant stakeholders to outline a viable cyber security regime. Lt. Col. Walker quoted in the introductory epigraph to this paper, eight years ago properly challenge the legal community, and this writer has chosen to extend his challenges to the wider global policy community.

## neg

### !! – AT Cyber

#### The impact is empirically denied---NATO is cyber-attacked daily.

University of Exeter 20. “Should NATO Adopt a Joint Offensive Cyber Capability?” September 2020. <https://socialsciences.exeter.ac.uk/media/universityofexeter/strategyandsecurityinstitute/pdfs/mstrat/James_Prideaux.pdf>. //AN

But despite these measures, NATO’s members have continued to face increasing cyberattacks since 2016, primarily from state actors. In 2017, Russia launched the huge NotPetya attack against Ukraine, wiping data from the computers of banks, energy firms, senior government officials and an airport.34 Although Ukraine is not part of the Alliance, the virus still affected member states because it spread to the rest of the world. It crippled the Danish shipping company Maersk and the American pharmaceutical giant Merck, causing an estimated $10 billion in damages.35 NATO itself faces hundreds of significant hacking attempts every month, principally from Russia, North Korea and China.36