# Negative

## Topicality---“Cybersecurity”

### OFF

#### Interpretation---Cybersecurity is defensive tactics that prevent and isolate attacks.

Ricoh No Date. Multinational imaging and electronics company. "What is cybersecurity?". https://www.ricoh-usa.com/en/insights/articles/an-intro-to-cybersecurity

Cybersecurity defined

Cybersecurity is the act of implementing sophisticated layers of network defense and firewalls to protect critical systems and sensitive information against threats from digital attacks.

The reality is that the types and severity of cybercrime are constantly evolving and multiplying.

* There are malware attacks such as viruses that attempt to destroy data.
* Ransomware is a particularly nasty type that locks down systems and threatens to erase data unless a ransom is paid.
* Phishing scams try to trick unsuspecting end users into giving up sensitive personal information such as social security (SSI) and credit card numbers to sell on the dark web.
* There are Distributed denial-of-service (DDoS) attacks that overwhelm a website with traffic.
* Man-in-the-Middle attacks involve hackers trying to intercept messages between two parties to steal company data.
* And not all threats are external. Current or former employees with a grudge and intimate network knowledge can wreak havoc on a business from behind the firewall. Companies must be on the lookout for cybercrime from all directions.

Cybersecurity solutions, therefore, are applications, measures, and devices that constantly monitor network traffic for suspicious activity. Upon detecting a threat, it isolates and quarantines affected files and devices, and immediately alerts IT staff as to the exact location and proper response to the breach, limiting its impact and assisting with recovery.

#### Violation---only deterrence by denial is cybersecurity. Punishment is distinct.

Stefan Soesanto and Max Smeets 21. The Risk and Resilience Team, Center for Security Studies (CSS). “Cyber Deterrence: The Past, Present, and Future.” In: Osinga, F., Sweijs, T. (eds) NL ARMS Netherlands Annual Review of Military Studies 2020. NL ARMS. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-419-8\_20

First, deterrence by denial is essentially synonymous to cybersecurity. At its core, the conceptual idea is that better cybersecurity will decrease the probability of network penetration, and thus influence the cost-benefit calculations of an adversary to the degree that it either disincentives an attack or grinds an attacker to halt over time. Second, deterrence by punishment seeks to discourage the adversary from attacking, recognizing the costly consequences following their actions outweigh the benefits. We have seen variations of this logic being proposed as well. According to Lucas Kello, instead of trying to deter individual acts, countries should go for punctuated deterrence: “a series of actions that generate cumulative effect, rather than tit for tat response”.Footnote35 Third, deterrence by entanglement rests on the unresolved discussion in international relations theory on whether state-to-state interdependence mitigates interstate conflict. Fourth, deterrence by de-legitimization focuses on the creation of norms and rules for state behaviour in cyberspace, will over time translate into a general principle of restraint, raise the reputational costs of bad behaviour, and shrink the battlespace to only encompass military combatants.

#### Prefer our interpretation---

#### 1---Predictable limits---deterrence is disaggregated---including deterrence by punishment allows anything that could result in less damage*.* Opens the floodgates to increasing entanglement and negotiating norms.

#### 2---Ground---plans that result in security create unique process advantage AND avoids spending and tradeoff disads by being less resource intensive.

### Interp/Case List---2NC

#### Cybersecurity protects networks from being attacks by defeating malicious cyberactivity. The brightline for a topical affirmative: if an enemy chooses to attack, would it still have the same effect on NATO networks? If yes, cybersecurity has not changed.

Dr. Charles W. Mahoney 21. Associate professor in the Department of Political Science at California State University, Long Beach. He holds a PhD from UCLA. His research on international security, foreign policy, and defense outsourcing has been published in numerous scholarly journals. “Corporate Hackers: Outsourcing US Cyber Capabilities.” Strategic Studies Quarterly. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-15\_Issue-1/SSQSpring2021.pdf?ver=St5HSe-vLIhxcbMF13qh-w%3D%3D&timestamp=1614258916947

The Joint Chiefs of Staff define cybersecurity as activities that protect United States government data, networks, and cyberspace-enabled hardware by defeating malicious cyber activity carried out by adversaries.11 Various technical responsibilities fall within the broad category of cybersecurity, including providing network defense, software application security, protection of command and tactical communications, and hardware and infrastructure protection against electronic attacks. The central objectives of cybersecurity operations are to protect United States government computers and electronic communication systems and to ensure that military and intelligence agencies possess data availability, integrity, and confidentiality.12

### Violation---Offensive Cyber Operations---2NC

#### OCOs aren’t cybersecurity.

Dr. Charles W. Mahoney 21. Associate professor in the Department of Political Science at California State University, Long Beach. He holds a PhD from UCLA. His research on international security, foreign policy, and defense outsourcing has been published in numerous scholarly journals. “Corporate Hackers: Outsourcing US Cyber Capabilities.” Strategic Studies Quarterly. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-15\_Issue-1/SSQSpring2021.pdf?ver=St5HSe-vLIhxcbMF13qh-w%3D%3D&timestamp=1614258916947

Cybersecurity operations protect United States government computer networks. By contrast, offensive cyber operations seek to penetrate enemy cyberspace and, at times, to impair adversaries’ hardware and critical physical infrastructure.25 The Joint Chiefs of Staff note that all cyber operations conducted outside of “blue cyberspace”—areas in cyberspace protected by the government and its mission partners—are classified as offensive cyber operations.26 Therefore, causing kinetic damage is not a necessary criteria for a cyber operation to be considered offensive in nature. In fact, much offensive cyber activity carried out by the DOD and the intelligence community consists of efforts to gather intelligence, with no intent to cause immediate physical or functional damage to adversaries’ computer systems or infrastructure. These types of nondestructive offensive cyber operations are referred to as “cyber exploitation” and constitute the primary activity of defense contractors operating in the offensive cyber market.

#### They are distinct fields.

Dr. Charles W. Mahoney 21. Associate professor in the Department of Political Science at California State University, Long Beach. He holds a PhD from UCLA. His research on international security, foreign policy, and defense outsourcing has been published in numerous scholarly journals. “Corporate Hackers: Outsourcing US Cyber Capabilities.” Strategic Studies Quarterly. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-15\_Issue-1/SSQSpring2021.pdf?ver=St5HSe-vLIhxcbMF13qh-w%3D%3D&timestamp=1614258916947

This article argues that structural economic differences in three distinct cyber markets—cybersecurity, offensive cyber operations, and data analytics—have important implications for the quality of outsourcing carried out by United States defense and intelligence agencies. In the cybersecurity market, which has existed for over 20 years, contracting is relatively efficient. The market is characterized by numerous suppliers, and government agencies possess detailed information about corporations’ capabilities and past performances. By contrast, the emerging market for offensive cyber operations has a small number of suppliers, and the tools companies develop for offensive cyber missions have limited utility outside national security settings. These two factors are likely to lead to an inefficient market in which government agencies are highly dependent on contractors. Finally, the market for “big data” analytics—which involve collection, analysis, and visualization of information using algorithms—is relatively new. Thus, the Department of Defense (DOD) and intelligence community have little experience assessing the capabilities of competing firms. This feature of the analytics market means that government agencies are more likely to make suboptimal choices when assessing the relative capabilities of companies in the field. However, the competitive nature of the analytics market coupled with the wide applicability of analytics products outside defense-specific settings suggests that assessment and oversight of firms will become more efficient as information about companies increases through repeated contracting.

### AT: Cybersecurity Includes Deterrence---2NC

#### Their evidence is about deterrence by denial, not the plan. Cybersecurity makes it harder to hack, but it doesn’t retaliate.

Dorothy Denning 16. Emeritus Distinguished Professor of Defense Analysis, Naval Postgraduate School. "Cybersecurity's next phase: Cyber-deterrence". Conversation. 12-12-2016. https://theconversation.com/cybersecuritys-next-phase-cyber-deterrence-67090

Cybersecurity aids deterrence primarily through the principle of denial. It stops attacks before they can achieve their goals. This includes beefing up login security, encrypting data and communications, fighting viruses and other malware, and keeping software updated to patch weaknesses when they’re found.

## Case

### Case---1NC

#### 1---Turn---the plan overcommits---fractures the alliance.

Erica D. Lonergan and Sara B. Moller 4/27/22. 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. “Opinion | 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

But despite this rhetoric, exactly how and when Article 5 applies to cyberspace remains unclear. This ambiguity is a problem — with potentially disastrous consequences. Staking the credibility of Article 5 to what are often murky activities in cyberspace threatens to undermine the broader principle of collective defense. We can’t risk fracturing the transatlantic alliance at a critical juncture in its history over a debate on what constitutes a major or minor cyberattack. For that reason, NATO should move quickly to clarify its policy on cyberattacks and explicitly state the threshold for what would trigger an Article 5 response. Furthermore, NATO members should commit to treating cyberattacks that do not rise to the level of a major attack as a national matter — not one for the alliance.

#### Outweighs and turns the case---cyber overcommitment destroys NATO---breaks Article 5 credibility by causing diverging views in the alliance.

Erica D. Lonergan and Sara B. Moller 4/27/22. 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. “Opinion | 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

This equivocation is not surprising, for several reasons. The nature of cyberspace often confounds unequivocal deterrence declarations. States tend to operate in cyberspace with plausible deniability, which can make it difficult to rapidly ascertain responsibility for cyber incidents. Also, it can be challenging to understand the intent behind observed cyber behavior, and there is often a substantial time lag between when an initial penetration of a network occurs and when the target even realizes the breach. And the vast majority of cyber operations cause virtual, not physical, damage, complicating efforts to assess and evaluate the implications of the costs inflicted. Moreover, it can take time to develop and identify a way to infiltrate a network as well as the computer code that takes advantage of a vulnerability for malicious ends. This means states may lack a palatable cyber response option for retaliatory purposes at the desired time.

This creates a slew of practical problems if Article 5 were to be invoked for a cyberattack. From an implementation perspective, it would trigger deliberations within the North Atlantic Council, NATO’s primary decision-making body. Decisions made within the NAC require unanimity, which can be difficult to achieve for many issues but is especially burdensome for cyber ones, given all of the ambiguities outlined above. The most likely outcome of this process would be a long, drawn-out deliberation resulting in a divided alliance unable to agree on how or whether to respond. Quite simply, some allies are unlikely to want to risk World War III for a cyberattack that disrupts the financial infrastructure, for instance, of another country but doesn’t lead to loss of life or sustained damage.

These challenges have major strategic implications for NATO. After years of publicly and repeatedly linking Article 5 to cyberspace and reinforcing that policy in response to the Ukraine conflict, a failure to achieve consensus and respond to a Russian cyberattack against a NATO member could imperil Article 5 in other areas. The disunity that is likely to be revealed during NAC deliberations would then undermine the broader political cohesion that has, for the most part, been remarkably strong throughout the war in Ukraine. This would make it more difficult for the alliance to respond to other forms of Russian behavior. As Biden emphasized at a press conference last month, “the single-most important thing is for us to stay unified … We have to stay fully, totally, thoroughly unified.”

NATO has achieved some strategic ambiguity with its current cyber policy, which may help to deter high-stakes Russian assaults during the present crisis. However, rather than an all-out Russian cyberattack, a far more plausible scenario is a lower-level attack carried out by the Russian government or a proxy group against one or more allies. In this case, the alliance’s interests — not to mention transatlantic security — would be better served by adopting nationally-tailored responses rather than pulling the Article 5 lever. Additionally, to prevent further escalation and reinforce the implicit firebreak that currently exists between cyber and conventional military operations, NATO allies should also agree to restrict any retaliatory response against Moscow to the cyber realm or non-military instruments of power.

#### 2---Turn---ambiguity is key to deterrence---the plan causes under-threshold conflicts.

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

29. NATO maintains a cyber deterrence policy of ambiguity. First, it does not draw a clear line for when a cyber attack is sufficiently harmful to cross the threshold to an armed attack. Second, it does not currently have an operational definition of what the collective response would be if that threshold were to be crossed. Such a cyber deterrence policy offers several advantages. If the Alliance were to set a clear threshold, the opponent would better understand how to stay below that threshold. This would strengthen deterrence of threats above the threshold but would encourage the opponent to increase attacks just below the threshold. A certain degree of ambiguity is beneficial because it could make opponents wary of going too far in their cyber attacks. The opponent always fears stepping over the invisible line, and thus prefers to tread lightly. A similar deterrence posture arguably worked well during the Cold War.

#### 3---Turn---the plan drags us into conflicts.

Michael Horowitz 10. Assistant professor of political science at the University of Pennsylvania and a senior fellow at the Foreign Policy Research Institute. He has also held fellowships at the Olin Institute for Strategic Studies at Harvard, the Belfer Center for Science and International Affairs at Harvard, and the Weatherhead Center for International Affairs at Harvard. “A Common Future? NATO and the Protection of the Commons”. Transatlantic Paper Series No. 3 October 2010. https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/Trans-Atlantic\_Papers\_3-Horowitz.pdf

Alternatively, creating a clear standard could force NATO member states into unnecessary and unwanted conflicts over unsubstantiated threats.44 Mike Rasch, the former head of the U.S. Department of Justice’s computer crimes division, believes that the vague standards at present help members avoid being dragged into conflicts by creating “wiggle room,” something that would not exist in a world of clear standards.45

#### 4---Attribution decks solvency---need consensus and certainty to retaliate.

Stewart M. Patrick 18. James H. Binger Senior Fellow in Global Governance and Director of the International Institutions and Global Governance Program. "NATO's Deterrence Problem: An Analog Strategy for a Digital Age". Council on Foreign Relations. https://www.cfr.org/blog/natos-deterrence-problem-analog-strategy-digital-age

Cyber deterrence is inherently more challenging than nuclear or conventional deterrence because such attacks are difficult to definitively attribute to a particular actor. For example, it is easier to mask the source of a cyberattack on a power grid than it would have been for the Warsaw Pact to conceal a massive incursion into West Germany. This attribution problem could complicate NATO’s capacity to conclusively determine the source of a cyberattack and justify and conduct a timely conventional response, particularly if member states diverge in their perceptions. This dilemma could strain the foundations of collective defense and undermine any unified front against cyberattacks.

For NATO to commit to military action, all of its members would need certainty, beyond a reasonable doubt, about the identity of the perpetrator. This is particularly true in the case of Russia—a known sponsor of cyberattacks. Without conclusive proof, it might be a challenge to convince a distant country like Portugal or a dangerously close one like Estonia to join in a counterattack. Complicating matters, such post-attack decisions would need to be made quickly, given Russia’s precedent of using cyberwarfare as a precursor to kinetic invasion. The need for speed leaves little room for philosophical debates over what constitutes an act of war.

#### 5---No cyber impact---doesn’t escalate and can’t produce successful election interference or anti-NATO sentiment.

Lennart Maschmeyer and Nadiya Kostyuk 2/8/22. Lennart Maschmeyer is a senior researcher at the Center for Security Studies at ETH Zurich. He holds a Ph.D. from the University of Toronto and co-chairs the FIRST Threat Intel Coalition as well as the European Cybersecurity Seminar. Nadiya Kostyuk is an assistant professor at the School of Public Policy and the School of Cybersecurity and Privacy at the Georgia Institute of Technology. She directs the Cybersecurity Summer Institute and co-chairs the Digital Institute Discussion Group. She holds a Ph.D. from the University of Michigan. "There Is No Cyber ‘Shock and Awe’: Plausible Threats in the Ukrainian Conflict". War on the Rocks. https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/

These predictions suggest that cyber operations will provide significant strategic advantages to Russia either as complements to military force, or as standalone instruments — or at least that policymakers and commentators think that they will. Current warnings of escalating cyber warfare conjure deep-seated fears of cyber doom and the recurring specter of a “cyber Pearl Harbor” strategic surprise attack. In practice, however, cyber warfare has been a failure. Our research shows that cyber operations have remained irrelevant on the battlefield, while standalone operations to weaken Ukraine through election interference, critical infrastructure sabotage, and economic disruption largely failed to contribute to Russia’s strategic goals of making Ukraine abandon its pro-European Union and pro-NATO foreign policy. Consequently, current fears of cyber warfare defy not only Russia’s track record in Ukraine, but also strategic logic. Given that Russia’s cyber operations have failed to produce significant strategic value to date, why would we expect this to suddenly change now? Or, to put it more pointedly: If cyber operations offer such effective and potent instruments, why did Russia go through the trouble (and costs) to mobilize its troops? Current predictions of cyber onslaught do not offer a persuasive answer.

Giving in to these fears risks fighting phantom threats, playing into Russia’s hands by distracting from the need to counter its military threat and sowing fear and confusion — at least among Western audiences. A level-headed analysis of the threat that distinguishes what is theoretically possible from what is practically feasible is urgently needed. Our research suggests that, contrary to hysteria, cyber operations will remain of secondary importance and at best provide marginal gains to Russia.

Expectations Versus Evidence: Cyber Operations and Their Limits

There are three distinct perspectives on the strategic role and value of cyber operations in conflict. Early scholarship on cyber conflict expected cyber operations to be primarily important in conventional military conflict, enabling crippling strategic strikes analogous to the surprise attack on Pearl Harbor during World War II. If successful, cyber operations could thus be substituted for the use of force. Yet research throughout the 2010s made the limitations of cyber operations as a means of force projection increasingly clear.

Subsequent scholarship thus sees cyber operations primarily as complements to force. Possible effects include disrupting command and control and communications systems, sabotaging equipment and infrastructure, spreading disinformation, and conducting psychological warfare to undermine morale among enemy troops.

The third and increasingly influential perspective instead suggests cyber operations are primarily relevant in “gray zone” conflict short of war. In this view, cyber operations offer standalone instruments of power that can influence and weaken an adversary through critical infrastructure sabotage, economic disruption, and influence operations. Hence, as in cyber Pearl Harbor scenarios, it also suggests that cyber operations could substitute for the use of force — achieving similar goals without going to war. However, rather than through a massive surprise strike, this third school of thought expects the effects to be gradual and cumulative, eroding adversary strength over multiple operations.

The empirical record of cyber conflict, however, suggests that what is feasible in practice is far more limited. Ukraine has been a “giant test lab” where Russia, one of the world’s foremost cyber powers, has experimented with cyber operations for eight years. Yet these operations have failed to produce significant strategic value either as force complements or standalone tools.

The substitutability argument — that states can or do substitute cyber operations for the use of force — has little empirical support since Russia levied no major cyber operations against Ukraine in the runup to the military escalation of the conflict in 2014. While it is possible that we do not know about such operations given their veil of secrecy, it is clear that any attempted but undetected cyber surprise strike failed to produce any measurable effects.

Evidence supporting the complementarity perspective is similarly sobering. One of us has examined the role of low-level disruptive cyber operations in the military conflict and their relevance for battlefield events (and outcomes). Disruptive attacks can directly affect military operations as they seek to sabotage an opponent’s ability to fight. For example, the Russia-backed separatists in the Donbas and Luhansk regions used malware to retrieve data from mobile devices on the locations of Ukrainian artillery troops, facilitating better reconnaissance against these troops. Pro-Ukrainian hackers hijacked CCTV cameras behind enemy lines to obtain intelligence on the movement of Russian artillery in the separatist-controlled territories.

Focusing on the period of the most intense fighting, between 2014 and 2016 — the time when, if cyber tools are an effective complement to armed force, Russia would have been most likely to use them — we applied a series of statistical tests to thousands of cyber and military operations. The findings showed a strong, escalatory dynamic between military operations by both sides but no significant correlation in either direction between military and cyber operations, and no reciprocity between cyber operations. This evidence demonstrates that in one of the first armed conflicts where both sides used low-level cyber operations extensively, digital operations unfolded independently from the events on the ground and had no discernible effect on them. Hence, in stark contrast to expectations about the force-multiplying advantages of cyber operations, these findings suggest hacking groups faced considerable difficulties in responding to battlefield events, much less shaping them.

Finally, the track record of cyber operations as standalone instruments in gray zone conflict in Ukraine also falls far short of expectations. One of us has examined the operational mechanisms, effects, and strategic value of five major Russia-sponsored cyber operations, including election interference, critical infrastructure sabotage, and economic disruption. Contrary to prevailing expectations, the majority made no measurable contribution towards Russia’s strategic goals. The NotPetya operation, whose large-scale disruption of businesses wiped off half a percentage point of Ukraine’s gross domestic product in 2017, is the exception. Yet this operation underlined a key shortcoming of cyber operations: the risk of losing control over the spread of effects, producing unintended consequences, added costs, and correspondingly lowering strategic value. Forensic analysis by internet security company ESET revealed that the Sandworm hacking group underestimated how far NotPetya’s data-destroying malware would spread. It “went out of control” and spread far beyond Ukraine, even disrupting targets in Russia — including the state-controlled oil giant Rosneft. These disruptions within Russia will have caused additional costs, as did the sanctions that Western countries imposed on Russia in response to NotPetya’s international disruption.

Evidence from Ukraine thus supports neither the force substitute nor the force complement argument. Instead, cyber operations have been most relevant as standalone, lower-intensity alternatives to the use of force — more in line with the third school of thought. Yet by and large they fell short of providing measurable strategic value. Indeed, all available evidence indicates that Russia’s cyber warfare efforts against Ukraine — combined with its larger gray zone campaign — have failed to make Ukraine abandon its rapprochement with the West. That is why Russia has mobilized its army, attempting to prevent Ukraine from joining the Western alliance through threat of invasion.

Plausible Threats in the Conflict Ahead

Considering the underwhelming track record of cyber warfare in Ukraine to date, there is little reason to expect cyber doom of the kind that some now predict. For these warnings of a Russian cyber onslaught to become reality, cyber operations would need to produce effects at a scope and scale that they have previously failed to attain. Importantly, current warnings fail to make a persuasive case on why we should expect such a transformation.

Rather, they rest on the implicit assumption that with the change in strategic context, the role of cyber operations will change as well. This comes out clearest in Maggie Miller’s recent commentary suggesting that military escalation in Ukraine would finally herald “a true cyberwar” where Russia could “take down the power grid” or launch a disinformation campaign to undermine the government in Kyiv. Dmitri Alperovitch offers a more level-headed analysis, underlining that cyber operations alone will fall short of achieving Russia’s goals. However, he also suggests that they can complement force as an “extension of warfare itself,” disrupting command and control to provide battlefield advantages, sabotaging critical infrastructure, and undermining public trust in the government to “send a powerful signal that resistance is futile.” Yet, as we have seen, Russia has attempted most of these objectives in the past and has failed. Even in a full-scale invasion, we have the same aggressor, with the same hacking groups, with the same skill level going after the same sets of possible targets. Why would we expect different results?

Changing the strategic context of deployment does not change the mechanism of action that cyber operations rely upon to produce outcomes — and its intrinsic constraints. Cyber operations rely on a mechanism of subversion that exploits vulnerabilities in adversary systems to use them against the adversary. This mechanism holds great strategic promise but poses significant operational challenges. It requires creativity and cunning to remotely manipulating complex systems that others designed and operate without alerting the victim to one’s presence. These challenges produce an operational trilemma between the speed, intensity of effects, and level of control that actors have over these effects. This trilemma limits strategic value, since in most circumstances cyber operations will be too slow, too weak, and too volatile to contribute measurably to strategic goals. The constraining role of this trilemma is evident across all five of Russia’s disruptive cyber operations against Ukraine thus far, underlining their relevance. Importantly, all available evidence indicates that these intrinsic constraints limit the strategic value of cyber operations regardless of strategic contexts.

#### 6---Status quo solves deterrence and credibility---grave cyber threats are incorporated into Article 5.

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

4. The Alliance first publicly recognised the need to strengthen cyber security and defence at the 2002 Prague Summit. In 2008, NATO adopted its first cyber defence policy. However, the crucial turning point came in 2014 at the Wales Summit, when the Alliance adopted an Enhanced NATO Cyber Defence Policy. Among other key decisions, NATO leaders explicitly stated a cyber attack could lead to the invocation of Article 5. For the first time, Allied leaders made clear that “[c]yber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability” (NATO, 2014).

5. Since the Wales Summit, NATO and the Allies have made cyber security, defence, and deterrence an unambiguous part of NATO's core tasks and implemented the steps to make this a reality. By now, any potential opponent should have realised that a sufficiently harmful cyber attack against one Ally will be considered an armed attack against all and that Allies will invoke Article 5 to collectively defend themselves. At the 2018 NATO Summit in Brussels, Allied leaders once again reiterated this commitment: “Reaffirming NATO’s defensive mandate, we are determined to employ the full range of capabilities, including cyber, to deter, defend against, and to counter the full spectrum of cyber threats, including those conducted as part of a hybrid campaign” (NATO, 2018a).

#### 7---Information infrastructure is private sector---they’ll says no.

Jamie Collier 15. DPhil Candidate in Cyber Security at Oxford’s Centre for Doctoral Training in Cyber Security. "NATO’s role in the cyber domain is unclear". https://www.cybersecurityintelligence.com/blog/natos-role-in-the-cyber-domain-is-unclear-775.html

First, there are a number of flaws in the militarisation of the cyber domain. The majority of those with the necessary technical skills to respond to the cyber security challenges work outside of the military sector. In addition, a large proportion of the infrastructure within the cyber domain is privately owned and operated. This prevents NATO from making a substantial contribution to its protection. Crucially, NATO does not have any rights, or powers, to intervene in the private sector. Given NATO’s current lack of expertise in the area, private sector firms are unlikely to welcome NATO assistance.

#### [IF APPLICABLE] 8---No democracy impact---democratic peace theory is wrong

Daniel Larison 12. PhD in history from the University of Chicago Democratic Peace Theory Is False http://www.theamericanconservative.com/larison/democratic-peace-theory-is-false/

Rojas’ claim depends entirely on the meaning of “genuine democracy.” Even though there are numerous examples of wars between states with universal male suffrage and elected governments (including that little dust-up known as WWI), the states in question probably don’t qualify as “genuine” democracies and so can’t be used as counter-examples. Regardless, democratic peace theory draws broad conclusions from a short period in modern history with very few cases before the 20th century. The core of democratic peace theory as I understand it is that democratic governments are more accountable to their populations, and because the people will bear the costs of the war they are going to be less willing to support a war policy. This supposedly keeps democratic states from waging wars against one another because of the built-in electoral and institutional checks on government power. One small problem with this is that it is rubbish.

Democracies in antiquity fought against one another. Political equality and voting do not abolish conflicts of interest between competing states. Democratic peace theory doesn’t account for the effects of nationalist and imperialist ideologies on the way democratic nations think about war. Democratic nations that have professional armies to do the fighting for them are often enthusiastic about overseas wars. The Conservative-Unionist government that waged the South African War (against two states with elected governments, I might add) enjoyed great popular support and won a huge majority in the “Khaki” election that followed.

As long as it goes well and doesn’t have too many costs, war can be quite popular, and even if the war is costly it may still be popular if it is fought for nationalist reasons that appeal to a majority of the public. If the public is whipped into thinking that there is an intolerable foreign threat or if they believe that their country can gain something at relatively low cost by going to war, the type of government they have really is irrelevant. Unless a democratic public believes that a military conflict will go badly for their military, they may be ready to welcome the outbreak of a war that they expect to win. Setting aside the flaws and failures of U.S.-led democracy promotion for a moment, the idea that reducing the number of non-democracies makes war less likely is just fantasy. Clashing interests between states aren’t going away, and the more democratic states there are in the world the more likely it is that two or more of them will eventually fight one another.

#### [IF APPLICABLE] 9---No secession---structural incentives outweigh.

Richard Rosecrance and Arthur Stein 08. Richard Rosecrance is Adjunct Professor of Public Policy at the John F. Kennedy School of Government and Senior Fellow at the Belfer Center for Science and International Affairs, both at Harvard University. Arthur Stein is Professor of Political Science at UCLA. “Separatism's Final Country”. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/Weinstein%2C\_Humphreys\_Is\_Ethnic\_Conflict\_Inevitable.pdf

More important, the nationalist prospect was and remains hopelessly impractical. In the world today, there are 6,800 different dialects or languages that might gain political recognition as independent linguistic groups. Does anyone seriously suggest that the 200 or so existing states should each, on average, be cut into 34 pieces? The doctrine of national self-determination reaches its reductio ad absurdum at this point.

Furthermore, the one-nation, one-state principle is unlikely to prevail for four good reasons. First, governments today are more responsive to their ethnic minority communities than were the imperial agglomerations of yesteryear, and they also have more resources at their disposal than their predecessors did. Many provinces populated by discontented ethnic groups are located in territories adjacent to national capitals, not overseas. And many governments in this era of globalization have annual budgets equivalent to nearly 50 percent of their GDPs, much of which is spent on social services. They can -- and do -- accommodate the economic needs of their states' differentiated units. They also respond to those units' linguistic requests. Basques, Bretons, Punjabis, Québecois, and Scots live quite well inside the bonds of multinational sovereignty and in some cases better than residents of other provinces with no claims of being a distinct nation.

Second, the achievement of separate sovereignty today depends on external recognition and support. Prospective new states cannot gain independence without military assistance and economic aid from abroad. International recognition, in turn, requires the aspiring nationalist movement to avoid international terrorism as a means of gaining attention. If a separatist group uses terrorism, it tends to be reviled and sidelined. If an ethnic group does not have enough support to win independence by peaceful electoral means inside its country, its resorting to terrorism only calls into question the legitimacy of its quest for independence.

Recognizing this, the Québecois abandoned the terrorist methods of the Quebec Liberation Front. Most Basques castigate Basque Homeland and Freedom (known by its Basque acronym ETA). Enlightened Europeans have withdrawn their support for the Chechen rebels. And the continued terrorist shelling of Israeli cities from a Hamas-dominated Gaza might undermine the previous international consensus in favor of a two-state solution to the Palestinian problem, or at least warrant an exceptional approach to Gaza.

With the possible exception of the Palestinians, the notion that any of these peoples would be better off in smaller and weaker independent states in a hostile neighborhood is unrealistic. Occasionally, dissidents make the case that if they were to leave the state unit, they would be taken into the comforting embrace of the European Union or the North American Free Trade Agreement, thereby gaining access to a large market. But that would depend a great deal on outsider support for their cause. The United Kingdom might not wish to see Scotland in the EU and would be in a position to veto its membership. The United States and Canada might not agree to let an independent Quebec join NAFTA. The belief that when a tiny nation is born it falls automatically into the loving hands of international midwives is questionable. The truth varies from case to case.

Third, although globalization initially stimulated ethnic discontent by creating inequality, it also provides the means for quieting discontents down the road within the fold of the state political system. Distributed economic growth is a palliative for political discontent. Indonesia, Malaysia, Singapore, and Thailand contain different ethnic groups that have largely profited from the intense economic resurgence of their states stimulated by globalization. Northern and southern Vietnam are culturally different, but both have benefited from the country's economic growth. Cambodia has a diverse population, but it has gained greatly from China's move to externalize some of its production.

Fourth, a discontented population may react to ethnic discrimination, but it also responds to economic need, and whatever its concerns, it does not always have to seek independence to alleviate them. It has another safety valve: emigration to another country. The state of Monterrey has not sought independence from Mexico; rather, many of its inhabitants have moved, legally or illegally, to the United States. The huge emigration from the Maghreb to France and Italy reflects a similar attitude and outcome; the dissatisfied populations of North Africa can find greater welfare in Europe. And when Poles move to France or the United Kingdom, they do not secede from the mother country but demonstrate greater satisfaction with French or British rule. Emigration is the overwhelming alternative to secession when the home government does not sufficiently mitigate economic disparities.

Even where the central government has used force to suppress secessionist movements, it has offered carrots at the same time that it has yielded sticks. The province of Aceh has been coaxed, even as it has been subjected to threats, to remain inside the Indonesian republic. Kashmir, facing a balance of restraints and incentives, is unlikely to emerge as an independent state in India. And the Tamil Tigers have lost the sympathy of the world by their slaughter of innocent Sinhalese.

The recent formation of an "independent" Kosovo, which has not yet been recognized by various key countries, does not foretell the similar arrival of other new states. It is unlikely that Abkhazia or South Ossetia, although largely autonomous in fact, will gain full and formal independence from Georgia or that the Albanian areas of Macedonia will secede. Rather, prospective secessionists, dissuaded by both central governments and the international community, are likely to hold back. Indeed, the most plausible future outcome is that both established states and their international supporters will generally act to prevent a proliferation of new states from entering the international system.

#### [IF APPLICABLE] 10---No NATO impact and collapse inevitable.

Sanbeer Singh Ranhotra 2/25/22. Senior Columnist. "The irrelevance of NATO is now out in the open". TFIGlobal. xx-xx-xxxx. https://tfiglobalnews.com/2022/02/25/the-irrelevance-of-nato-is-now-out-in-the-open/

NATO is a headless chicken. It has been reduced into an insignificant entity which when told to shut up by Russia, goes to a corner and quietly sits down – making sure to behave itself. It is quite remarkable how Ukraine thought this organisation would come to its aid in the event of a large-scale Russian invasion. Leave alone military aid, NATO has not even been able to agree on a decisive economic sanctions package that would have an immediate effect on Moscow.

Russia has invaded Ukraine. The world is outraged. The United States and its allies are angry. NATO is infuriated. But here’s the ridiculously painful part: NATO can do nothing but mutely spectate as Russian President Vladimir Putin redefines Eastern Europe. Essentially, NATO has failed. It had one mandate – to protect Europe. It has failed to achieve its primary objective, and this would have lasting consequences for the security alliance.

U.S.-led NATO a Failure

NATO is an expensive yet useless organisation that American taxpayers fund. The United States pays to keep Europe “safe”. But Europe buys billions of dollars worth of gas from Russia. So, Joe Biden refuses to sanction Russia’s energy sector.

On Thursday, Joe Biden announced a set of sweeping sanctions against Russia and Moscow’s elite. Biden said his administration would stunt the Russian military’s ability to finance and grow its force; freeze U.S. assets held by Russian banks; target elites and members of Putin’s inner circle, and curtail Russia’s high-tech imports.

But Biden left out Russia’s energy sector – which in a way, pretty much bankrolls Russia’s economy. Because the Biden administration and NATO merely want to appear to be taking on Russia. They don’t want to antagonise Moscow.

What else explains European countries – led by the likes of Italy, Germany and others vetoing a proposal to ban Russia from using the SWIFT global interbank payments system? You see, data from the Bank of International Settlements (BIS) shows that European lenders hold the lion’s share of the nearly $30 billion in foreign banks’ exposure to Russia.

Late on Thursday, Ukrainian President Volodymyr Zelensky couldn’t keep it to himself any longer. So, in an address to Ukrainians, he lambasted European countries and other Western powers for making false promises.

He said, “I have asked 27 European leaders whether Ukraine will be in NATO… Everyone is afraid, no one answers.” NATO has abandoned Ukraine. Europe – which until recently referred to Ukraine as a compatriot, has failed to provide any substantial and meaningful aid to the country that is being invaded.

Ukraine, by Zelensky’s admission, is all alone. NATO is nowhere to be seen, and the United States is imposing convenient sanctions against Russia which Moscow has grown immune against.

NATO Will Cease to Exist

The invasion of Ukraine has shown that Europe is not united. Every European country is keeping its interests above the supposed idea of protecting ‘Europe’ as a whole. There is no cohesion among European nations, and Joe Biden’s administration remains simply clueless.

The United Kingdom, meanwhile, is thanking its stars that it left Europe at the right time. But the larger message that this fiasco has sent out has not been lost on any country. Now, every European country knows that NATO – for all purposes – is a toothless organisation.

The crisis in Eastern Europe will lay the foundation for the disintegration and ultimate evaporation of NATO.

#### 11---EU solves---they’ll fill NATO gaps.

Oliver Noyan 21. Journalist at Euractiv. "European Parliament calls for increased EU cybersecurity capacity". euractiv. 7-10-2021. https://www.euractiv.com/section/cybersecurity/news/european-parliament-calls-for-increased-eu-cybersecurity-capacity/

The EU cyber defence capabilities report took stock of the current cybersecurity framework in the EU and outlined several gaps, ranging from the need to intensify cooperation between the member states to increasing collaboration with NATO.

The main goal is “to strengthen cyber resilience and develop common cyber security and defence capabilities to respond to these kinds of security challenges,” said Renew Europe MEP Urmas Paet, who authored the report.

Hybrid Threats and Collective Defence

The report also said that the EU is increasingly involved in “hybrid conflicts with its adversaries,” notably China, North Korea, and Russia.

“The picture could not be any clearer, for state actors’ hostile to the EU, like Russia, the cost for attacks is infinitely smaller than the rewards, and that has to change,” centrist MEP Barry Andrews said.

Parliament considered these hybrid conflicts to be particularly dangerous and destabilising for democracies, as they blur the line between war and peace through cyber-enabled disinformation campaigns or targeting digital service providers and critical infrastructure.

However, these attacks are not severe enough to trigger the collective defence clauses under Article 5 of the NATO treaty or the defence and solidarity clauses under the treaties of the EU.

To tackle this legal vacuum, the parliamentary report stressed that the provisions for collective defence in the EU treaties should be reinterpreted to allow for voluntary collective countermeasures.

“This is the only effective means to counter the paralysis in reacting to hybrid threats,” the report reads.

Cyber Diplomacy Toolbox

The EU already has several tools at its disposal to respond to cyber-attacks, most notably the cyber diplomacy toolbox.

### XT---1NC 1---Divergence---Alliance Impact

#### The plan alienates NATO.

Alex Xiao 20. J.D. Candidate at Duke University School of Law, Class of 2020. “Responding to Election Meddling in The Cyberspace: An International Law Case Study on The Russian Interference in The 2016 Presidential Election”. Duke Journal of Comparative & International Law. Vol. 30:349. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1565&context=djcil

Categorizing the Russian DNC hack as an armed attack might also invite an escalation of cyber conflict by triggering Article 5 of the North Atlantic Treaty Organization (“NATO”) Charter,62 which calls for a collective response from all NATO States. It could alienate NATO partners to put the entirety of NATO in a confrontation with Russia over an election meddling operation that caused no physical damage. After all, Estonia, even after suffering a much stronger attack from Russia in 2007 that temporarily disabled a large percentage of its Internet system, did not invoke Chapter 5 for these considerations.63

#### Cyber article 5 fractures the alliance and distracts from other priorities.

Jason Blessing 4/25/22. Jeane Kirkpatrick Visiting Research Fellow @ AEI. "The Russian cyber threat is here to stay and NATO needs to understand it". American Enterprise Institute - AEI. 4-25-2022. https://www.aei.org/op-eds/the-russian-cyber-threat-is-here-to-stay-and-nato-needs-to-understand-it/ https://www.aei.org/op-eds/the-russian-cyber-threat-is-here-to-stay-and-nato-needs-to-understand-it/

Since the Russian invasion of Ukraine, the Biden administration has escalated warnings about likely Russian cyber-attacks on American infrastructure and business. More worrying still, cyber alarmists like Senate Intelligence Committee Chairman Mark Warner, D-Va., have suggested that cyber-attacks from the Kremlin could be acts of war that trigger NATO’s collective defense.

This sky-is-falling delusion, particularly from leaders with access to classified intelligence, is at best counterproductive and at worst dangerous.

Cyber-attacks are rarely acts of war, and treating them as if they are undermines NATO’s ability to deal with real threats short of cyber war.

NATO has only invoked Article 5 – which triggers a collective response – once and that was after the 9/11 attacks.

Cyber-attacks are unlikely to destroy buildings and kill thousands in an instant. While collective defense extends to cyberspace, few operations could realistically be a cause for war.

This would include cyber-attacks resulting in death or damage like traditional military operations or coordinated assaults that take the power grid or entire economic sectors offline. These scenarios are unlikely though: such attacks require far too much time, funding, manpower, and control. Instead, most attacks temporarily overwhelm servers with traffic, deny network access, hold computers hostage, and steal or delete data.

Even if allies wanted to trigger Article 5 over cyber operations, disagreements about the definitions of threats, origins of attacks, and pain thresholds in cyberspace can derail the process.

Collective retaliation requires a unanimous vote across NATO; building unity across these points is nearly impossible for most cyber activity. Unlike missile attacks or tanks in the streets, few “red lines” exist to distinguish cybercrime, cyber espionage, and cyber disruption from digital acts of war.

#### Threshold probing collapses the alliances---allies will be choosing between NATO cred and internal interests.

James Joyner 10. Managing editor of the Atlantic Council. "NATO's Cyber Threat". National Interest. 7-2-2010. https://nationalinterest.org/commentary/natos-cyber-threat-3590

That seems reasonable enough and is certainly a matter that deserves discussion within NATO. Indeed, I have it on good authority, it’s in fact being discussed frequently. But, while it makes sense for the allies to draw up contingency plans and reinforce their cooperation and capabilities in this burgeoning arena, we should stop short of formally declaring what precise set of circumstances would allow Article 5 to be invoked.

First, doing so would put the members in a bind. A cyber attack might technically meet the theoretical definition put forth in advance without the actual circumstances generating consensus for any number of reasons. Perhaps the aggrieved party will be perceived to have provoked the attack by belligerence—belligerence that would actually be encouraged by an a priori declaration of support.

Or perhaps the risks of retaliation simply outweigh the damage done by the attack because of complicating circumstances. This is hardly unthinkable given that the most probable nation-state aggressors are Russia and China.

Regardless, the allies would then be forced to choose between the credibility of NATO and their own short-term interests. It’s an untenable position far more likely to harm the alliance and its members than to ward off the cyber threat.

Second, there’s tremendous value in strategic ambiguity. This was commonly understood during the Cold War, when the United States refused to declare that it would not engage in first use of nuclear weapons. While our leaders almost certainly had no intention of launching a first strike, they knew that declaring this formally would make a conventional attack—which could be expected to escalate to a nuclear war—more likely.

In the cyber case, drawing a bright line for potential adversaries virtually invites actions just short of casus belli. By instead simply declaring that there may be circumstances in which NATO will consider a cyber attack on one of its members an attack on all—but not spelling out what those circumstances may be—those contemplating such an attack will have an additional risk factor to deter them.

The North Atlantic Council should simply come to an understanding that the charter’s 1947 language requiring an “armed attack” to invoke collective defense is dated and that flexibility is needed for emerging threats. Plus, they should agree to increase cooperation in this arena and streamline the process by which consultation under Article 4 can take place.

#### Divergence causes tensions.

Dr Max Smeets 21. Center for Security Studies, ETH Zürich (Switzerland) . "NATO allies’ offensive cyber policy: A growing divide?". 8-6-2021. https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/

The divergence in cyber policy across NATO member states is problematic. Allies disagree on both the goals of cyber policy and the ways and means to achieve them. This can cause tension between allies, especially when it comes to the necessity and legitimacy of operating on each other’s national systems and networks.

Some may argue that these differences result from differences in maturity. Some states simply have not caught up with the latest developments, goes the argument. This assumes a single path to cyber maturity or that the dynamics of cyberspace pull all states in the same direction. It suggests that – even without major policy coordination – allies’ cyber policies will converge over time. But a more persuasive understanding of the current trend is that even though states can learn from each other’s institutional progress, differences do not merely stem from states “lagging behind.” These states are on a different policy path. This means it requires dedicated and sustained policy attention to, at a minimum, coordinating the different policies of states – and potentially bring them closer together.

### XT---1NC 1---Divergence---Cyber Response

#### NATO won’t agree in practice.

David E. Sanger 2/1/22. White House and national security correspondent at NYT. "U.S. Sends Top Security Official to Help NATO Brace for Russian Cyberattacks". New York Times. 2-1-2022. https://www.nytimes.com/2022/02/01/us/politics/russia-ukraine-cybersecurity-nato.html

If Russia conducts cyberattacks on Ukraine that are not connected to a traditional military invasion, American officials acknowledge it is uncertain whether Europe would agree to invoke the sanctions that the United States has promised would follow a ground assault. As President Biden himself acknowledged in a news conference two weeks ago, the allies are divided on what kind of sanctions or other steps would be triggered by an action that falls short of a full-fledged invasion.

When the White House tried to explain what Mr. Biden meant when he questioned how the West would respond to a “minor incursion” into Ukrainian territory, the White House press secretary, Jen Psaki, suggested in a statement that he had “cyberattacks and paramilitary tactics” in mind, which fall short of traditional military attacks. Still, she said that “those acts of Russian aggression will be met with a decisive, reciprocal and united response.”

But Mr. Biden’s comments highlighted the reality that NATO and the European Union have never acted in concert in responding to a broad cyberattack. When Russia was blamed for the SolarWinds supply chain attack in late 2020 and early 2021, which affected the U.S. government and hundreds of global firms, only Washington announced significant sanctions. And Mr. Biden himself pulled back from warnings during the transition to the presidency that he would authorize a counter cyberattack.

#### They can’t get public buy in.

Christopher Porter and Klara Jordan 19. Christopher Porter is the chief intelligence strategist of cybersecurity company FireEye and a nonresident senior fellow at the Atlantic Council. Klara Jordan is director of the Cyber Statecraft Initiative at the Atlantic Council’s Scowcroft Center for Strategy and Security. "Don’t Let Cyber Attribution Debates Tear Apart the NATO Alliance". Lawfare. 5-18-2022. https://www.lawfareblog.com/dont-let-cyber-attribution-debates-tear-apart-nato-alliance

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

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

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

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

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

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

### XT---1NC 1---Divergence---Guideline Formation

#### Forming guidelines is a fight.

Stephen Jackson 16. JD from George Mason University School of Law and is a Research Associate at the Center for Infrastructure and Protection at the George Mason University School of Business. "NATO Article 5 and Cyber Warfare: NATO's Ambiguous and Outdated Procedure for Determining When Cyber Aggression Qualifies as an Armed Attack." Center for Infrastructure Protection & Homeland Security, https://cip.gmu.edu/2016/08/16/nato-article-5-cyber-warfare-natos-ambiguous-outdated-procedure-determining-cyber-aggression-qualifies-armed-attack/

The formation of binding cyber-attack guidelines for all NATO members and the North Atlantic Council will not be an easy task. As stated earlier, each NATO nation has independently formed its own set of standards for combating cyber aggression. Individualization among members will assuredly create friction in drafting these guidelines. However, NATO would be wise to begin the process before these individualized standards become too offensive for a uniform NATO procedure.

#### That zeros solvency.

Khatuna Burkadze 18. Fulbright scholar at the MIT Center of International Studies as well as a visiting researcher at Columbia University, Bard College and the Fletcher School of Law and Diplomacy. Graduate of the Fletcher School of Law & Diplomacy, Tufts University. “A Shift in NATO's Article 5 in the Cyber Era”. 42 42 Fletcher F. World Aff. 215 (2018).

As for Article 5 of the North Atlantic Treaty, despite the changing security environment, the original treaty has never had to be modified.4 3 Practically, it is impossible to make an amendment in Article 5 to clearly define what constitutes a cyberattack. Nevertheless, the Tallinn Manuals emphasize that the language of the North Atlantic Treaty allows for the possibility of using collective defense in cases of cyberattacks. These manuals analyze existing binding regulations applicable to cyberspace. We can say that the Tallinn Manuals are non-binding documents with the interpretations of binding international norms. Professor Schmitt mentioned that these Manuals are intended to be secondary sources of law: they explain the law, but they do not create it.4 4

### XT---1NC 1---Divergence---AT: US Convinces

#### The US can’t convince allies---we lack technical expertise.

James Stavridis 2/26/22. Bloomberg Opinion columnist. He is a retired U.S. Navy admiral and former supreme allied commander of NATO, and dean emeritus of the Fletcher School of Law and Diplomacy at Tufts University. He is also chair of the board of the Rockefeller Foundation and vice chairman of Global Affairs at the Carlyle Group. "The West’s Cyber Appeasement Helped Give Putin a Green Light". Washington Post. 2-26-2022. https://www.washingtonpost.com/business/energy/the-wests-cyber-appeasement-helped-give-putin-a-green-light/2022/02/26/339f5a68-970d-11ec-bb31-74fc06c0a3a5\_story.html

There are three explanations for this modern-day form of digital appeasement.

The first is that the West’s diplomatic corps is simply not equipped to engage in influential dialogue with other cyber-powers. Said differently, our diplomacy isn’t technical enough. This isn’t a pejorative statement; rather, the diplomatic culture hasn’t adapted to the digital dimension of geopolitics.

### XT---1NC 2/3---Over/Underreaction

#### The plan ties NATO’s hands---ambiguity is best to prevent under and overreaction.

Ken M. Jones 15. Lieutenant, United States NavyB.A.S., Wayland Baptist University, 2008. Master Thesis in Cyber Systems and Operations Cyber War: The Next Frontier For NATO. Naval Postgraduate School.

Finally, NATO needs to maintain ambiguity on what justifies an Article 5 response. As mentioned previously, ambiguity has served NATO well. A set threshold for when NATO will invoke an Article 5 response to a cyber-attack on a member country is not necessary. This ambiguity has historically served the alliance well, as demonstrated by the 9/11 attacks. If the alliance had said weapons were only include guns, bullets, tanks, and bombs, it would have set a threshold precluding a NATO response to attacks that turned four planes into improvised missiles. The larger issue of ambiguity is that there is no set definition of what constitutes an armed attack and what circumstances dictate a collective response, as per Article 5. Remaining ambiguous on the severity threshold of a cyber-attack allows the alliance to act in cases of future cyber-attacks that cause severe damage, but also allow NATO to refrain from over-reacting, even if an event is a cyber, or kinetic, attack as per a definition. It would be a mistake to set a threshold for attacks that cannot currently be anticipated.

When NATO was originally formed, it was with the purpose to be unambiguous, with the promise of “massive retaliation” by Eisenhower. This was meant to constantly act as a reminder to the Soviet Union and the Red Army that if they were to surge into Western Europe, in no uncertain terms NATO would respond with nuclear weapons. Ambiguity is useful in times, and at other times, it is not. Had NATO been ambiguous in dealing with the Soviet Union, there could have been opportunity for the Red Army to advance further across Europe, to test and see what NATO, and the United States, would allow them to get away with, without an attack. Ambiguity can also cause problems, particularly in the event of a cyber-attack with some members feeling an attack might warrant retaliation through Article 5, with others feeling that the necessary thresholds have not been met. It is important for NATO to have a clear understanding, or general belief, of what would constitute a serious enough cyber-attack in order to respond, but not through official policy or rules to ensure proper consideration.

B. CONCLUSION

This thesis has reviewed the history of NATO and its role in the world, and has found that since its creation post-WWII, the NATO alliance has been able to adapt to changing times. It remains an organization that promotes peace but will use force if necessary. NATO has taken on the new challenge of cyber-attacks that the current world faces today. It has also taken steps to prevent cyber-attacks on itself and member countries, as well as to make it clear to any person, nation, or organization that an Article 5 response will be invoked in the case of a serious cyber-attack that can be deemed an armed attack according to scale, effects, and attacker motivation.

Article 5 is the most important article in the Washington Treaty, on which the entire alliance is hinged. As in the 9/11 attacks on the United States by a foreign enemy, NATO showed it was a force to be reckoned with when it invoked Article 5 for the first time in its history. It came to the aid of the United States and sent a loud resounding message to the world that terrorism would not be tolerated.

Since the cyber world is still so new and continues to advance each day with new technologies, NATO is still trying to find the best policies and best course of action to take in response to the new threats to peace and democracy that cyber-attacks pose on the alliance and this new world. NATO welcomes and many experts on cyberspace give it recommendations on how to deal with this new threat. The cyber world is too new for NATO to bind its hands, so to speak, with rigid rules and laws regarding when, how, and why it would invoke Article 5 in the case of a cyber-attack on a member country. In response, at the 2014 summit in Wales, the alliance made it clear that a cyber-attack can and will invoke an Article 5 response. It also made it clear that ambiguity has served the alliance well, and it refused to define the kind of attack that would invoke an Article 5 response.

### XT---1NC 2---Low Level Attacks

#### The plan greenlights low level attacks.

Michael Horowitz 10. Assistant professor of political science at the University of Pennsylvania and a senior fellow at the Foreign Policy Research Institute. He has also held fellowships at the Olin Institute for Strategic Studies at Harvard, the Belfer Center for Science and International Affairs at Harvard, and the Weatherhead Center for International Affairs at Harvard. “A Common Future? NATO and the Protection of the Commons”. Transatlantic Paper Series No. 3 October 2010. https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/Trans-Atlantic\_Papers\_3-Horowitz.pdf

One option is to lay out a specific policy that would be a part of the Strategic Concept and that describes the sort of cyber attack that is damaging enough to trigger an Article 5 commitment from other NATO member states. The risk of such a specific declaration is that it could “green light” lower level attacks by guaranteeing that they would not trigger a NATO response. The advantage of a specific policy is that it sets up a clear red line for potential adversaries and potentially deters more dangerous types of cyber attacks. Bureaucratically, clear guidance about responding to cyber attacks could facilitate rapid responses in a crisis and prevent dangerous delays that place the security of member states at risk. While individual NATO member states are capable of acting quickly, NATO as an institution, like many institutions, works more slowly. Having preset procedures in place to govern the response to a cyber attack could help NATO members effectively coordinate in a crisis.

#### Turns the case---redlines embolden cyber adversaries by boxing NATO into a corner---collapses Article 5 credibility.

Z’hra M. Ghavam 16. Lieutenant Commander, United States Navy; B.S., United States Naval Academy, 2007. MA Thesis in Security Studies Europe and Eurasia. “NATO’s Preparedness For Cyberwar.” https://calhoun.nps.edu/bitstream/handle/10945/50552/16Sep\_Ghavam\_Zhra.pdf?sequence=1&isAllowed=y

NATO’s publicly declared policy on cyber threats is consciously and purposefully vague.207 Why? Strategic ambiguity has its benefits. According to the Atlantic Council panel, there is no “redline” or “determined threshold” that would automatically define a cyber act as an act of war.208 Leaving the rules undefined affords NATO ample room in which to operate. For a 28-member multinational organization that operates on the principle of consensus, time and latitude for solidifying strategic-level decisions are critical. If NATO publicized a cyber redline, it would box the Alliance into a corner. This kind of policy could embolden cyber offenders and provoke massive intrusions that target NATO’s networks at just below this threshold. Having a defined redline could also invite nefarious cyber actors to cross it to test NATO’s resolve, damage its reputation as a leader in Euro-Atlantic security, and undermine the credibility of its Article 5 commitments.

#### The plan results in attacks under the threshold.

Warwick Ashford 14. Senior analyst @ Kuppinger Cole. "NATO to adopt new cyber defence policy". . 9-3-2014. https://www.computerweekly.com/news/2240228071/Nato-to-adopt-new-cyber-defence-policy

“The new cyber policy has already been endorsed by Nato’s 28 member countries, and I have no doubt the heads of state and government will do the same,” said Jamie Shea, Nato deputy assistant secretary general for emerging security challenges.

“For the first time we are making an explicit link in this policy between cyber attacks at a certain threshold and the invocation of a Nato article 5 collective defence as part of the treaty,” he told Computer Weekly.

Article 5 of the North Atlantic treaty requires member states to come to the aid of any member state subject to an armed attack, which includes cyber attack in the new cyber defence policy.

But at what threshold collective defence will be triggered, and how this threshold will be measured, will remain secret as a form of deterrent.

“We are keeping that ambiguous so a potential aggressor does not get the idea they can carry out cyber attacks up to a certain level with impunity,” said Shea.

#### Ambiguous Article 5 is key

Mustafa Canbolat 16. Canbolat is a 1st Lieutenant in the Turkish Army and has a B.S from the Turkish Military Academy. “Is NATO Ready for a Cyberwar?” Naval Postgraduate School, https://www.hsdl.org/?view&did=810939

NATO’s collective defense role against cyber threats is a difficult topic due to its complexity. However, NATO needs to defend itself and its members in every domain including the cyber. Therefore, letting adversaries know that Article 5 could be invoked in case of a serious cyber-attack is a significant policy and resolution in the alliance’s cyber defense. Jones (2015) summarizes the actions that NATO should take to build a better collective defense against cyber threats and have effective and reliable Article 5 execution in order to deter the adversaries very well. First, he states that “as part of its cyber defense program, NATO should establish an early warning system that lets the alliance and its members know when an attack is happening within enough time to stop it” (p. 45). This would give the alliance a further notice before a cyber-attack leads to a cyber conflict. Second, “NATO’s deterrence strategy should focus more on denial” (p. 45), because deterrence by denial will result in adversary’s abandonment of the action, and threat of punishment is not effective due to the attribution problems. Third, “NATO and its allies should encourage information sharing among its member nations and within the alliance itself” (p. 45) because transparency is one of the most significant aspects of a successful cyber defense for the Alliance. Fourth, “NATO needs to hire or train a team of experts in hacking, computer forensics, and cyber defense to aid its own organization and come to the aid of member countries that have experienced a breach in their security networks” (p. 47). Therefore, cooperation and information sharing is one of the most significant and essential assets in fighting against the cyber threats to defend the alliance in the cyber realm. Finally, “NATO should maintain ambiguity for justifying an Article 5 response in order to ensure that NATO can act when justified” (p. 45). This could give NATO flexibility and windows of opportunity when evaluating a cyber-attack and attributing it to an adversary.

### XT---1NC 3---Draw In

#### The plan draws NATO into wars.

James A Lewis 11. Senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies (CSIS), where he writes on technology, security and the international economy. Before joining CSIS, he worked at the Departments of State and Commerce as a Foreign Service Officer and as a member of the Senior Executive Service. "Cyberwar Thresholds and Effects."IEEE Security & Privacy, vol. 9, no. 5, pp. 23-29, Sept.-Oct. 2011. https://ieeexplore-ieee-org.proxy.library.emory.edu/document/5719593

This threshold question is important for decisions regarding collective defense. The exploits against Estonia, for example, didn't trigger the formal commitment under NATO's Article 5, in which an armed attack against one is considered an armed attack against all. [6] Article 5 and its emphasis on the use of force has shaped Western attitudes on warfare and defense for 60 years, and NATO nations will need to carefully consider how to extend its application to cyberspace. The attacks on Estonia were intended to intimidate and punish but not to create damage. Lowering the threshold so Estonia-like incidents qualify as the use of force could have some deterrent effect against state opponents, but it could also be destabilizing, as many nonstate groups and even individuals could launch similar denial-of-service exploits (but nothing more damaging), and a forceful reaction by defenders, even against the right target, could result in overreaction and increased tension.

#### Escalates and causes more election hacking.

Jack Goldsmith 16. Jack Goldsmith is the Learned Hand Professor at Harvard Law School, co-founder of Lawfare, and a Senior Fellow at the Hoover Institution. Before coming to Harvard, Professor Goldsmith served as Assistant Attorney General, Office of Legal Counsel from 2003-2004, and Special Counsel to the Department of Defense from 2002-2003. "The DNC Hack and (the Lack of) Deterrence". Lawfare. https://www.lawfareblog.com/dnc-hack-and-lack-deterrence

The Sanger and Perlroth piece reviews the unattractive options the United States has to respond to the DNC hack. The name and shame strategy has no chance of working with the Russians, and would be a laughable and self-defeating response to election-related intrusions. Something more aggressive—like a cyber or kinetic attack of some sort against Russia—runs the risk of serious escalation, including serious escalation by the Russians to further interfere in the U.S. election. Morell proposes instead “deep sanctions on the entire Russian economy” and an “aggressive Voice of America program in Russian to tell the Russian people that Putin is only interested in his own aggrandizement.” Can the United States coordinate effective deeper sanctions against Russia? Would the VOA strategy change the minds of the Russian people? I think these responses would not work in the first instance. But the important point is that the USG must, and does, think about the Russian response to any of these tactics. And if (as seems likely) Russia is willing to raise the stakes in cyber in response, the U.S. probably has much more to lose than win by ratcheting things up. And so the USG responds with uncertainty and weakness, thereby emboldening adversaries in a cycle that has been repeating itself, to our detriment, for years.

The tepid U.S. response to cyber intrusions may be surprising to some, since the USG possesses the greatest offensive cyber capabilities on the planet, which it often deploys for cyber-exploitation and cyber-attacks and, one can guess, for information operations of various kinds. Here we come to the crux of the matter. For two basic reasons, the USG is not willing to use these tools, or its redoubtable kinetic tools, to redress fully the very serious cyber-operations by adversaries inside U.S. networks. First, our adversaries have a wide array of sophisticated digital weapons that they are willing and able to use to harm or exploit porous and poorly defended U.S. networks. And second, the United States is by far more dependent on digital networks and the digital economy than any other nation in the world, and thus has the most to lose from any escalation related to cyber. As Sanger and Perlroth put these points: “Well-armed cyberpowers face few limits to their ability to escalate attacks. And it is unclear how the United States can establish what the generals call ‘escalation dominance’ — the assurance that America can ultimately control how a conflict ends.”

#### It escalates.

Warwick Ashford 13. Senior analyst. "Cyber attack retaliation a bad idea, says international panel". ComputerWeekly. 9-27-2013. https://www.computerweekly.com/news/2240206279/Cyber-attack-retaliation-a-bad-idea-says-international-panel

Retaliatory cyber attacks are not a good idea, an international panel has told attendees of a joint session of the ASIS International and (ISC)2 2013 annual congresses in Chicago.

Although security practitioners' ability to trace the source of cyber attacks is improving, they said it is seldom possible to do this with total certainty, particularly in the most sophisticated attacks.

But even where attribution is possible, retaliation is not good because it typically leads to an escalation of attacks and an increase in complexity, said Scott Borg, chief of the US Cyber Consequences Unit.

“We already know attackers are able to dodge every defence trick and, as we get better at attribution, attackers will go to increasingly sophisticated methods, and then we are in trouble,” he said.

Dave Tyson, senior director of global information security at SC Johnson & Son, said that, when eBay sought to take action against someone selling eBay fraud kits, he went after the company with all he could.

“It took eBay a lot of time, effort and money to put this guy in jail,” Tyson said.

Global collateral damage

Unintended consequences and collateral damage mean extreme care and caution need to be exercised when considering retaliatory attacks, said Hord Tipton, executive director of (ISC)2.

Crawford Samuel, project leader at the International Cyber Security Protection Alliance (ICSPA), said retaliatory attacks could have a global effect and consequences.

### XT---1NC 4---Attribution

#### Attribution fails---tanks deterrence.

Michael Horowitz 10. Assistant professor of political science at the University of Pennsylvania and a senior fellow at the Foreign Policy Research Institute. He has also held fellowships at the Olin Institute for Strategic Studies at Harvard, the Belfer Center for Science and International Affairs at Harvard, and the Weatherhead Center for International Affairs at Harvard. “A Common Future? NATO and the Protection of the Commons”. Transatlantic Paper Series No. 3 October 2010. https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/Trans-Atlantic\_Papers\_3-Horowitz.pdf

Cyberspace is also a realm where traditional notions of deterrence may break down. Deterring a threat by issuing counter-threats to deliver a devastating response to any cyber attack against the United States and its NATO allies may seem like an attractive solution to the cyber security challenge. The high costs associated with defending networks from cyber intrusions and the relatively low costs of launching a cyber attack have led many to analogize cyber deterrence to nuclear deterrence.31 However, cyber attacks lack the stable footprint of conventional military forces. The fact that terrorist attacks do not leave a “return address” is accentuated in the case of cyber warfare. In the case of a cyber attack, for example, even tracking down the specific computer from which an attack was launched might not give the attacked country sufficient information to distinguish whether a country, terrorist group, or rogue individual launched an attack from that particular computer. These concerns, in part, are why U.S. Deputy Secretary of Defense William Lynn recently stated that denying adversaries access to U.S. information systems in the first place, rather than planning to retaliate in case of an attack, encompasses the bulk of U.S. defensive efforts.32 The United States and its NATO partners must invest heavily in defending their networks from intrusion and cannot be confident that maintaining nascent retaliatory capabilities will suffice to deter attacks. Furthermore, while strong cyber ties between NATO members might not ensure that deterrence succeeds, weak cyber ties will almost certainly encourage adversaries to launch more cyber incursions against NATO members.33 Finally, since many future wars will likely include major cyber components, thinking about cyberspace as a very separate sphere of warfare delinked from other areas of conflict is counterproductive.34

#### Adversaries can conceal attacks.

James A. Lewis 09. Center for Strategic and International Studies. The “Korean” Cyber Attacks and Their Implications for Cyber Conflict. October 2009. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy\_files/files/publication/091023\_Korean\_Cyber\_Attacks\_and\_Their\_Implications\_for\_Cyber\_Conflict.pdf

Cyberspace enables anonymous attacks. Identities are easily concealed or fabricated in cyberspace, and an astute opponent will of course make it look as if another was responsible for an attack. The use of botnets complicates attribution - the source of an attack, at the first iteration, will be innocent and unknowing third parties. Forensic work may eventually reveal the source of an attack, but a sophisticated opponent will be able to operate clandestinely and with a high degree of deniability. The “Confickr” worm is a good example of this difficulty. Confickr was a global malware that infected millions of computers.1 Many companies and governments made a coordinated effort to fend it off, but we still have no idea who launched Confickr, what their intent was, or even whether it has been removed from all infected systems.

#### Attribution and collateral damage zero solvency.

James A. Lewis 09. Center for Strategic and International Studies. The “Korean” Cyber Attacks and Their Implications for Cyber Conflict. October 2009. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy\_files/files/publication/091023\_Korean\_Cyber\_Attacks\_and\_Their\_Implications\_for\_Cyber\_Conflict.pdf

Weak attribution and unpredictable collateral damage make deterrence ineffective in cyberspace. Deterrence is a threat of retaliation, but it is hard to credibly threaten unknown parties and counterproductive to threaten or damage the wrong party. The United States is widely recognized to have pre-eminent offensive cyber capabilities, but it obtains little deterrent effect from this.

In the absence of attribution, the response options for the United States to the July 4 events were extremely limited. We could not retaliate against an unknown attacker. Deterrence is the threat of violent retaliation. This threat changes the opponent’s calculus of the benefits and costs of an attack. But it is hard to convincingly threaten an unknown attacker, and weak attribution makes traditional deterrent concepts – those based on the threat of reprisal for an attack (either counterforce or countervalue) – largely irrelevant in cyberspace.

#### Attribution makes cyber deterrence impossible.

Myriam Dunn Cavelty 12. ETH Zurich - Center for Security Studies. Cyber-Allies: Strengths and Weaknesses of NATO’s Cyberdefense Posture IP Global Edition, Vol. 12/3, pp. 11-158, 2011 5 Pages Posted: 2 Feb 2012 . <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997153>

The main reason behind this was likely a desire to maximize the deterrent effect of the Alliance in the cyberdomain. However, the cyberdomain poses considerable deterrence limitations. Deterrence works if one party is able to successfully convey to another that it is both capable and willing to use a set of available (military) instruments in retaliation if the other crosses a line. But for this to work, the opponent should first, be a state, and second, be identifiable as an attacker. While states can be behind some cases of cyberincidents (they are not usually the culprits), attackers do not have to fear retaliation, since they can likely remain anonymous if they choose. It is particularly tricky to identify actors in a timely manner due to frequent time lapses between the action that an perpetrator takes, the intrusion itself, and the effects of the intrusion. And even if one or several perpetrators could be identified certainly—proving that a state actor (or a terrorist organization) had coordinated their actions would be the next difficulty.

### XT---1NC 5---No Cyber Impact

#### Countries are already deterred from cyber---no stand alone conflicts

James A. Lewis 09. Center for Strategic and International Studies. The “Korean” Cyber Attacks and Their Implications for Cyber Conflict. October 2009. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy\_files/files/publication/091023\_Korean\_Cyber\_Attacks\_and\_Their\_Implications\_for\_Cyber\_Conflict.pdf

Absent such larger conflict, however, a nation-state is no more likely to launch a serious cyber attack than they are to shoot a random missile at an opponent.9 The risk is too great and the benefits of a cyber attack by itself too small for political leaders to authorize the use of this capability in anything short of a situation where they had already decided on military action. Cyber weapons are not decisive; cyber attack by itself will not win a conflict, particularly against a large and powerful opponent. It is striking that to date; no cyber "attack" that rises above the level of espionage or crime has been launched outside of a military conflict.

Even in a conflict, a decision to strike civilian targets in an opponent’s homeland using cyber weapons is a major step that brings the risk of serious escalation. Engaging American military forces overseas is not the same as attacking critical infrastructure in the United States. Nations may reserve these serious cyber attacks against targets in the opponent’s homeland for either retaliation for attacks against their own homeland or for when they are in extremis.

### XT---1NC 7---Private Sector

#### Defending the private sector is impossible---attempts overstretch the alliance and shred credibility

Todd Rosenblum 16. Former Acting Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs. "NATO and Cyberwar Strategy: Proceed with Caution". Cipher Brief. https://www.thecipherbrief.com/column\_article/nato-and-cyberwar-strategy-proceed-with-caution

For example, attacks against domestic critical infrastructure constitute an unrefined and hugely expansive mission space. Should it be an alliance military mission? Should this come under NATO’s security umbrella? Expanding Article V protections to attacks against private sector operations may seem logical to some, but NATO should proceed with great caution before promising its security umbrella to cyber homeland security and resiliency. Asserting protection and response to attacks in this area, over-states NATO’s capacities and undermines alliance credibility.

There are a host of reasons why NATO must confine its ambitions to government network defense and response, and rethink whether domestic infrastructure protection really is – or should be – part of its writ.

First among the reasons is that the private sector owns and operates the vast majority of critical infrastructure and may not want NATO or even their own government’s help. The private sector has its own diverse perspectives, and the crisis management links between government and the private sector simply do not exist. Calling this a NATO mission makes essential coordination with the private sector exponentially harder. Differing national laws and ethos that define government–private sector cooperation makes it nearly impossible.

NATO members, like so many national governments, continue to minimize the reality that the private sector is at least as central as governments in cyber crisis management and response. Unlike traditional armed conflict, deterrence and crisis management is a joint venture with the private sector, no matter how often governments think they will be the tip of the spear.

The private sector is not only a co-equal branch in cyber crisis management but has different stakes than governments and multinational alliances. Information technology and other major companies are borderless, and responsive to global stakeholders and financial markets. Their interests often do not align with those of governments, and certainly not major military alliances. The private sector generally has superior capabilities than governments. Its decisions about what to do, when to do it, and how to do it, will take government views into account but will not be beholden to them.

Revisiting North Korea’s repeated attacks against Sony America’s networks throughout 2014 highlight how different and difficult crisis management is in the domestic digital domain. NATO will do well to remember how complicated this event was for the United States national security apparatus.

In brief, the North Korean state attacked the digital data stores of the American subsidiary of a Japanese company. The key actors through most of the crisis were all in the private sector, and Sony responses were framed more by the actions of its rivals and business partners in industry than anything said or done by government. Not surprisingly, individual business interests outweighed common cause. Private sector unity was not possible.

Of course the U.S. government played an important role late in the crisis when President Obama declared there to be a national interest in the situation and imposed sanctions on the North Korean state. But the central point is that critical decisions were made by the private sector, based on business needs, damage assessments, and capabilities.

Government was not able to manage this major crisis even though it involved a nuclear weapon state threatening physical strikes in the U.S. homeland. Events since, such as Apple’s refusal to cooperate with a court order to assist the government in accessing encrypted information on a terrorist’s iPhone, reinforces the reality that the relationship between government and industry is getting more distant, not closer. Apple probably would be even less likely to cooperate with a 28 nation military alliance than with its “home” government.

Just imagine how complex it would be for a 28 nation military alliance to assert response dominion against digital attacks by a known adversary against the networks controlling a member’s key infrastructure. What if the company(s) involved had deep business interests in the adversary nation and refused to work with the alliance in fashioning a response? What if its business interest compelled accommodation? What if it did not want to share its essential capabilities with government (or a large military alliance) fearing doing so would be a competitive disadvantage?

National security officials across the globe struggle with the idea that the private sector is not subservient to government in protecting their information technology interests and often is just as capable as government in intelligence gathering and response planning. Cohesion between the two worlds is not likely unless the private sector becomes an essential actor in this element of national security decision making space.

This is not to say industry can operate alone. Industry has many dependencies on government. Only governments can set laws and press treaty enforcement between states. Industry relies on government to provide emergency response assistance if digital strikes have a physical effect, such as a major power outage. Governments often hold key bits of information that can complete the operating picture environment.

The shared dependency between government and the public sector provide opportunity to remake decision-making processes heretofore made solely by government actors. Until we make more headway remaking these processes, NATO would be wise to constrain its ambitions to defending its own networks and improving its operational resiliency. It should set aside planning to protect and respond to digital strikes against privately owned domestic critical infrastructure.

NATO has more than enough challenges ensuring its communications integrity and updating war plans to fully accommodate for fighting in the digital domain. Let’s leave the hornet’s nest of what the alliance should do in response to attacks on domestic infrastructure and private companies to a more settled period.

### XT---1NC 8---No Democracy Impact

#### No democratic peace

Jeff Grabmeier 15. Senior Director, Research communications, Media & PR "'Democratic peace' may not prevent international conflict". No Publication. 9-3-2015. https://phys.org/news/2015-09-democratic-peace-international-conflict.html

Using a new technique to analyze 52 years of international conflict, researchers suggest that there may be no such thing as a "democratic peace."

In addition, a model developed with this new technique was found to predict international conflict five and even ten years in the future better than any existing model.

Democratic peace is the widely held theory that democracies are less likely to go to war against each other than countries with other types of government.

In the new study, researchers found that economic trade relationships and participation in international governmental organizations play a strong role in keeping the peace among countries. But democracy? Not so much.

"That's a startling finding because the value of joint democracy in preventing war is what we thought was the closest thing to a law in international politics," said Skyler Cranmer, lead author of the study and The Carter Phillips and Sue Henry Associate Professor of Political Science at The Ohio State University.

"There's been empirical research supporting this theory for the past 50 years. Even U.S. presidents have touted the value of a democratic peace, but it doesn't seem to hold up, at least the way we looked at it."