CYBER AFFIRMATIVE—HARVARD DEBATE WORKSHOP

Table of Contents

[1AC—Plan + Russia Advantage 2](#_Toc107571906)

[Aff—Case—Emerging Tech Add-On 14](#_Toc107571907)

[Aff—Case—Extend: Strategic Ambiguity Fails 16](#_Toc107571908)

[Aff—Case—Extend: Russian Cyberattacks 20](#_Toc107571909)

[Aff—Case—Extend: Solvency 23](#_Toc107571910)

[Neg—AT: Cyber Aff—Deterrence Turn—1NC 25](#_Toc107571911)

[Neg—AT: Cyber Aff—Deterrence Working Now—1NC/2NC 26](#_Toc107571912)

[Neg—AT: Cyber Aff—Deterrence Turn—2NC 28](#_Toc107571913)

[Neg—AT: Cyber Aff—Impact Defense—1NC 30](#_Toc107571914)

[Neg—AT: Cyber Aff—Impact Defense—2NC 33](#_Toc107571915)

### 1AC—Plan + Russia Advantage

#### The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization in the area of cyber, by defining proportional response and increasing interoperability.

#### Russian cyberattacks are inevitable post-Ukraine, and current policy of strategic ambiguity fails at deterrence. This undermines NATO’s credibility and unity, which imperils the alliance. Refining cyber policy is key.

Erica D. Lonergan & Sara B. Moller 4/27—Assistant professor in the Army Cyber Institute and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University; former Eisenhower Fellow at the NATO Defense College. ("NATO’s Credibility Is on the Line with its Cyber Defense Pledge. That’s a Bad Idea." March 27, 2022, from POLITICO, https://www.politico.com/news/magazine/2022/04/27/nato-credibility-cyber-defense-pledge-russia-ukraine-00027829)

President Joe Biden has issued grave warnings that Russia might launch a cyberattack against the United States in retaliation for the punishing sanctions levied after Moscow’s invasion of Ukraine. He’s advised American companies to “accelerate efforts to lock their digital doors,” and many officials expect an attack against critical U.S. infrastructure to be inevitable.

One way Biden and other Western leaders are attempting to deter potential Russian cyber retaliation during the Ukraine crisis is through NATO’s Article 5 collective defense pledge — that an attack on one is an attack against all. That’s because since the 2014 NATO summit in Wales (which, coincidentally, took place following another Russia-Ukraine crisis), the alliance has affirmed that Article 5 extends to cyberspace. In other words, a cyberattack against any NATO member could conceivably represent an attack against the entire alliance. The pledge is the embodiment of the allies’ security guarantee to each other and the beating heart of NATO.

After Russia invaded Ukraine, NATO Secretary General Jens Stoltenberg confirmed that NATO policy on collective defense and cyberspace holds strong, noting that NATO has “decided to make clear that a cyberattack can trigger Article 5.” And following an extraordinary meeting of heads of state and government on March 24, the alliance reinforced that it is “ready to impose costs on those who harm us in cyberspace.”

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.

Such a shift might face some initial resistance, particularly in light of the Kremlin’s history of malicious cyber activities. One of the first state-initiated cyberattacks was perpetrated by Russia against Estonia, a NATO member, in 2007. In the intervening years, Moscow has increased its malicious cyber activities, such as the SolarWinds breach uncovered in December 2020 in which Russia gained access to a treasure trove of U.S. data. Russian President Vladimir Putin’s maneuvers against NATO members, along with the annexation of Crimea in 2014, spurred the alliance to adopt a Cyber Defense Pledge in 2016 that recognized cyberspace as a military domain. Two years later, NATO created a Cyberspace Operations Center in Mons, Belgium to improve situational awareness and coordinate cyber operations. Since then, the alliance has consistently reaffirmed the application of Article 5 to cyberspace. At the 2021 summit in Brussels, NATO committed to a new Comprehensive Cyber Defense Policy, with allies agreeing to employ the “full range of capabilities” at all times to “deter, defend against, and counter the full spectrum of cyber threats.”

Notably, NATO refined its language with last summer’s summit communique to account for the fact that some cyber incidents may not be individually decisive, but nevertheless significant when viewed in the aggregate. Specifically, the allies recognized “the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack.” In practice, however, NATO leaders have avoided clarifying the conditions under which a cyberattack would trigger Article 5 and how NATO would respond. When pressed about Russian cyberattacks in the Ukraine context, Stoltenberg cautioned that, “we have never gone into the position where we give a potential adversary the privilege of defining exactly when we trigger Article 5.”

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.

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

#### NATO needs to present a multilateral front to deter Russia—otherwise, they’ll devastate the grid

Dina Aldanova 5/30—Master’s Candidate at Georgetown University’s Eurasian, Russian, and East European Studies Program. ("Will Russia Launch a New Cyber Attack on America?" May 30, 2022, from National Interest, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/will-russia-launch-new-cyber-attack)

Nevertheless, cybersecurity experts speculate on a range of consequences in a worst-case cyber scenario: Russia might attempt to attack U.S. critical infrastructure, turn off the lights, target the operation of ATMs and credit card systems, attack Amazon’s cloud, disrupt the transportation and supply of clean water, and target pharmaceuticals companies’ manufacturing facilities, power grids, and colonial pipelines. But will such a threat manifest?

Not only would a cyberattack against the United States contradict the historically peripheral nature of Russian cyber warfare, but Russia’s cyber capacity would be insufficient for the task. For the past several years, the West has largely overestimated Russian military capabilities in conventional warfare. U.S. intelligence agencies predicted the 2022 war in Ukraine would be the most destructive the European continent has seen since the end of World War II, expecting the fall of Kyiv to come within days. However, the still ongoing, drawn-out war has revealed weaknesses in the Russian armed forces, its military arsenal, and strategic leadership. Russian officials, for their part, underestimated the strength of the Ukrainian resistance and the united position of the international community. Spending slightly more than 4 percent of the country’s GDP on the military, the Russian president mobilizes domestic support for the military budget by articulating the external threat of NATO. In a relatively undigitized society like Russia, lobbying to spend more on the cyber budget would prove less effective. Taking this into account, it seems possible the West could be overestimating Russian cyber competence as well.

Furthermore, Russia is unlikely to wage a cyberattack on the United States due to fear of retaliation on multiple fronts. Russian society is already experiencing the consequences that the war has wrought: an economic crisis and the psychological pressure of being cast as a global pariah. In case of a Russian cyberattack, the consequences of U.S. cyber retaliation would hit the public first. Given current conditions, depriving people of water and electricity could trigger public discontent on an unprecedented scale. Decades of increasingly authoritarian leadership have undoubtedly engendered public grievances hidden deep within society. At some point, this simmering disgruntlement can boil over into outrage. Putin can ill afford to front further domestic unrest now.

Current U.S. cyber capabilities could also contribute to the fear of retaliation. For the past few years, the United States has developed an impressive cyberinfrastructure, restructured its system of governance, and invested in cyber training and education. As Richard Clarke and Robert Knake emphasize in their book, The Fifth Domain, following the Cold War strategy of deterrence and containment, the United States has largely restrained itself from involvement in cyber counter activities. Although for a long time America has focused on defensive cyber policy, today, the U.S. Cyber Command prioritizes offensive measures. As such, in 2019, the United States successfully targeted the Iranian intelligence service and missile launch system as a response to an Iranian strike against an American drone and U.S. oil tankers. Earlier in 2012, the Stuxnet computer worm, designed in cooperation with Israel, successfully infiltrated nuclear facilities in Iran.

In addition to an offensive preference, a more consolidated system of governance and a set of regulations have advanced U.S. cybersecurity. A clear allocation of roles and responsibilities between the Department of Homeland Security and U.S. Cyber Command and the relevant leadership improved the system of reporting incidents and information sharing. It facilitated communication within federal agencies and between the government, the private sector, and the public. U.S. private enterprises now spend billions of dollars on cybersecurity, employee training, and encrypted channels. The United States also takes a leading role in collaborating with strategic allies on sharing best practices, detecting flaws in networks, and promoting cyber hygiene.

International cooperation to this degree is not an asset that Russia benefits from. With the support of NATO Cooperative Cyber Defense Center of Excellence’s research and development projects, expertise, and training, U.S. retaliation to a potential Russian cyber attack could be not only detrimental but even more profound as a multilateral response. Based on all this, the fear of retaliation could indeed prevent Putin from engaging in offensive cyber operations against the United States.

Finally, Putin has lost the upper hand in launching an attack by surprise. For instance, Russia invaded Georgia during the Olympics Games in Beijing in 2008, and Ukraine during the Sochi Winter Olympics in 2014. When Putin waged war on Ukraine in 2022—incidentally, immediately following the Beijing Winter Olympic Games—the West anticipated it. Putin invaded Ukraine anyway. He is unlikely to act recklessly in this way again, considering the failures the Russian military has experienced since the invasion. Furthermore, knowing that the United States and European allies have shielded up, Putin has no incentive to strike. Nevertheless, would Putin wait for a more favorable moment? Or scale back a potential attack, for instance, by meddling in the U.S. midterm elections in November?

It would be misleading, however, to underestimate Russian cyber capabilities or Putin’s mind games and lose vigilance. In 2020, despite denying its involvement, Russia evidently hacked U.S. software company SolarWinds. By installing malware into the company’s updated Orion software program, the attack affected thousands of customers, a hundred companies such as Microsoft and Intel, and some federal agencies like the Treasury Department, the Pentagon, and the Cybersecurity and Infrastructure Security Agency. Cyber experts acclaimed the code used as phenomenal. More astonishingly, if not for a performance assessment and proper investigation, the attack could have easily gone unnoticed. For over six months, Moscow tracked emails and other traffic of sensitive information. Could there already be a similar malware in U.S. networks?

Now, on the brink of a new Cold War, the United States must keep its guard up on cybersecurity. Although there are significant factors that challenge the probability of an imminent Russian cyber-retaliation, the United States should not disregard the potential for malicious activity in the near future. It needs to keep a sober view and not act hastily. Setting priorities for the long run, the United States needs to continue advancing cyber mechanisms that detect sensitive activity like the Solar Winds hack, and invest more in training and education about cyber hygiene for government agencies, private companies, and the public. It should not neglect to regularly test offline backups, run software updates, report incidents, use multifactor authentication, block unusable domain IP addresses, and assess third-party risks.

Although Putin’s intentions are far from clear, his decision to pursue a cyberattack on the United States’ critical infrastructure that would instantly shut down electricity or disrupt clean water supply, the offense might come unexpectedly, and soon. Cornered with sanctions and burdened by the bitterness of defeat, Putin might act furiously. The United States and Western allies need to be vigilant and maintain strong lines of communication about any malicious activity. With a strong multilateral front in the West, Russia will have fewer incentives to engage in cyber warfare.

#### But absent cooperation, allies will disagree and lack an effective, uniform response

Jackson 16—Received his juris doctor degree from George Mason University School of Law and is currently a Research Associate at the Center for Infrastructure and Protection at the George Mason University School of Business (Stephen, 8/16/2016, “NATO Article 5 and Cyber Warfare: NATO’s Ambiguous and Outdated Procedure for Determining When Cyber Aggression Qualifies as an Armed Attack”, George Mason 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/>)

Article 5 is useful for assessing state and non-state actions used in traditional warfare. However, the NATO allies drafted Article 5 in light of the technology and tactics of the World War II era. While NATO continued to successfully adapt Article 5 to the evolving challenges post-Soviet Union, it cannot properly invoke the principle of collective self-defense against cyber attacks without at least new definitions for the various forms of cyber events. In particular, without unambiguous guidelines for identifying from where a cyber attack originated, NATO will face difficulty in both locating the origin of a cyber attack and determining whether the cyber attack was sanctioned by the host nation. Also, without proper definitions for the various forms of cyber attacks, NATO will likely encounter unnecessary debate between NATO allies over any cyber attack against a NATO country. Furthermore, without removing ambiguity in identifying cyber events that equate to a traditional armed attack, the North Atlantic Council will face difficulty in deciding upon a proper and proportionate armed response in accord with the principles of jus in bello.

Currently, almost every NATO ally has an individual national security and defense strategy related to cybersecurity.[12] These strategies vary in detail and scope, and lack uniformity in defining the elements of which cyber attacks warrant an aggressive response. Some scholars argue that the International Court of Justice accurately determined that collective self-defense is triggered when an act “inflicts substantial destruction upon important elements of the target state,” even if the attackers used non-traditional weaponry like airplanes or cyber attacks.[13] For instance, this “scale and effects” test does not adequately address the technical differences between using cyberspace to create either a kinetic disruption to a power plant or the potential to dismantle an entire financial infrastructure with zero physical effects. The potential for a single cyber attack to result in major disturbance, with or without any physical element, is sufficient to warrant specific guidelines. However, as long as the North Atlantic Council assesses individual cyber attacks on a case-by-case basis without predetermined specialized rules, the various interests of all 28 NATO nations will pose obstacles for a swift and efficient NATO response.

#### Russia will gradually escalate and use cyber as a pretext for military force. This fractures NATO, feeds misperceptions, and sparks nuclear war

Fisher 15—Foreign policy editor at Vox (Max, 6/29/2015, “How World War III became possible”, Vox, <https://www.vox.com/2015/6/29/8845913/russia-war#hybridwar>)

This poll is even worse than it looks. It assumes that Russia would launch an overt military invasion of the Baltics. What would actually happen is something far murkier, and far more likely to leverage European hesitation: the playbook from Ukraine, where Russia deployed its newly developed concepts of postmodern "hybrid war," designed to blur the distinction between war and not-war, to make it as difficult as possible to differentiate grassroots unrest or vigilante cyberattacks from Russian military aggression.

Putin may already be laying the groundwork.

In March of 2014, shortly after Russia had annexed Crimea, Putin gave a speech there pledging to protect Russians even outside of Russia, which many took as a gesture to the substantial Russian minorities in the Baltics.

Then, in October, Putin warned that "open manifestations of neo-Nazism" had "become commonplace in Latvia and other Baltic states" — repeating the language that he and Russian state media had earlier used to frighten Russian speakers in Ukraine into taking up arms.

This April, several Russian outlets issued spurious reports that Latvia was planning to forcibly relocate ethnic Russians into Nazi-style ghettos — an echo of similar scaremongering Russian propaganda broadcast in the runup in Ukraine.

Martin Hurt, a former senior official of the country's defense ministry, warned that his country's ethnic Russian minority could be "receptive to Kremlin disinformation." Moscow, he said, could generate unrest "as a pretext to use military force against the Baltic states."

In early 2007, Estonia's parliament voted to relocate a Soviet-era military statue, the Bronze Soldier, that had become a cultural symbol and annual rallying point for the country's ethnic Russians. In response, Russian politicians and state media accused the Estonian government of fascism and Nazi-style discrimination against ethnic Russians; they issued false reports claiming ethnic Russians were being tortured and murdered. Protests broke out and escalated into riots and mass looting. One person was killed in the violence, and the next day hackers took many of the country's major institutions offline.

Russia could do it again, only this time gradually escalating further toward a Ukraine-style conflict. NATO is just not built to deal with such a crisis. Its mutual defense pledge, after all, rests on the assumption that war is a black-and-white concept, that a country is either at war or not at war. Its charter is from a time when war was very different than it is today, with its many shades of gray.

Russia can exploit this flaw by introducing low-level violence that more hawkish NATO members would consider grounds for war but that war-averse Western European states might not see that way. Disagreement among NATO's member states would be guaranteed as they hesitated over where to declare a moment when Russia had crossed the line into war.

Meanwhile, Russian state media, which has shown real influence in Western Europe, would unleash a flurry of propaganda to confuse the issue, make it harder to pin blame on Moscow for the violence, and gin up skepticism of any American calls for war.

Germany, which is widely considered the deciding vote on whether Europe would go to war, would be particularly resistant to going to war. The legacy of World War II and the ideology of pacifism and compromise make even the idea of declaring war on Russia unthinkable. German leaders would come under intense political pressure to, if not reject the call to arms, then at least delay and negotiate — a de facto rejection of NATO's collective self-defense.

In such a scenario, it is disturbingly easy to imagine how NATO's European member states could split over whether Russia had even crossed their red line for war, much less whether to respond. Under a fog of confusion and doubt, Russia could gradually escalate until a Ukraine-style conflict in the Baltics was foregone, until it had marched far across NATO's red line, exposing that red line as meaningless.

But the greatest danger of all is if Putin's plan were to stumble: By overreaching, by underestimating Western resolve to defend the Baltics, or by starting something that escalates beyond his control, it could all too easily lead to full-blown war.

"That kind of misperception situation is definitely possible, and that’s how wars start," Saideman said, going on to compare Europe today with 1914, just before World War I. "The thing that makes war most thinkable is when other people don’t think it’s thinkable."

In 1963, a few months after the Cuban missile crisis had almost brought the US and Soviet Union to blows, President John F. Kennedy gave a speech drawing on the lessons of the world's brush with nuclear war:

"Above all, while defending our vital interests, nuclear powers must avert those confrontations which bring an adversary to a choice of either a humiliating retreat or a nuclear war."

That is the choice that Putin may well force upon NATO.

#### Strategic ambiguity only *emboldens* Russian aggression, which they’ll use to exploit disunity in the alliance

Emilio Iasiello 17, cyber intelligence expert, leading teams at the Defense Intelligence Agency and the Department of State in strategic cyber intelligence production supporting national-level decision makers to include the Executive Office, the U.S. Congress, and senior civilian and military policymakers. NATO’s Cyber Operations Center – Will Russia Feel Threatened? <https://www.cyberdb.co/natos-cyber-operations-center-will-russia-feel-threatened/>, language edited change denoted by brackets

According to recent reporting, the North Atlantic Treaty Organization (NATO) announced that its Cyber Operations Center (COC) is expected to be fully staffed and functional by 2023. The new COC marks NATO’s understanding of the importance that cyberspace plays in conflict, particularly in times of political tensions that has resulted in cyber malfeasance that has targeted elections and critical infrastructure. The establishment of the COC is a natural evolution in how to address cyber attacks in a more timely manner by integrating cyber actions with more conventional military capabilities. In early 2014, after notable cyber incidents were a part of international incidents that occurred in Estonia in 2007 and Georgia in 2008, the Alliance updated its cyber defense policy to classify digital attacks as the equivalent of kinetic attacks under its collective security arrangement under Article 5 of the treaty. In those particular instances, Russia was suspected in orchestrating or at least tacitly supporting the cyber attacks that afflicted both states. Since then, Russia’s alleged cyber activities have only become more brazen in their scale and aggressiveness. From suspected involvement in launching cyber attacks against Ukrainian critical infrastructure to launching a variety of cyber operations to meddle in the elections of foreign governments, Russia has taken advantage of the uncertainty of cyberspace where there is little consensus on key issues such as Internet governance, cyber norms of state behavior, or the criteria by which cyber attacks escalate to a point of war.

NATO has always provided a strong military counterpoint to Russian influence in the European region and projecting a credible threat in cyberspace is an important complement to NATO capabilities. However, previously, NATO didn’t have any of its own cyber weapons, a significant problem given Russia’s perceived position of a near-peer level adversary of the United States. With the establishment of the cyber command, the United States, United Kingdom, and Estonia have offered the Alliance their cyber capabilities. As described in one news article, the alliance hopes to integrate individual nations’ cyber capabilities into alliance operations, coordinated through the COC and under the command of NATO’s top general. With this in hand, it will be interesting to see if this will serve as the deterrent it’s intended to be and how Russia may adjust their cyber activities, particularly against NATO member countries.

However, there is still the lingering problem the Alliance faces with regards to the rules of engagement. Classifying cyber attacks under Article 5 is a start but doesn’t help provide a path forward to how NATO can and should engage and respond to cyber attacks. While this provides NATO a certain flexibility in addressing cyber attacks allowing the Alliance to take each on a case-by-case basis in determining the extent of its response, it does not provide adversarial states an idea of tolerated and intolerable cyber activities. This shortcoming serves only to provide states like Russia enough wiggle-room to continue their offensive cyber operations as long as they don’t cross an undefined threshold. It’s long been hypothesized that attacks ~~crippling~~ [destroying] critical infrastructures would meet that threshold, but as seen in Ukraine, this bar keeps being pushed a little farther each time.

#### Russian grid attacks collapse US and European grids AND spark US nuclear retaliation

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

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

#### Grid collapse causes extinction

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

Consequences of a sustained power outage The EMP Commission states “Should significant parts of the electrical power infrastructure be lost for any substantial period of time, the Commission believes that the consequences are likely to be catastrophic, and many people will die for the lack of the basic elements necessary to sustain life in dense urban and suburban communities.” [67]. Space constraints preclude discussion on how the loss of the grid would render synthesis and distribution of oil and gas inoperative. Telecommunications would collapse, as would finance and banking. Virtually all technology, infrastructure, and services require electricity. An EMP attack that collapses the electric power grid will collapse the water infrastructure—the delivery and purification of water and the removal and treatment of wastewater and sewage. Outbreaks that would result from the failure of these systems include cholera. It is problematic if fuel will be available to boil water. Lack of water will cause death in 3 to 4 days [68]. Food production would also collapse. Crops and livestock require water delivered by electronically powered pumps. Tractors, harvesters, and other farm equipment run on petroleum products supplied by an infrastructure (pumps, pipelines) that require electricity. The plants that make fertilizer, insecticides, and feed also require electricity. Gas pumps that fuel the trucks that distribute food require electricity. Food processing requires electricity. In 1900, nearly 40% of the population lived on farms. That percentage is now less than 2% [69]. It is through technology that 2% of the population can feed the other 98% [68]. The acreage under cultivation today is only 6% more than in 1900, yet productivity has increased 50 fold [69]. As stated by Dr. Lowell L Wood in Congressional testimony: “If we were no longer able to fuel our agricultural machine in the country, the food production of the country would simply stop, because we do not have the horses and mules that used to tow agricultural gear around in the 1880s and 1890s”. “So the situation would be exceedingly adverse if both electricity and the fuel that electricity moves around the country……… stayed away for a substantial period of time, we would miss the harvest, and we would starve the following winter” [70]. People can live for 1–2 months without food, but after 5 days, they have difficulty thinking and at 2 weeks they are incapacitated [68]. There is typically a 30-day perishable food supply at regional warehouses but most would be destroyed with the loss of refrigeration [69]. The EMP Commission has suggested food be stockpiled for a possible EMP event. A prescription for failure Even if all the recommendations of the Congressional EMP Commission were implemented, there is no guarantee that the grid will not sustain a prolonged collapse. There should therefore be contingency plans for such a failure. There is also another consideration. The foundational pillars of prior American nuclear defense policy, in today’s climate, are of uncertain validity. Mutual assured destruction is the Maginot line of the 21st century. Nonproliferation will prove difficult to resurrect. The consequences of a widespread nuclear attack have been positioned to the public as massive deaths from blast effects, and then further lingering deaths from the effects of radiation. We suspect there will be no electricity, and there will be no electricity for a very long time. There should be an actionable plan in anticipation of a possible prolonged collapse of the grid—a retro-structure and a skill set to provide a framework for survival. Our sense is there is no plan.

#### US-Russia war causes extinction

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

The bombings of Hiroshima and Nagasaki demonstrated the unprecedented destructive power of nuclear weapons. However, even in an all-out nuclear war between the United States and Russia, despite horrific casualties, neither country’s population is likely to be completely destroyed by the direct effects of the blast, fire, and radiation.8 The aftermath could be much worse: the burning of flammable materials could send massive amounts of smoke into the atmosphere, which would absorb sunlight and cause sustained global cooling, severe ozone loss, and agricultural disruption – a nuclear winter.

According to one model 9 , an all-out exchange of 4,000 weapons10 could lead to a drop in global temperatures of around 8°C, making it impossible to grow food for 4 to 5 years. This could leave some survivors in parts of Australia and New Zealand, but they would be in a very precarious situation and the threat of extinction from other sources would be great. An exchange on this scale is only possible between the US and Russia who have more than 90% of the world’s nuclear weapons, with stockpiles of around 4,500 warheads each, although many are not operationally deployed.11 Some models suggest that even a small regional nuclear war involving 100 nuclear weapons would produce a nuclear winter serious enough to put two billion people at risk of starvation,12 though this estimate might be pessimistic.13 Wars on this scale are unlikely to lead to outright human extinction, but this does suggest that conflicts which are around an order of magnitude larger may be likely to threaten civilisation. It should be emphasised that there is very large uncertainty about the effects of a large nuclear war on global climate. This remains an area where increased academic research work, including more detailed climate modelling and a better understanding of how survivors might be able to cope and adapt, would have high returns.

It is very difficult to precisely estimate the probability of existential risk from nuclear war over the next century, and existing attempts leave very large confidence intervals. According to many experts, the most likely nuclear war at present is between India and Pakistan.14 However, given the relatively modest size of their arsenals, the risk of human extinction is plausibly greater from a conflict between the United States and Russia. Tensions between these countries have increased in recent years and it seems unreasonable to rule out the possibility of them rising further in the future.

#### Ambiguity entangles the US and allies with offensive action—increasing cyber cooperation and defining proportional response solves

Arts 18—Program coordinator supporting The German Marshall Fund of the United States’ (GMF) security and defense policy work in Washington DC, strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan (Sophie, December 2018, “Offense as the New Defense: New Life for NATO’s Cyber Policy,” GMF Policy Brief, No. 039, <https://nato-engages.org/wp-content/uploads/2019/04/Offense-as-the-New-Defense-New-Life-for-NATO%E2%80%99s-Cyber-Policy.pdf>)

Perhaps most importantly, as NATO stands ready to integrate defensive and offensive cyber operations, it should further clarify how these relate to its collective defense provision. Although NATO holds that Article 5 could be invoked following a “significant” cyberattack against one or more of the allies,46 officials have remained deliberately ambiguous when it comes to defining the parameters of a qualifying attack so as to discourage hostile operations that would fall just below such a specific threshold.47 Without a clear line, allies have more room to maneuver in a cyber crisis short of invoking Article 5. However, recent experience across the alliance has yielded little proof that the strategic ambiguity in this domain is effective in preventing hostile operations.

As NATO seeks to address this challenge, it will need to assess how to develop an effective cyber policy that balances deterrence with the potential risk for escalation. With this in mind, it should establish more precise thresholds for cyber-attacks and define proportional response scenarios.48 Without these, it will likely remain very challenging to mobilize allies to invoke Article 5 in a cyber crisis. This could be particularly difficult if a crisis were to be triggered or exacerbated by offensive cyber operations under the command of a NATO ally or if such operation on the part of NATO were used as a pretext for crisis. Considering the potential escalatory nature of a more forward-leaning posture – within NATO and driven by its largest member, the United States – these questions should be urgently addressed.

#### Communication over cyber definitions is key to enable operational planning

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

NATOs cyber-resilience experienced in crisis management and communication

Societal security, an emerging phenomenon in the field of strategy and security, requires good crisis management skills but also communication effectiveness in both the real and virtual worlds. Business continuity at NATO requires as foresaid the Alliance, to be resilient and surely for the purposes of this research paper, the Alliance and allies to be or become cyber-resilient.

By methodological approach, societal vulnerability continues and will always continue to exist, so far and as long as threats are there. Considering the current civil need to be always preparing for a new “cold era,” among others, considering the unlawful annexation by Russia of Crimea in 2014 (BBC, 2014) and following the disintegrating relations of NATO due to the unlawful act of Russia to Ukraine, the establishment of the USA and then taken over by NATO, of the Missile installation in Romania (Reuters, 2016) and the immediate reaction and accusation of Russia in regard to these developments (New York Times, 2016), the refugee challenges as an outcome on the constant fight against ISIS (US Homeland Security Committee, 2015), but also the phenomenal changes in the financial world (i.e., The Panama Papers (The International Consortium of Investigative Journalists (ICJ), 2016)), NATO is required to become truly resilient NATO, as should also nations and leaders.

All aforementioned elements are crisis management factors. NATO provides the tools and methodologies, in which the Alliance is requested to reply strategically and operationally. To mitigating plans for pre-crisis, during crisis and after crises situations. For and during operations, logistics of deployment or information gathering and or training purposes, among others.

In such similar cases, the legal and political perspectives also on cyber operations should be clear. The success of an operation lays to effective logistical and operational support. Therefore, the legal aspects that come with sharing of information, on how to deploy forces, identify key threats and elements in cyber-space, are important. The Internet has no borders. And threats can easily infiltrate the national e-space and boundaries. Leaders are welcomed upon to take strong strategic-led decisions.

NATO is to ensure protection of all infrastructure. The Allies should be able to anticipate, identify, mitigate, and recover from “hybrid attacks (NATO Review, 2016)”—the dimension(s) of simultaneous attacks, while reducing the threat of destabilization and or spreading fear.

In a civic society, it is our responsibility to ensure adequate awareness on cyber-defense and security. To learn about the necessity to protect all infrastructures, NATO’s collective defense should be characterized by burden sharing, openness, flexibility, and transparency in cooperation and information flow among member states. Through preparedness, strategic and operational awareness, strategic resilience can be achieved. Response time and framework will then allow NATO to counter threats as they emerge.

#### Interoperability solves—it fills capability gaps, reassures worries, and allows for escalation management

Łukasz Kulesa 19, Łukasz Kulesa is the deputy head of research at the Polish Institute of International Affairs (PISM), “The Future of Deterrence: Effectiveness and Limitations of Conventional and Nuclear Postures,” Carnegie Europe, 11/28/19, https://carnegieeurope.eu/2019/11/28/future-of-deterrence-effectiveness-and-limitations-of-conventional-and-nuclear-postures-pub-80440

THE WHAT

Internally, NATO members need to be clear about specific actions they can reasonably expect the alliance to deter. Clearly, an armed attack—from whatever direction—is one course of action to be deterred, but other actions are not so simple.1

In the case of Russia (and other state actors), the focus is also on deterring coercion: the act of adversaries imposing their will on NATO allies through a combination of military threats and nonmilitary means. For now, the thinking at NATO has emphasized deterrence of a territorial grab or blockade in the Baltic region. However, the characteristics of the Russian approach to warfare mean that the alliance has to look beyond the Baltic Sea and beyond the physical domain, mainly to the cyber realm.2 More and more of the critical systems running hospitals, carrying electricity, or patrolling the skies are now connected to the internet and therefore vulnerable. NATO’s adversaries can, in theory, block allied governments from coming to each other’s aid by threatening devastating cyber attacks that will cause populations to panic and cripple economies.

NATO has already declared that a cyber attack could lead the alliance to invoke its Article 5 collective defense clause, a statement that aims to have a deterrent effect—though there is little evidence that it has stopped adversaries from trying.3 This is mainly because most cyber attacks are designed to stay below the level that would trigger a response of the whole alliance. The allies need a clearer policy on what to do if the line is crossed one day. That policy must also address the thorny issue of credible attribution and should be rehearsed rigorously.

THE HOW

NATO does not need to mirror the activities of its adversaries to deter effectively. The idea is to signal that the alliance will not be intimidated or coerced, but that can be done in multiple ways.

With regard to Russia and the threat of a land incursion, NATO has decided to rely on limited forward deployments along its Eastern flank and on the ability to reinforce quickly those small contingents in times of crisis. The shortcoming of this posture is that if Russia overwhelms the first line of defense, it may be able to use the strength of its conventional forces, as well as the threat of nuclear weapon use, to thwart allied reinforcement.

NATO, as a whole, is adapting its posture to respond, and the United States is strengthening its military presence in Europe to address these potential weak points. The mix of U.S. troops and stored equipment and supplies in Europe is being expanded, including in Poland. And NATO has taken steps to improve its ability to deploy units from North America and move them around Europe by creating a Joint Force Command for the Atlantic and a Joint Support and Enabling Command. Other means of strengthening deterrence include implicit or explicit threats of political or economic sanctions or threats of countermeasures in cyberspace.

Regarding the South, the exact form of deterrence has to match the threat that NATO chooses to deter. With regard to potential state adversaries, NATO’s existing deterrence tools and military capabilities can be utilized against threats from that direction. The creation of the Strategic Direction South Hub—a consultation and coordination body for allies and partners—at the NATO command in Naples, Italy, also contributes to the deterrence mission. However, these measures alone will not deter the main challenge in the South: terrorist groups, with the potential to strike in Europe, operate in lawless spaces.

RECOMMENDATIONS

NATO may be back to its traditional mission of deterrence, but deterrence itself has evolved. A new approach must be adapted to today’s environment, in which a number of deterrence challenges need to be tackled simultaneously and sophisticated nonconventional means can be used jointly with traditional military tools to test the alliance.

MAINTAIN ALLIANCE COHESION

While the allies’ initial response to deterrence challenges has been impressive, in the long run, deterrence fatigue may present problems. NATO needs to keep all allies committed to the deterrence mission and continue to secure sufficient contributions of committed forces, capabilities, and resources. The risk is that allies’ unity and cohesion—the indispensable foundations of NATO—will weaken as memories of the Islamic State’s caliphate and of Russia’s aggression against Ukraine fade. Adversaries will do their part to sow or exploit divisions or doubts about the strength of solidarity among alliance members.

To keep cohesion from fraying, NATO’s leadership should continuously engage every ally in dialogue about the rationale for the posture, the threat assessment, and members’ views on, and concerns over, the implementation of the deterrence mission. National governments have the same essential responsibility toward their parliaments and publics. NATO must also make sure that discussions do not focus only on one strategic direction but rather address both defense and crisis-management tasks.

Engagement with partners should include a dedicated dialogue on deterrence issues. In some cases, based on mutual consent, NATO should be ready to explore coordinated deterrence signaling or mutually reinforced deterrence activities, such as joint statements, deployments, or exercises.

Engagement with adversaries must be seen as an inseparable companion to deterrence. Dialogue and multiple contact channels remain crucial to convey and receive deterrence signals, avoid accidental or inadvertent escalation, and explore risk-reduction and arms control opportunities.

DETER RUSSIA’S ADVENTURISM

In the foreseeable future, specific challenges connected with deterring Russia will continue to dominate the practical agenda. As a priority, the allies should fully implement the 2018 decisions to adapt NATO’s command and force structure.4 The military credibility of the current deterrence posture depends, to a large extent, on the alliance’s ability to speedily augment its forward-deployed units with follow-on forces.

The allies should look for new ways of stimulating the development of necessary capabilities and interoperability. A more transparent discussion of the major gaps in allied capabilities could help exert pressure on members to make relevant investments. The NATO Military Committee should play a more active role in the alliance’s adaptation by more visibly highlighting the military requirements for credible deterrence to civilian authorities and—via individual military leaders—to NATO populations.

The alliance should continue Article 5–related exercises, especially in more vulnerable regions, as the exercises play a role in deterrence signaling. But NATO must also increase the realism of such exercises to identify the areas where the alliance is lagging behind. The alliance needs more exercises that test mobility, logistics, and the preparedness of infrastructure to transport troops.

NATO’s Enhanced Forward Presence and Tailored Forward Presence strengthen deterrence, but the units deployed need to become a more coherent military force. This calls for further calibrating their combat potential, particularly by adding enablers such as air and missile defense, logistical support, and intelligence, surveillance, and reconnaissance. Flank countries should step up their regional cooperation to help advance that goal.

The process of adapting deterrence is ongoing, and developments on the Eastern flank will require the alliance to constantly reassess its posture. For example, Russia’s deployment of the dual-use SSC-8 cruise missile system and other long-range missiles requires a response.5 On the deterrence track, NATO will need to react to the threat of Russia striking targets away from the border such as harbors, airfields, or command centers, which are crucial for NATO’s ability to deploy its reinforcements. This response should include a mix of bolstering defensive measures and strengthening NATO’s ability to strike back. On the dialogue track, NATO can signal its openness to potential arms control talks.

An additional area that requires attention is the nuclear dimension of NATO deterrence. A more integrated approach to conventional and nuclear planning and exercises is needed. For example, conventional and nuclear exercises should be based on the same scenarios, although not necessarily conducted in the same region or at the same time. NATO needs to walk a fine line by sending deterrence signals to Russia but without suggesting a lowered threshold for the use of nuclear weapons. Fully integrating cyber, space, and information operations into a comprehensive deterrence posture is a less controversial but equally pertinent task.

DETER UNCONVENTIONAL AND HYBRID THREATS

NATO needs to be careful about defining and signaling its redlines. Making these boundaries too specific could embolden adversaries to intensify their actions below NATO’s declared threshold of response. Being deliberately ambiguous and raising the fear of retribution may be more useful for encouraging adversaries’ self-restraint.

At the same time, NATO should aim to deter specific types of particularly threatening unconventional activities. These include major and sophisticated cyber attacks against allies’ military forces and critical military and civilian infrastructure, proxy military and special forces operations, and state-sponsored terrorism. NATO could declare that such activities may lead it to invoke Article 5 and respond in various ways, including asymmetrically (for example, the response to a cyber attack may not involve only cyber capabilities).

The alliance must be able to identify early whether and when unconventional and hybrid gray-zone actions have become a more substantial and coordinated campaign. In such a case, NATO should aim to deter the adversary from escalating further. This requires increasing the alliance’s capacity to share early-warning intelligence and pool national intelligence-gathering, investigation, and attribution capabilities. NATO should not shy away from attributing ongoing operations to state adversaries, relying on national data as needed. The alliance and its members should be prepared to use direct channels of communication and other means to deliver immediate deterrence signaling in specific cases.

On the Southern flank, NATO faces state actors that use unconventional tactics and proxy forces (for example, Iran and Syria); state collapse and the emergence of ungoverned spaces in Libya, Yemen, and parts of the Sahel; and the activities of a range of nonstate actors, from loose groups to terrorist and criminal networks to highly organized quasi-state structures like Hezbollah. Cooperation with regional partners in addressing these threats will be vital. NATO’s primary task, as elsewhere, should be to deter states in the region from using unconventional tactics against NATO and its allies, using signaling and attribution tools. When possible, the alliance should aim to affect the calculus of nonstate actors to prevent them from harming alliance interests. This may not work with jihadist groups but may be possible with actors motivated by political or economic interests.

Since many of the unconventional threats are not linked to specific regions or actors, a more general approach is called for. The alliance and its members need to continue investing in passive and active measures to neutralize unconventional threats, including in peacetime. Further developing cyber defense and offensive capabilities—NATO’s toolbox for countering hybrid tactics—and strengthening resilience can affect adversaries’ willingness to use unconventional means against NATO and thus help establish deterrence by denial. The toolbox—counterterrorism, special forces, information operations, disruption of terrorist groups’ cyberspace activities—that allies develop for dealing with nonstate and quasi-state entities posing unconventional threats can also be used to deter state adversaries that rely on such tactics.

ENCOURAGE FURTHER DEBATE

For deterrence to work, the allies must clearly communicate their resolve and readiness to respond to an aggressive action. Clear communication is also needed to reassure the allies concerned. At the same time, the alliance faces a challenge in explaining to many citizens of NATO countries the necessity of deterrence. This is especially difficult in the area of nuclear deterrence, where reliance on such destructive weapons remains politically dubious and morally repulsive for many.

#### Forging shared understandings of threats and NATO’s role in countering cyberwar is essential for unity

Jovana Marović 19, PhD, Faculty of Political Science, University of Belgrade, Executive Director of the Politikon Network, 11/28/19, “Wars of Ideas: Hybrid Warfare, Political Interference, and Disinformation,” <https://carnegieeurope.eu/2019/11/28/wars-of-ideas-hybrid-warfare-political-interference-and-disinformation-pub-80419>

THINK AND SPEAK COHERENTLY

NATO is meeting the hybrid challenge with twenty-nine member states experiencing very different sociopolitical realities and often using different concepts. A unified vocabulary and strategy would limit the misunderstanding of threats, improve collaboration, and make the sharing of lessons learned more effective—so would an agreement on the prioritization of tasks and responsibilities and a shared understanding of NATO’s role.

This would greatly help individual countries to build compatible and comparable national strategies. Many of these strategies, including that of the youngest member Montenegro, are in early stages of preparation, but divergences are already becoming evident. Those that have been completed—such as Slovenia’s 2018 regulation on cyber and information security or Croatia’s 2017 National Security Strategy, which partly deals with hybrid challenges—have largely opted for different approaches.

NATO member states must send a unified message inside and out. As strategic communication is a mind-set, it has to be built together carefully and fundamentally.12 NATO’s communication strategy should be a result of joint efforts and hence a common instrument against all threats, not just hybrid ones, at all levels.

### Aff—Case—Emerging Tech Add-On

#### NATO cyber interoperability solves emerging tech risks

Nicolas Mazzucchi and Alix Desforges 19, Nicolas Mazzucchi is a research fellow at the Foundation for Strategic Research and Alix Desforges is a postdoctoral fellow at Geopolitics of the Datasphere (GEODE), “Web Wars: Preparing for the Next Cyber Crisism” Carnegie Europe, 11/28/19, https://carnegieeurope.eu/2019/11/28/web-wars-preparing-for-next-cyber-crisis-pub-80420

The acceleration of the military use of cyber capabilities and the simultaneous militarization of cyberspace create new threats and opportunities for NATO. The alliance must respond in a number of ways, including by increasing investment, strengthening technical cooperation with the European Union (EU), and seeking political consensus on the attribution of, and responses to, cyber attacks.

ISSUES AT STAKE

Armed forces and vital civilian organizations, such as operators of energy networks, rely more and more on computer systems for their operations. This increases both their efficacy and their vulnerability. NATO saw the significance of this trend some time ago, and since 2016, the allies have recognized cyberspace as a domain in itself. The alliance integrates cyber capabilities into its thinking and planning for operations, even if mainly in defensive terms. The alliance’s 2016 Cyber Defense Pledge helped member states strengthen their national cyber defense capabilities by working together.2

Twenty-four of NATO’s twenty-nine member states have issued public cyber doctrines that deal with military issues.3 Dedicated units are being created across NATO countries, either with a unified cyber command, as in France and the United States, or with a devoted cyber force, like in Germany. This is the right step overall, although allies’ differing approaches to cyber strategy and organization could cause challenges when it comes to joint and combined operations.

NATO is responsible for protecting its networks and infrastructure, as well as promoting cooperation among allies and with partner nations. For the moment, the alliance’s most important prerogatives and capabilities lie in the defensive use of cyber capabilities, although individual countries can volunteer various cyber services—not only defensive ones—to NATO commanders. In 2018, the alliance set up the Cyberspace Operations Center in its command structure to help nations and commanders better understand these possible national contributions and their uses. NATO also strengthened its cooperation on cyber matters with the EU through a joint declaration at the alliance’s 2016 summit in Warsaw.4

There is often little difference in offensive cyber capabilities between criminal groups and some military forces. Hacking tools are becoming more accessible. In 2017, the U.S. National Security Agency’s sophisticated offensive suite was stolen or leaked and subsequently used in attacks.5 In parallel, critical civilian infrastructure, such as the networks that govern energy or water distribution, is becoming more dependent on the internet, making it a target in potential conflicts. This infrastructure could even be used as a tool for a large attack: if corrupted by hackers, it could be turned into a botnet—a network of computers linked by malware. It has become possible, in theory, to achieve a strategic effect with cyber attacks on civilian facilities and infrastructure, which tend to be less protected than military equipment. As a result, the line between the defense of military and nonmilitary assets in cyberspace is becoming increasingly blurred.

One consequence of this trend is closer military cooperation with civilian authorities, including law enforcement. However, military organizations and armed forces tend to invest more than civilian ministries or agencies in cyber defense and cybersecurity. In the United States, for example, the Department of Defense accounted for more than 50 percent of the 2018 federal cybersecurity budget, representing $8.5 billion out of $15 billion.6 Unchecked, this trend creates a growing gap between military and civilian spending.

Several international organizations and, more recently, companies have decided to address stability in cyberspace and the regulation of cyber conflicts. Some states and nonstate actors are even suggesting the adoption of a treaty on the use of information technology and international security. After meetings of the United Nations (UN) Group of Governmental Experts failed in 2017 to reach a consensus on what constitutes states’ responsible behavior in cyberspace, the UN initiated two new negotiation processes. One is a resolution, sponsored by the United States and European countries, to create a new group of governmental experts.7 The other is a Russia- and China-sponsored resolution to set up an open-ended working group.8 The two tracks have different calendars and mandates, including on consultative meetings. The outcomes of their work, and the potential codes of conduct for cyber conflict they could generate, will provide guidance for how all countries, including NATO allies, should behave in the future regarding cyber operations

RECOMMENDATIONS

Research and development policies and investment strategies in cyber and military technologies are key elements to ensure that armed forces are equipped with up-to-date capabilities. The fast pace of technological evolution requires NATO member states to make significant, continuous investments to avoid falling behind in terms of capabilities.

Alongside investments in technology, allies need to strengthen education in cyber matters, not only in engineering, but also in strategic thinking and social use. All military personnel have to be involved to ensure greater cybersecurity awareness and a better integration of cyber capabilities into military operations. The most important challenge for NATO as an alliance is to bridge the gap between those states with first-rate cyber capabilities and awareness and those that lag behind. Currently, a handful of member states are pulling away from the others in terms of the mass integration of connected devices, quantum computing, and artificial intelligence–based systems. This gap could have a major impact on burden sharing in NATO, because a low level of spending by one or more countries would need to be compensated by the others to maintain a satisfactory global level for the alliance.

Allies should draw up national cyber rules of engagement for offensive operations in accordance with principles of international law. Certain policies espoused by some member states, such as hack-back, which allows private firms to pursue attackers into other companies’ networks, or cyber deterrence, could lead to uncontrolled escalation.9 International law tends to limit this escalation to mainly economic responses, such as sanctions and countermeasures. All NATO allies also need to ensure that their rules of engagement are compatible with the alliance’s agreed approach to cyber defense. At present, different countries have different views on offensive cyber policies, in particular.

The alliance should give technical assistance to member states that are willing to share information and national best practices. NATO should expand its rapid-response system to cover attacks that blur the line between the military and nonmilitary realms, such as an attack on critical nonmilitary networks in the context of a NATO military mission.

Unity is important when it comes to external communications by the allies, or by NATO’s secretary general, on attribution. While the decision to attribute an attack to a particular entity remains a sovereign and political one, allies should discuss any such communication from individual capitals before it is made. This would not only prevent uncontrolled escalation but also preserve the strength and unity of the alliance.

NATO should develop standards on the security of emerging cyber technologies in close partnership with the EU. Allies could address the interoperability and security of connected devices in the defense sector by devising a common policy in the alliance. NATO should also impose a minimum standard of cybersecurity in products, such as connected devices and systems; computer-based technologies; and command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems during the acquisition process.

Quantum computers deserve particular attention from NATO, because they can be game changers in the military domain. The alliance should act as a gateway between member states’ militaries and defense companies to promote further industrial cooperation, notably on technical standards. Such cooperation should be based on the NATO Industry Cyber Partnership, which provides platforms for the exchange of information, threat trends, and best practices. The alliance must foster the maximum possible level of cooperation to ensure that NATO countries are the first to implement this technology.

#### Emerging tech causes inadvertent escalation

Dr. James Johnson 21—Assistant Professor in the School of Law and Government at Dublin City University and a Non-Resident Fellow with the Modern War Institute at West Point, previously a Postdoctoral Research Fellow at the James Martin Center for Nonproliferation Studies in Monterey, California, 1/13/2021, ‘Catalytic nuclear war’ in the age of artificial intelligence & autonomy: Emerging military technology and escalation risk between nuclear-armed states, Journal of Strategic Studies, Routledge

The remainder of the article proceeds as follows. First, it contextualizes the concept of ‘catalytic nuclear war’ with emerging security technologies, particularly AI. The article uses this analytical framework to examine how and under what circumstances the nefarious (mis)use of these technologies by non-state actors (i.e., terrorists, criminals, and state-proxy actors) might create or exacerbate escalation pathways leads to an accidental nuclear confrontation between nuclear-armed powers. Next, in the articles’ empirical core, it considers four aggravating features in the interaction of emerging technology with nuclear weapons and the pathways to nuclear escalation examined in the article – information complexity and asymmetry; greater automation of NC3; disinformation, misinformation, and information manipulation; and nuclear multipolarity.15 This article posits that AI-enhanced capabilities will likely amplify these underlying conditions (or second-order effects), thus increasing the risk of sparking unintentional escalation between strategic nuclear-armed powers – especially in crisis and conflict conditions. The next section uses four fictional scenarios – cyber false flag operation, cyber-attack on nuclear early-warning systems, drone swarming targeting ISR systems, and deepfake disinformation – to demonstrate how AI-enhanced capabilities in the hands of non-state actors might accidentally or inadvertently drag a competitive nuclear dyad into conflict. The final section considers possible ways of reducing catalytic escalation risk caused by non-state actors, particularly how militaries can maintain effective command and control of their nuclear forces in a rapidly evolving and complex conflict environment.

### Aff—Case—Extend: Strategic Ambiguity Fails

#### Russian cyber adventurism is inevitable. Strategic ambiguity within NATO strains the alliance and wrecks deterrence

Patrick 18—James H. Binger senior fellow in global governance and director of the International Institutions and Global Governance (IIGG) Program at the Council on Foreign Relations (CFR) (Stewart Patrick, 8/8/2018, “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>)

While the North Atlantic Treaty Organization (NATO) was founded on the idea of collective defense, the nature of security threats has changed since its inception. The Cold War-era alliance is struggling to adapt to evolving technology and the altered nature of warfare. Nowhere is this more true than in the cyber realm. NATO policymakers have acknowledged cyberwarfare as a distinct sphere of conflict, but they have not yet tailored nuclear-era concepts of deterrence and response to this new domain. As cyberattacks increase in destructive potential and remain difficult to attribute, the alliance face the dilemma of whether and how to adapt their policy of strategic ambiguity to a new era of cyberwarfare.

At their annual summit last month, the twenty-nine allies reaffirmed the integral role cybersecurity plays in NATO, creating a Cyberspace Operations Center to supplement existing cyber defense facilities and reaffirming the need for an offensive capability “to deter, defend against, and to counter the full spectrum of cyber threats.” Missing from the communique, however, were any rules of engagement for the cyber sphere. This raises the question: How would NATO respond if a member state were to invoke Article V of the North Atlantic Treaty following a cyberattack?

The NATO alliance has long maintained a policy of strategic ambiguity when it comes to nuclear policy, leaving open the possibility that a conventional attack might be met with a nuclear response. (By contrast, China and India have adopted “no–first use” policy for nuclear weapons.) NATO’s nascent cyber policy exhibits a similar ambiguity, intentionally leaving unclear how the alliance would react to a cyberattack. Rather than responding in kind, NATO might instead conduct conventional attacks, such as missile strikes, allowing for rapid escalation.

Early cyberattacks were largely seen as low-stakes events: an inconvenience for the financial sector and dangerous for personal data, but not a threat to national security or justification for a military response. This is no longer necessarily the case. A coordinated Russian cyberattack against a nuclear power plant in Europe and the United States could have devastating consequences, were it to result in major radiation leaks. An attack on a country’s electric grid, a softer target, could in theory cause hundreds of billions of dollars in damage and put lives at risk as traffic lights stop working, hospitals lose power, and unrest erupts.

Given these stakes, NATO has an obvious incentive to strengthen its capacity to deter and punish cyberattacks, including through conventional retaliation. A U.S. Department of Defense memorandum published in early 2017 stated that at least for the next decade, offensive cyber capabilities are likely to outpace cyber defense, making deterrence the most viable option. Both the United States and NATO also recognize that a devastating cyberattack could quickly escalate to violent conflict by triggering a conventional response. Unfortunately, the alliance’s policy of strategic ambiguity falls short. By failing to define the rules of engagement for retaliation, the alliance leaves open the potential for chaos in determining an appropriate response to cyberattacks. In doing so, it invites adversaries to test the waters.

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.

To be sure, NATO’s strategic ambiguity is not without its benefits. Uncertainty about the threshold for a military response could persuade an adversary not to push the envelope with an audacious attack. But that same ambiguity could lead an adversary to miscalculate. Moreover, the doctrine also leaves open the possibility of discord in the ranks of NATO member states regarding how to deal with any such attack.

NATO’s policy of strategic ambiguity served it well during the long Cold War nuclear confrontation. But it may be less appropriate to the era of cyberwarfare, particularly given the problem of attribution and the potential for inter-allied disagreement on the appropriate response to any particular incident. NATO policymakers need to resolve this dilemma by formulating a more explicit cyberwarfare doctrine to which all of its member states can adhere. This should include updating their mutual understanding of what constitutes an act of aggression under NATO’s collective defense provisions, making explicit to potential adversaries just what its red lines are, and establishing clear procedures and channels for robust allied response to cyberattacks. Unless NATO clarifies current ambiguities, Russian aggression in the cyber realm could go unchecked.

#### Ambiguous Article 5 thresholds causes both over AND under reactions to cyberattacks

Ethan Williamson 19, Current Analyst with Morgan Business Consulting LLC and recently became CompTIA Security+ Certified and hold a Secret clearance, “NATO’s Expanding Role in Cybersecurity,” Charged Affairs, 5/13/19, <https://chargedaffairs.org/natos-expanding-role-in-cybersecurity/>, language edited change denoted by brackets

Through these organizations and agreements, NATO has improved and strengthened its unified cyber defense capability, seemingly positioning itself to be a standard bearer for cybersecurity. However, these commitments lack specifics and could hamper NATO’s ability to respond to an attack because of bureaucratic and security protocols. Following the inclusion of cyber attacks under Article 5, NATO and its allies could not agree on what kind of attack would trigger the collective defense response. Allies still use their own incident standards to define cyber incidents and in some cases do not make these standards public. This results in an uneven response and makes it difficult for NATO and its allies to provide a unified, Article 5 response to cyber incidents. Stoltenberg has defended this vague definition by stating that, “a clearly defined threshold only invites attacks immediately beneath it.” This clarification does not address the larger issue of which attacks would trigger an Article 5 response, as NATO already defends against low-level cyber attacks daily. Ambiguous guidelines could also cause NATO to misappropriate responses to cyber attacks, leading to potentially embarrassing overreactions to minor incursions or devastating slow responses to ~~crippling~~ [devastating] attacks. Without a clear definition, NATO will struggle to respond to attacks.

As stated earlier, NATO’s focus is on deterring attacks—to such an extent that the cost of an attack would outweigh any benefits. However, this focus has resulted in NATO lacking the offensive capabilities to respond in the same capacity as its allies, like the United States. There is some discussion within NATO over taking an “offensive defense” role within cyber in order to respond directly after an attack. This change will have its own repercussions, as it may lead to an attack being wrongly attributed or a response unnecessarily escalated.

#### Status quo isn’t deterring Russia—they’ll continue pursuing gray-zone tactics below the threshold

John R Deni 19, John is a Research Professor of Joint, Interagency, Intergovernmental, and Multinational Security Studies at the US Army War College’s Strategic Studies Institute, “The Paradox at the Heart of NATO’s Return to Article 5,” RUSI Newsbrief, November/December 2019, Vol.39 No.10, <https://rusi.org/sites/default/files/20191101_newsbrief_vol39_no10_deni_web.pdf>, \*ableist language edited

Despite the necessity of exercises like Defender 2020, new purchases of advanced military equipment and the expansion of military manpower (all underway since 2014), these steps together constitute a growing paradox that the Alliance has been slow to recognise and respond to. That is, just as the Alliance is becoming more focused on and more capable of responding to an Article 5 threshold-crossing event, the probability of a conventional manoeuvre warfare scenario is decreasing. Put another way, major improvements in the Alliance’s ability to defend the territory of its member states are necessary, but it is becoming ever more obvious that these steps will not be sufficient for collective defence in NATO’s next decade.

Many European security analysts believe an Article 5 threshold-crossing event is unlikely in the coming years. Russia is a declining state along several measures, especially in economic terms, and over time the acute threat that it represents today should diminish. Certainly, it has made advances recently in limited military capability areas, such as indirect fires and precision munitions. Yet, the Russian playbook evidently continues to eschew frontal attacks on states that are members of a military alliance, at least in the air, sea, land and space domains.

A frontal attack in one of these domains or some other egregious assault compelling NATO to invoke Article 5 would not play to Russia’s strengths – instead, it would actually expose its many weaknesses, ultimately resulting in certain defeat. Moscow’s military and governing elites know this. For this reason, the Kremlin has consistently chosen to emphasise and leverage its comparative advantages to make effective use of its clearly limited resources. The military policy tools that facilitate this do not resemble armoured columns crossing national frontiers. Rather, they include fomenting civil unrest with the goal of creating a justification for Russian military or paramilitary action in unaligned, neighbouring or near-neighbouring states, as seen in Moldova (1992), Georgia (2008) and Ukraine (2014). They also include cyber attacks, such as that unleashed on Estonia in 2007. They include influence peddling and the cultivation of patronage networks. And they include semi-deniable election interference, as occurred in the US in 2016 and 2018 and in Europe in recent years as well. All of these policy tools represent asymmetric responses to US and Western power, especially military capacity and capabilities. They enable Moscow to cost-effectively pursue the disintegration of Western power and the Western alliance, as a way of achieving Russia’s strategic and material ends. Given the current state of the Russian economy and the rather grim outlook for the years to come, Moscow is very likely to continue pursuing these sorts of policies in the coming decade, because it lacks other options.

The fundamental challenge facing NATO between now and the Alliance’s 80th anniversary is figuring out how, where and when it will counter and compete iteratively with Russia – but also China – in the grey zone, the space between war and peace, or between offense and defence. Because grey-zone challenges do not neatly correspond to classical notions of those which fall in the military’s domain and those which do not, they are particularly vexing. This is why adversaries such as Russia and China employ grey-zone tactics and operations – they allow Moscow and Beijing to confront the West on more favourable terrain.

The good news is that NATO’s leaders appear to understand the character of the competition, and have taken several steps to address the challenge. The Alliance has reportedly developed a strategy outlining NATO’s role in responding to grey-zone or hybrid threats. In some cases, grey-zone scenarios are finding their way into NATO and member states’ exercises. And critical infrastructure protection, energy security and societal resilience have become important topics of discussion at Alliance-sponsored events and seminars, and among Alliance-affiliated entities such as centres of excellence.

However, in several important aspects, the Alliance response remains ~~handicapped~~ [weak]. Although NATO declared in 2016 and again in 2018 that it could consider a hybrid attack as grounds to invoke Article 5, the bar seems high – perhaps impossibly so. Achieving consensus – and quickly – in the face of an ambiguous attack or in response to ostensibly unrelated low-level provocations will not be an easy task. Perhaps more importantly, NATO remains in a defensive crouch when it comes to grey-zone challenges – Alliance rhetoric, exercises and actions emphasise response and reaction. It is precisely for this reason that grey-zone challenges against NATO are likely to be effective – actors such as Russia and China are evidently undeterred by the Alliance’s defensive posture, and attacks on Western institutions continue to this day. To be clear, defence is important, but in the current international security environment, offense and the competitive actions in between the two are equally important.

Given the arguably inadequate Alliance response to date, some guideposts may be helpful to illuminate the path ahead as NATO attempts to ensure collective defence remains robust into its eighth decade. First, Article 5 is an imperfect tool for determining when and where the West must spend blood and treasure in defence of its interests and way of life. Despite Alliance rhetoric regarding hybrid warfare as a potential Article 5 trigger, the threshold for Alliance-wide action is too high, and adversaries like Russia and China know it – this is why they pursue grey-zone tactics in the first place. To facilitate the speedy response that will be necessary to meet the needs of Allied defence against grey-zone challenges, greater, routine use can be made of Article 4 and Alliancewide consultations and coordination on issues and topics that go beyond conventional military operations that are NATO’s bread and butter. For instance, the Alliance can and should conduct more vigorous, regular consultations and intensified coordination on topics such as keeping Chinese investment out of sensitive information-technology and logistics sectors, limiting and rolling back Russian broadcast and print media penetration of Western markets, undermining the Kremlin’s and Putin’s trustworthiness within Russia, and exposing Russian and Chinese official corruption at home and abroad, all as mechanisms to compete and thereby strengthen collective defence.

#### Shared understanding now is impossible—that decks credibility

Limnell 16 (Jarno Limnéll, Professor of Cybersecurity, Aalto University, Finland Charly Salonius-Pasternak, Senior Research Fellow, The Finnish Institute of International Affairs. "Challenge for NATO – Cyber Article 5." http://www.diva-portal.org/smash/get/diva2:1119569/FULLTEXT01.pdf)

The current ‘cyber warfare playbook’ is still a slim volume - but it is growing by the day. In order to remain a credible defence alliance, NATO must possess a credible cyber policy, including cyber deterrence. Credibility comes from a largely similar set of actions as NATO has engaged in regarding conventional military. Doing it in the cyber domain is, however, harder at the moment. For example, what is the equivalent of standing up in practice permanent battalions in member states? How do you exercise, publicly message determination to defend and counter aggression, in a serious but non-threatening way?

NATO has to find a clear way to deal with a ‘Cyber Article 5’ event. It may be necessary to reinterpret what Article 5 and an armed attack constitute in today´s world. The biggest challenges is to reach a shared understanding of the limits (physical and cyber) which could lead a member state to invoke Article 5 and delineate what proportionality in response means. The decisions are political by their nature and requires strong understanding

#### Commitment to proportional response restores deterrence credibility and prevents escalation spirals

Schulze 19 (Dr Matthias Schulze is Associate in the International Security Division at SWP; “Cyber Deterrence is Overrated” SWP, August 2019; https://www.swp-berlin.org/10.18449/2019C34/)

Deterrence fails if the threat of punishment is not considered credible. Deterrence fail­ure often leads to the use of capabilities and thus escalation. This raises questions about the proportionality, effectiveness and accuracy of cyber retaliation capabilities. How much objective damage must be in­flicted so that A considers the costs of further offensive action to be too high? How does D know whether A considers threats against certain assets to be particularly painful or not? A and D most likely have different perceptions about what assets are considered especially sensitive. These different perceptions make proportional reactions difficult. There is no inter­national consensus on how proportional cyber retaliation might be conceived. Thus there is an increased risk of escalation. The damage caused by cyber retaliation must be appropriate. If the damage threat­ened by D is too great, the probability of a renewed retaliation by A increases. It is well researched in political science, that escala­tion spirals are often a consequence if a retaliation is perceived as inappropriate or too painful. In these cases, deterrence fails. If the threat of punishment is considered not costly enough and thus not credible, deterrence does not work either. Determining the correct measure is highly complex and also a function of the attribution prob­lem: the lower the chance of being caught, the greater the threat of punishment by D must be

### Aff—Case—Extend: Russian Cyberattacks

#### Russian cyber operations blur the line between wartime and peace—they’ll utilize cyber and AI in tandem to escalate

Aaltola 21—Director of the Finnish Institute of International Affairs, Finland, and Professor of International Relations at Tallinn University, Estonia (Mika Aaltola, 2021, *Democratic Vulnerability and Autocratic Meddling*, Chapter 4: Russian Cyber-Enabled Diversions in the West, Springer)

The challenge to the existing regional order inevitably blurs the line between normal and unconventional. What is considered legal, established, and conventional becomes an obstacle as the challenger tries to reset the rules and expectations. This logic increases the possibility of unexpected events in the region. The distinction between peacetime and wartime practices can become more blurred. However, there is no evidence of using cyberattacks to cause widespread physical damage in the region; infrastructure has been outside of the targets.

So far, the attacks have been unlikely to attract clear retaliatory actions. Risks have clearly been taken by Russia, but in a calculated way that maximizes the psychological and political effects and minimizes the chances of punishment. On the other hand, the harm scale that focuses on physical damage misses the real significance of politically motivated cyberattacks. For example, the damage caused by rigging an election process far surpasses some of the physical harm scenarios.

It is important to realize that even when uncovered, the attacks showcase the perpetrators’ capabilities. This can even be useful for the attacker, as its image as a powerful modern actor is highlighted in public discussions. When an operation becomes public, the perpetrators can always point to attribution issues and deny their role in the operations to delegitimize any retaliation. Perhaps paradoxically, public revelations about ongoing and active cyber operations can even be part of the overall strategic goal of demonstrating power and impunity. This is a possibility that target states and institutions have to consider.

Although many lessons have been learnt by now, the main response to cyberattacks has been to strengthen deterrence by bolstering cybersecurity. The systems are now in a much higher reactive mode. Vigilance has been increased against different types of shocks, disruptions, and attacks. It is likely that the West will continue to be a target of low- to mediumintensity cyber operations. One may argue about whether high resilience can be achieved without more active deterrent measures. On the other hand, it takes two to tango online. The higher the active deterrence, the stronger the counterreaction is likely to be. The fear is that this may culminate in a destabilizing cyber arms race.

Ever higher awareness is needed to recognize that cyber operations have strategic aims that go beyond mere snooping and spying and, especially those, that can be sowing the seeds for or be parts of much more serious societal destabilization and democracy meddling operations. Clearly, cyber tools and operations can be effective in spreading mistrust, blackmail, and bullying, and in displaying capabilities and deterrence. They are useful in combination with other politically pressurizing tools. The spectrum of these combinatorial tools is still being experimented and the tools are likely to evolve considerably. The clear concern is that the situation may escalate, in which case the level of harm caused by cyber operations in combination with other influence tools will become higher and more intense for the highly digitalized democracies. One should also note that the level of harm is always realized in hindsight. The Dukes and Red October/Turla were identified only a long time after the infections. This suggests that in the present moment, there might already be ongoing attack campaigns with a higher level of harm which are yet to be detected. The analysis cannot exclude the possibility of a further escalation in malicious cyber and AI activities and their use in tandem with destabilizing cognitive operations and hybrid tool. If such a scenario materializes, then the intensifying cyber operations of today can be seen as a preparatory phase for a far more aggressive challenge directed mainly at the key functions and stability of the Western political systems.

#### Russia will utilize cyberattacks to spark conflict across the region—the plan solves

Stojkovski 21—freelance journalist covering foreign policy and technology based in Skopje, North Macedonia (Bojan, 1/4/2021, “Flawed Cybersecurity Is a Ticking Time Bomb for the Balkans”, Foreign Policy, <https://foreignpolicy.com/2021/01/04/flawed-cybersecurity-is-a-ticking-time-bomb-for-the-balkans/>)

On the night of July 15, 2020, the Balkan nation of North Macedonia was anxiously awaiting the preliminary results of its parliamentary election. Soon after the polls closed, in what was first believed to be a minor technical glitch, the website of the State Election Commission went down.

The polling results were nowhere to be found on the website in the next several hours, as the commission resorted to manually announcing the latest updates on a makeshift YouTube channel. And things didn’t get any better in the late hours of the night.

That night, the country suffered the biggest cyberattack in its history. The website of the electoral commission stayed down for the next few days, recovering from a full-scale distributed denial-of-service (DDoS) attack that ~~paralyzed~~ its functions, as thousands of IP addresses targeted the site. Months later, the authorities’ probe into the matter has yet to produce any findings about who might have been behind the attack.

While authorities claimed that the cyberattack did not have any serious consequences on the election process and the results themselves, it managed to highlight how fragile the IT systems of government institutions in the country are. A few weeks later, hackers also targeted several ministries, again demonstrating the urgent need for better cybersecurity measures.

The lack of expertise among the staff, insufficient financial resources, and the overall neglect of officials when it comes to the topic of cyberdefense are among the main issues plaguing state institutions across the region. It’s not only North Macedonia; many other countries in the region just aren’t doing enough when it comes to having strong cyberdefense systems. And in most cases, individuals prove to be the weakest link because they have not been trained and educated on how to defend against such attacks.

In March 2020, North Macedonia became NATO’s newest member. Looking to boost its overall defense capabilities, the country is now also putting its hopes on NATO’s assets and expertise when it comes to improving its cybersecurity.

However, during the last few years, NATO member states across the region have also been hit hard by various cyberattacks. In 2019, neighboring Bulgaria suffered the largest theft of personal data in the region, after its National Revenue Agency was hacked. More than 5 million Bulgarians have had their personal data exposed, and the hacked database was shared on various hacking forums.

Authorities charged a 20-year-old Bulgarian cybersecurity expert for the hack, although the motives behind it remained unclear. The attack illustrated just how weak cybersecurity practices at Bulgarian government institutions were.

With the country currently in a political turmoil and facing its next parliamentary elections in March 2021, the cyberattack on the National Revenue Agency could also serve as a warning of what’s about to come.

Apart from ransomware attacks, DDoS and malware attacks are some of the most common tools that hackers have been using to target state institutions. In most cases, the damage that these types of attacks can do could be very expensive.

“DDoS are one of the most common hacker attacks … due to the fact they are relatively simple and inexpensive to implement, compared to other types of attacks,” said Ljubica Pendaroska, a Skopje-based privacy and data protection expert.

“But the potential harm that they can do could be worth millions—counted in lost earnings, compromised systems, creating distrust in institutions, data theft, and the like.”

According to Pendaroska, such threats should constantly keep state institutions on alert and maintain an institutional awareness of the need for highly organized and functional protection systems.

The motives for these cyberattacks can vary. For some, as is the case with ransomware attacks, the gains could be purely financial. Others, however, might have more malicious intentions.

Montenegro, a NATO member since 2017 and an EU hopeful, held elections at the end of August. Fearing a reprisal of meddling attempts like the one that the Balkan country suffered in 2016, when a Russia-backed attempted coup took place, Montenegrin authorities held a joint mission with cybersecurity experts from the United States toward the end of 2019.

The mission aimed to prepare both sides for any possible Russian hacking attempts that could target the election processes in the two countries. However, as a recent suspected Russian hacking attack on U.S. government agencies showed, this might not be such an easy task—no matter how developed or technologically advanced a country might be.

“This was a cunning cyber-espionage campaign that was very hard to detect. It reveals that the U.S. government needs to enhance its cyberdefenses,” said Bilyana Lilly, an assistant policy researcher at Rand Corp.

Even if the U.S. government itself remains vulnerable, Washington is a cyberpower that can aid smaller countries. Various U.S. agencies can assist Bulgaria, Romania, North Macedonia, and other U.S. partners in the region, and they have done so on multiple occasions, Lilly explained.

In the Balkans, a region known for its political and economic instability, cyberattacks on state institutions could be used to fuel tensions among the many countries that have ongoing disputes, which could in turn have political and economic consequences.

### Aff—Case—Extend: Solvency

#### Defining proportional response averts the fog of war and adversarial probing

Weed 17 (Maj Scott A. Weed is the commander, 724th Special Tactics Support Squadron, 724th Special Tactics Group, 24th Special Operations Wing, Pope Field, North Carolina, Air Force Strategic Policy Fellow for Cyber Issues, Department of State.US Policy Response to Cyber Attack on SCADA Systems Supporting Critical National Infrastructure USAF CPP–7 <https://www.hsdl.org/?view&did=803892>)

The 2014 North Atlantic Treaty Organization (NATO) Wales Summit further affirmed the UNGGE recommendations by maintaining that “international law, including international humanitarian law and the UN Charter, applies in cyberspace.” NATO’s assertion is categorical—cyberspace will not be a lawless space. NATO also determined that cyber attacks could threaten national security and stability, holding that “cyber defence is part of NATO’s core task of collective defence” meriting case-by-case Article 5 consideration.13 It is worth noting that neither the UN nor NATO yet specifies a specific “red line” response threshold, automatically determining retaliation and strategic options. Without established and recognized norms of cyber behavior to frame the use of national instruments of power, “We could be forced to live in the worst of all possible cyber worlds—routinely vulnerable to attack and self restrained from bringing our own power to bear.”14

There is also significant policy context necessary for any US cyber response. The US International Strategy for Cyberspace holds that existing Internet governance bodies should continue to guide and shape the development of the Internet.15 The US strategy is aimed at continuing the Internet tradition of innovation, rather than a competing vision of state control. The United States desires to ensure appropriate representation from governments, academia, and private and civil sectors.16 US policy makers insist on not conflating control over standards and protocols with a perceived (by some) need for sovereign ability to act unilaterally or multilaterally in cyberspace to preserve vital national interests.

Policy makers and strategists must likewise endeavor to stay informed by and ahead of technology. In this way, there must be consensus about distinguishing among sophisticated cybercrime, ubiquitous cyber espionage, and legitimate cyberwarfare. The current blurred lines among these three are often used by adversaries in cyberspace to disguise and obscure intent and patronage.17 States should also realize that policy decisions in cyberspace will likely have international consequences due to interconnectedness, and there should be understood requirements for “global interoperability, network stability, reliable access, multi-stakeholder governance, and cybersecurity due diligence.”18 This well-informed spirit of transparency in policy would help mitigate the fog of war inherent in cyber incidents and potentially avert unnecessary conflict.19 The political landscape and societal contexts are not the only considerations. There is also the development of the US whole-of-government approach to respond to cyber attack.

#### Setting a framework for cyber defense is key to innovative resilience

Marios Panagiotis Efthymiopoulos 19, designated Dean and Associate Professor of International Security and Strategy of the College of Security and Global Studies, at the American University in the Emirates AUE, “A cyber-security framework for development, defense and innovation at NATO,” Journal of Innovation and Entrepreneurship (2019) 8:12, https://link.springer.com/content/pdf/10.1186/s13731-019-0105-z.pdf

Setting the stage

Cyber-security is yet to be globally, legally, operationally, and strategically defined. The scale of a security perspective is more attractive at this time considering the geostrategic challenges and threats. The possibility of innovation and entrepreneurship in the field is also a tangible reality, due to the necessary research and development methods. More so, the possibility of an open market economy sharing of knowledge and technological skills makes security and cyber-security or defense for that matter more attractive. What lacks in the world wide legal and political framework of operations, exchange of information and protectiveness from new sources or methods that can be deemed as elements of infiltration.

The article’s aim is to examine and recommend a global strategic framework for operational capacity and management resilience between allied and cooperative partners in the field of cyber-security. The current article is a follow up of prior scientific publications made in 2014 first and later in 2018, on NATO’s cyber-security strategy, presented through a framework of Cyber-Development, Cyber-Democracy, and Cyber-Defense (Carayannis, Campbell & Efthymiopoulos, 2014; Carayannis, Campbell & Efthymiopoulos, 2018). The aim is to converge diversified information on cyber-security, in a single strategic framework; reflect to the actual practical needs in understanding operations and tactical ability to deliver in multi-complex and dimensional world through management and operational efficiency capabilities. The article requests interoperability of aims and objectives under a global framework of cyber-security; through a strategic framework on cyber-security, global law can be proposed, defined, and adopted by the international community. The strategic framework will define structures that are needed to be put in place on a global scale, when reflecting issues of cyber-security and inclusive for NATO. It will define threats and challenges, as cyber-attacks are real. Cyber-security is not an asymmetrical or hybrid threat, but an existential one. Its destructive capacity can be multi-leveled and can also lead to human casualties. The future of e-safety lays at both a global estimation framework of what constitutes cyber-security and how we react to it; it lays in between cooperation of allies and members of wider alliances, against specified or approximate threats. Yet, its framework of aims and objectives, management, command and control, and operations will be defined and decided by allied parties only such as is the case of NATO.

Operationally, national and cooperative forces need to be continuously agile and technologically advanced. In an asymmetrical world, which is complete with unforeseen challenges and threats, we need forces with flexibility, adaptability, operational and strategic command structure, based on high technologically sophisticated information “coming in,” but also being used while in training or through active operations.

On a theoretical scale, the current article requests a cyber-security strategic framework adoption of resilient adaptability and interoperability policy in the framework of safety and defense. The article considers that understanding the realities of threats is by definition a natural innovation and as we move ahead, we structure and operate a single strategy on cyber-security against a virtual threat from wherever it comes from. Its long-term resilience may be more complex as operational capacity needs to constantly develop and adapt into the convergence of societal structures, and methods; where socio-economic, technological, defense even health, and education issues are affected.

When theory on cyber-security, resilience, and operational capacity will be applied at NATOs level, it will enable allies and members, jointly, to create a true policy and strategy for cyber-security resilience against hybrid virtual threats. The methodology on how to is presented through this current article.

The article’s design is based on cross-disciplinary and interdisciplinary approaches. It combines elements of global security and strategy, national and international law, economic development, and technological research and advancement and most importantly is innovative and entrepreneurial; its understanding will enable us to comprehend global and regional market establishment and convergence, as also economic changes. The setting of the study required lapse of time to showcase the need and the necessity of the subject. Current output reflects a set of written analyses, rules, and primary experiences. It methodologically acquired sources of information of related necessity and relevance, shaped the understanding, and need to point out for a framework of rules, regulations, management, and operations on cyber-security.

The article and its author frames a specific policy recommendation with regards to the creation of not only a regional alliance (NATO-based scale), Cyber-Security Strategy for the twenty-first century but a global one. The article defines the “dynamism” of cyber-security both as a topic and subject. Cyber-security is a twenty-first century element of policy orientation; a necessity for both collective and individual defense and security resilience.

In specific, a cyber-security strategy for NATO will enhance its innovation and creativity core of operations and methodologies against any kind of virtual threats. It will set standards, policy procedures, and recommendations. NATO’s strategy of cyber-security through its new Cyberspace Operations Centre, in Mons (Belgium) as decided in the Brussels Summit of July 2018 (Cyber-Space Operations Center Mons Belgium, 2018) unfolds options and opportunities, innovation, and entrepreneurship in operations efficiency and capabilities application. Current technological advancements and dynamisms through innovation and sustainable futuristic advancement will soon be evident

### Neg—AT: Cyber Aff—Deterrence Turn—1NC

#### Turn: ambiguity is better for preventing cyber escalation

Lt. Ken M. Jones 15—United States Navy, MA student at Naval Postgraduate School in Science of Cyber Systems and Operations, B.A.S., Wayland Baptist University. (“Cyber War: The Next Frontier for NATO,” March 2015, https://apps.dtic.mil/sti/pdfs/ADA620763.pdf)

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.

#### Otherwise, attackers would be *more* impelled to start cyber wars

Susan Davis 19—General Rapporteur for this report, Congresswoman. ("NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence,” October 2019, from NATO Parliamentary Assembly, Science and Technology Committee, 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)

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.

### Neg—AT: Cyber Aff—Deterrence Working Now—1NC/2NC

#### They have it backwards – the prevalence of grey-zone activities proves deterrence is *strong* now.

Hal Brands 16, PhD @ Yale, Distinguished Professor of Global Affairs at the Johns Hopkins School of Advanced International Studies, “Paradoxes of the Gray Zone”, https://www.fpri.org/article/2016/02/paradoxes-gray-zone/

In many ways, the prevalence of gray zone approaches is actually a testament to the strength of the liberal international order that America has led since World War II. Gray zone approaches reflect the fact that there are strong international norms against outright aggression and territorial conquest, and that even moderately revisionist powers often hesitate to pay the costs—from moral opprobrium, to economic penalties, to the potential for a military response—associated with flagrantly violating those norms. In the same vein, gray zone conflict actually underscores the fact that U.S. military power, alliances, and security guarantees—the structures that have long served as the backbone of the international order—have generally proven quite effective in deterring or punishing such flagrant military aggression. Indeed, these strengths of the international system have fostered the very ambiguity and incrementalism that characterize gray zone approaches, persuading revisionist powers—usually—to take small steps that sow doubt about what is really happening, and that avoid more dramatic provocations that might cross clearly established “red lines.”[[11]](https://www.fpri.org/article/2016/02/paradoxes-gray-zone/" \l "_ftn11" \o ")

#### The status quo is working—there’s a conceptual understanding of what invokes Article 5, while maintaining effective ambiguity

Lt. Ken M. Jones 15—United States Navy, MA student at Naval Postgraduate School in Science of Cyber Systems and Operations, B.A.S., Wayland Baptist University. (“Cyber War: The Next Frontier for NATO,” March 2015, https://apps.dtic.mil/sti/pdfs/ADA620763.pdf)

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.

However, that is not to say that NATO has been irresponsible or lackadaisical in trying to give some understanding on when a cyber-attack becomes an armed attack. With the help of experts in the field of cyberspace, international law, and policymakers, the Tallinn Manual was written and published to provide guidance to NATO and any other international or national alliance or government seeking it. Although the Manual offers guidance on what scale, effects, and attacker motivation would be severe enough to fall into the category of an armed attack, it does not give specific details, only a conceptual idea of what an armed attack might look like in the cyber realm. Then, with the guidance of the Manual, and international law, there could be a better understanding of what would then invoke an Article 5 response. Nevertheless, it is not, and was not intended to be, a complete go-to-guide for how each member country should conduct itself in the cyber world.

**The whole point of hybrid war is that it doesn’t escalate *by design*. Russia will take actions approaching redlines but won’t actually trigger them – solves conflict**

Alexander **Lanoszka 20**, PhD, Assistant Professor in the Department of Political Science, Balsillie School of International Affairs, University of Waterloo, “Thank goodness for NATO enlargement”, Int Polit (2020) 57:451-470

The defensibility of NATO’s northeastern flank NATO enlargement has provided a key source of insurance by raising the costs of direct Russian aggression against alliance members. This is true even in arguably the weakest part of the alliance, the Baltic littoral region. Conventional wisdom holds that the defense of this region against Russian aggression is especially costly for the USA and NATO to undertake. The countries located there are exceptionally vulnerable. Whereas most benefciaries of NATO enlargement are at least largely separated from Russia thanks to Belarus and Ukraine, the Baltic countries are directly contiguous and have only a short land connection to continental NATO by way of the Polish–Lithuanian border. According to this perspective, a rebalancing of alliance commitments in Europe is necessary because the local military balance favors Russia too much and the political will to defend the Baltic states is too low. The USA will never ‘trade Toledo for Tallinn’ (Shifrinson 2017, 111). Note the contradiction: According to critics, enlarging NATO simultaneously provokes Russia and weakens the alliance. But what rational cause would Russia have to be dismayed when a potentially adversarial military alliance willingly takes on major liabilities? The alliance security dilemma—whereby the strengthening of one coalition may inadvertently create insecurity for another—suggests that Russia would be justifiably concerned if NATO either incorporated states that meaningfully aggregate capabilities or increased military ties with such powerful states (Snyder 1984, 477). By NATO enlargement critics’ own admission, the Baltic countries subtract from, rather than add to, what the alliance can do. Russian might have reasons to protest enlargement, but these reasons likely concern the perceived slight to its honor when former Soviet states became formal defense partners of the USA (Götz 2017, 236–239).4 NATO enlargement has not been responsible for Russian authoritarianism or international revisionism because it never threatened Russia. Pessimism regarding the defensibility of NATO’s so-called northeastern flank is also unwarranted. To begin with, much of the policy literature on this region concentrates on Russia’s strengths while ignoring its key weaknesses. The Baltic countries would almost surely lose set piece battles against Russia, but deterrence ultimately hinges less on being victorious in a potential war than on imposing unacceptable costs on the adversary. The Baltic states have already begun embracing unconventional strategies intended to boost national resiliency and make occupation difficult (Collins and Beehner 2019). Guerrilla tactics and territorial defense serve to augment their denial capabilities that in turn would complicate Russian efforts to hold territory and pacify the local population. Moreover, **Russia may have local escalation dominance**, **but it does not have global escalation dominance**, **given the forces that NATO members possess**. **A large-scale land grab made at the expense of any of the Baltic countries might precipitate escalatory dynamics that it could not control. Nuclear war** may be a remote possibility, but it **cannot be discounted altogether**. **One reason why Russia has resorted to so-called hybrid tactics against the Baltic countries**—**such as political subversion and eforts to foment unrest**—**is that it does not wish to provoke a reaction that it cannot handle** (Lanoszka 2016). **Put simply, Russia may believe in NATO’s Article Five collective defense commitment more than NATO members themselves do.**

### Neg—AT: Cyber Aff—Deterrence Turn—2NC

#### Redlines embolden aggression *more* than clarity AND jeopardize NATO’s credibility

Z’hra M. Ghavam 16—Lieutenant Commander, United States Navy, B.S., United States Naval Academy. ("NATO’s Preparedness for Cyberwar," September 2016, <https://calhoun.nps.edu/handle/10945/50552>)

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.

Following the Wales Summit in 2014, NATO affirmed its stance on law and cyberspace while refusing to address cyber redlines:

Our policy also recognizes that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm, therefore, that cyber defense is part of NATO’s core task of collective defense. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.209

However, an invocation of Article 5 does not necessarily mean that a NATO response would include force. Article 5 of the Washington Treaty states the following:

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.210

Thus, as long as each Alliance member takes “such action as it deems necessary,” it cannot be found in violation of the collective defense principle.211 In the case of a major act of cyberwar against one of its members, NATO could invoke Article 5 as a show of solidarity but opt to refrain from employing kinetic military force; instead, the Alliance could use purely cybernetic means or a hybrid alternative that combined cybernetic tools with military force to fulfill its objectives.

In all, NATO’s establishment, organization, and employment of its sophisticated cyber response agencies and IT resources like the NCIRC, NCIO, NCIA, and RRT are indicative of how seriously the Alliance has implemented its cyber defense policies at the operational level. NATO’s cyber policy, standard operating procedures, and ambiguous thresholds for the use of military force make the Alliance highly prepared to respond effectively to major acts of cyber aggression against one or more of its members. If an act of cyberwar met the threshold of an armed attack, NATO would probably be prepared to manage, counter, and resolve the issue in cyberspace; still, one cannot exclude the possible need to take kinetic measures. Out of a numerical ranking of 1–3, the Alliance earned a preparedness score of 3 in cyber strategy.

#### Retaining flexibility is key for appropriate response

Lt. Ken M. Jones 15—United States Navy, MA student at Naval Postgraduate School in Science of Cyber Systems and Operations, B.A.S., Wayland Baptist University. (“Cyber War: The Next Frontier for NATO,” March 2015, https://apps.dtic.mil/sti/pdfs/ADA620763.pdf)

In light of the recent developments of NATO, it would seem to be in NATO’s best interest to remain ambiguous and allow the organization to approach its response to a cyber-attack on a case-by-case basis. For instance, the attacks on Estonia might require intervention on behalf of the Estonian people due to the fact they are a smaller, lesser defensible state. Estonia would not be successful standing up against Russia, and as Russia becomes more aggressive in the former-Soviet bloc region, small states like Estonia are at risk. If another attack were to occur against Estonia, the attacks would have to be more severe to invoke an Article 5 response. Such a response would enable NATO states to act as if they too have been attacked as per the mutual defense announcement against cyber-attacks at the Wales Summit. Yet, if the United States is attacked in a similar manner, there likely does not need to be the same scale of defense taken, because the United States has more resources and capabilities to respond on its own. Remaining ambiguous allows NATO to choose the best opportunities for supporting and defending member states.

Before it could decide on a response, NATO would first need to consider the severity of the attack to determine the appropriate level of response, whether it be sanctions, cutting off financial aid to the offending country, or a boots on the ground campaign. However, even while retaining flexibility in its response to a cyber-attack, NATO understands the importance of cyber defense. It aims to deter cyber-attacks against its networks and member country’s networks through strong cyber defenses, although NATO has yet to fully seek what Cold War theorists have called “deterrence by denial,” and which could be an effective mechanism.161 With such a posture, the enemy need not be convinced that a cyber-attack will be followed by retaliation or punishment; instead, it is only necessary to convince the enemy that the initial attack will have no effect.16

#### Ambiguity produces better *tailored responses* to re-establish deterrence

Susan Davis 19—General Rapporteur for this report, Congresswoman. ("NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence,” October 2019, from NATO Parliamentary Assembly, Science and Technology Committee, 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)

NATO’s ambiguity also extends to the type of punishment it threatens were it to suffer a cyber attack. The Alliance has made clear that it neither limits punishment to similar cyber attacks nor excludes them. Instead, it keeps the option open to use the full range of Allied capabilities to deter and counter cyber attacks. Once again, this introduces useful doubt in an opponent’s mind. A more technical reason for the difficulty of restricting retaliation to cyber attacks is that it is hard to credibly threaten the assets of the attacker in a similar fashion. If an attacker shuts down a power plant, would the Alliance have cyber options to attack an opponent’s power plants or similar infrastructure? Would NATO even want to if it could, as it complies with the principle of proportionality and international law in all its activities? NATO’s ambiguity on the type of retaliation serves a convincing purpose. It produces doubts in the would-be attacker’s mind and presents more options to tailor and scale a response to re-establish deterrence.

### Neg—AT: Cyber Aff—Impact Defense—1NC

#### No large-scale Russian cyberattacks

Baezner 17 (Marie and Patrice Robin; Feb; Cyber Defense Project (CDP) Center for Security Studies (CSS), ETH Zürich, “Cyber-Conflict Between the United States of America and Russia” https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/184547/Cyber-Reports-2017-02.pdf?sequence=1)

On the other hand, both states might not desire further escalation, preferring to restrain the conflict to cyberspace. Each would follow the “tit-for-tat” logic and accuse each other while never reaching a tipping point where the conflict spills over to a conventional war. Such a tipping point would be linked to the intensity of the attack or the nature of the targets. Both nations would keep the cyberattacks small enough not to trigger a bigger reaction. The same would be observed on the choice of targets, with both avoiding certain critical or sensitive targets, for instance critical infrastructures. In order to contain the conflict in cyberspace, both states would have to demonstrate their restraint by selecting options with low risk of miscalculation (Lin, 2012, pp. 64–66). In the future, it might also be possible to see a deescalation in the form of the emergence of an international treaty or at least further bilateral treaties between the USA and Russia on cyberattacks. For example, during the last few years, businesses in the USA were often hacked and spied on by the Chinese military. These intrusions were mostly cyber-economic-espionage and were said to have supported the theft of billions of dollars’ worth of intellectual property (Bamford, 2016). In September 2015, the USA and China signed an agreement engaging both countries not to support or conduct cyber-theft of intellectual property. Moreover, the parties have made the commitment not to use cyberattacks against each other’s critical infrastructures in peace-time and to support the establishment of international behavioral norms in cyberspace (Rosenfeld, 2015). Both states also highlighted the fact that they could not control each individual in their country and therefore could not be held responsible for individual acts. Since then it seems that the number of attacks on commercial targets has diminished (Timm, 2016). Former President Obama suggested the creation of a position of cybersecurity ambassador to deal with bilateral or multilateral treaties concerning cyber-norms (Lee, 2016). For this kind of de-escalation to take effect, the termination of the conflict at hand must be the stated aim of both parties. A clear common understanding of the terms of agreement is required and must be based on trust-building efforts, as well as the assurance of mutual adherence. The difficulty of tracking the implementation of such agreements in cyberspace has been an obstacle preventing more states consenting to such solutions (Lin, 2012, pp. 62–64). Nevertheless, a dialogue on cyberspace already exists between the USA and Russia since July 2013. This cooperation includes Confidence Building Measures (CBM) such as the creation of working groups on the issue of ICT security, exchange of information between the two national Computer Emergency Response Teams (CERT), and the creation of a direct communication line to directly manage ICT incidents (Segal, 2016; The White House, Office of the Press Secretary, 2013). In October 2016, former President Obama used the latter to inform Russian President Putin that the USA was accusing Russia of interference in the election process (Ignatius, 2016). Furthermore, Russia and the USA take part in the UN GGE supporting the future establishment of international norms on actions in cyberspace. They stated that international law can be applied in cyberspace and therefore, the rules of proportionality and limited collateral damage should also be respected in cyberattacks (Ignatius, 2016; United Nations General Assembly, 2015). These examples demonstrate that even though the two states are involved in a “tit-for-tat” logic in their relations on a tactical level, there was still a dialogue on the strategic level, at least until 2015. The recent cyberattacks in USA and the election of Donald Trump as US President, bring new uncertainties.

#### No nuclear retaliation

Tucker 18 (Patrick; Feb 2; Technology Editor for Defense One, MA from Johns Hopkins University, BA from Sarah Lawrence College, Former Deputy Editor for The Futurist; “No, the US Won’t Respond to A Cyber Attack with Nukes,” https://www.defenseone.com/technology/2018/02/no-us-wont-respond-cyber-attack-nukes/145700)

No, the US Won’t Respond to A Cyber Attack with Nukes Defense leaders won’t completely rule out the possibility. But it’s a very, very, very remote possibility. The idea that the U.S. is building new low-yield nuclear weapons to respond to a cyber attack is “not true,” military leaders told reporters in the runup to the Friday release of the new Nuclear Posture Review. “The people who say we lowered the threshold for the use of nuclear weapons are saying, ‘but we want these low-yield nuclear weapons so that we can answer a cyber attack because we’re so bad at cyber security.’ That’s just fundamentally not true,” Gen. Paul Selva, vice chairman of the Joints Chiefs of Staff, said Tuesday at a meeting with reporters. It’s an idea that military leaders have been pushing back against since the New York Times ran a Jan. 16 story headlined, “Pentagon Suggests Countering Devastating Cyberattacks With Nuclear Arms.” When would the U.S. launch a nuclear attack in response to a non-nuclear event? The Defense Department says the threshold hasn’t changed since the Obama administration’s own nuclear posture review in 2010, but a draft of the new review that leaked online caused a bit of drama in its attempts to dispel “ambiguity.” The new review gives examples of “non-nuclear strategic attacks,” Robert Soofer, deputy assistant secretary for nuclear and missile defense policy, told reporters on Thursday. “It could be catastrophic attacks against civilian populations, against infrastructure. It could be an attack using a non-nuclear weapon against our nuclear command-and-control [or] early-warning satellites. But we don’t talk about cyber.” In his own conversation with reporters, Selva broadened “early warning” systems to include ones that provide “indications of warning that are important to our detection of an attack.” He also emphasized, “We never said ‘cyber.’” There’s a reason for that. While cyber attacks on physical infrastructure can be very dangerous, they are unlikely to kill enough people to provoke a U.S. nuclear response. An National Academies of Science and Engineering analysis of the vulnerability of U.S. infrastructure makes that point. A major cyber attack could cut off electrical power, resulting in “people dying from heat or cold exposure, etc.,” said Granger Morgan, co-director of the Carnegie Mellon Electricity Industry Center and one of the chairs of the report. “A large outage of long duration could cover many states and last for weeks or longer. Whether and how many casualties there could be would depend on things like what the weather was during the outage.” It’s a huge problem but not an event resulting in tens of thousands of immediate deaths. Contrast that with a nuclear attack on a city like Moscow, even one using a device of 6 kilotons, much smaller than the ones the United States used against Japanese targets in World War II. The immediate result: there would be 40,000 deaths, according to the online nuclear simulation tool NukeMap. Russia has demonstrated a willingness to take down power services with cyber attacks, as they did in Ukraine on Christmas Eve 2015. But these attacks were brief and occured in the context of actual fighting. In other words, the worst cyber physical attack that top experts believe credible likely does not meet the threshold that the Defense Department has set out for deploying a nuclear weapon.

#### Cyber-attacks won’t take down the grid

Craig 16 (Victoria; Feb 2; Analyst at Fox Business, Citing the Senior Manager of Industrial Control Systems at Mandiant, “The U.S. Power Grid is 'Vulnerable,' But Don't Panic Just Yet”, http://www.foxbusiness.com/features/2016/02/02/u-s-power-grid-is-vulnerable-but-dont-panic-just-yet.html)

The idea of the nation's power grids becoming the next battleground for cyber warriors could make hacking into consumers’ credit card accounts and personal information seem like child’s play. While U.S. power companies are likely targeted by foreign governments and others in increasingly sophisticated breaches, actually shutting off the lights and causing chaos is far more complicated than many pundits make it seem. Dan Scali, senior manager of industrial control systems at Mandiant, a cybersecurity consulting arm of FireEye ([FEYE](http://www.foxbusiness.com/quote.html?stockTicker=FEYE)), explained that while cyber criminals may gain access to power and utility data systems, it doesn’t necessarily mean the result will be a power outage and a total takedown of power grid control systems. In other words, the power grid is controlled by more than just a panel of digital buttons. “Losing the control system is bad from the perspective that it takes you out of your normal mode of operations of being able to control everything from one command center, but it doesn’t mean you’ve lost control or all the lights go out [in the city],” Scali explained. While many of the systems have been modernized to include digitized control panels, if a hacker were to infiltrate the system, a utility worker could still have the ability to manually control the machines by flipping a switch, pushing a button, or tripping a breaker. As the world saw with the recent attack in Ukraine, which caused a blackout for 80,000 customers of the nation’s western utility, the biggest problem may be ensuring the power grid’s control systems are not vulnerable to cyber break ins. The January attack in Ukraine was likely caused by a corrupted Microsoft Word attachment that allowed remote control over the computer, according to the U.S. Department of Homeland Security. Scali said there was no evidence from the incident in Ukraine that the hacker’s malware was able to physically shut down the power. “It wiped out machines, deleted all the files. Kill disk malware made it impossible to remotely control things. It caused chaos on the business network, and the area where control system operations sat. But the attacker, we believe, would have had to actually used the control system to cause load shedding, which caused the power to go out, or trip breakers to cause the actual problem. Malware itself didn’t turn the power out,” Scali said. He said what most likely happened in that incident was the hacker stole user credentials and logged into the system remotely. The bottom line: Yes, a similar event could happen in the U.S. And corporate America is concerned. A recent survey released in January on the state of information security, conducted by consulting firm Pricewaterhouse Coopers, showed cybersecurity as one of the biggest concerns among the top brass at U.S. power and utilities firms. Part of the problem, Brad Bauch, security and cyber sector leader at PwC said, is the interconnectedness of the industry’s tools. “Utilities want to be able to get information out of [their] systems to more efficiently operate them, and also share that information with customers so they have more real-time information into their usage,” he explained. While allowing access to their own consumption data allows the companies to give their customers more of what they want, it also opens up a host of access points for hackers, making the systems more vulnerable than they otherwise would be. But to say that the power grid is susceptible to cyber hackers is a bit of an oversimplification.

#### No Russian war

Khramchikhin 18—Aleksandr Khramchikhin, deputy director of the Institute for Political and Military Analysis in Moscow. (Rethinking the Danger of Escalation: The Russia-NATO Military Balance, 1-25-18, https://carnegieendowment.org/2018/01/25/rethinking-danger-of-escalation-russia-nato-military-balance-pub-75346)

But conventional wisdom is often wrong, and so it is this time. The hysteria that has engulfed public commentary throughout Europe about this ostensibly dire military situation on the brink of getting out of hand has little, if any, basis in fact. Both sides in the standoff exaggerate the tensions and the danger of escalation, and the risks of the military moves—their own and their adversary’s—supposedly driving these tensions.

In reality, the military balance between Russia and NATO is stable, the danger of escalation is hardly approaching critical levels, and little needs to be done militarily to defuse the current tensions. The true cause of the tensions is not military, but political and diplomatic. Until those causes are resolved, tensions between Russia and the West will remain high. The likelihood of a military confrontation will remain low, however, because neither side’s posture points to a heightened state of readiness or intention to go on the offensive. Until that changes, political and diplomatic tensions will remain mere tensions.

### Neg—AT: Cyber Aff—Impact Defense—2NC

#### Deterrence and norms solve cyberattacks

David **Lonsdale 17**, School of Law and Politics, University of Hull, Cottingham Road, “Warfighting for Cyber Deterrence: A Strategic and Moral Imperative.” Philosophy & Technology, doi:10.1007/s13347-017-0252-8

3.4 The Failure of Cyber Deterrence? The potency of cyber deterrence is difficult to judge. This is partly because there exists no consensus on what constitutes an act of sufficient cyber aggression. Therefore, it is not entirely clear what is to be deterred. Where exactly the threshold for response should be will be discussed in section three of this paper. For now, we can state that low-level nuisance attacks are a daily occurrence. For example, U.S. military networks are probed and scanned millions of times each day (Work 2015, 1). Similarly, acts of cyber espionage are reasonably common. However, what is also evident is the lack of major cyber attacks. For a while, Stuxnet, Wiper, Shamoon and Bronze Soldier appeared to signal the rise of cyber attack as a potent new instrument of policy. However, medium to large-scale attacks have essentially dried-up. Indeed, reflecting the empirical evidence, and marking a shift in tone, in his September 2015 testimony to the Senate Armed Services Committee, Director of National Intelligence, James Clapper, talked down the possibility of an ‘electronic Pearl Harbor’. Instead, he focused on ongoing ‘low-to-moderate’ level threats (Clapper 2015, 2). What does this all tell us? Is deterrence working? If one considers low-to-moderate threats as deterrable, then the answer would seem to be no. From this perspective, and according to some policy makers, deterrence is already failing. In a 2015 Senate Armed Services Committee Hearing, Chairman John McCain was scathing in his assessment: ‘Our adversaries view our response ... as timid and ineffectual. Put simply, the problem is a lack of deterrence. The administration has not demonstrated to our adversaries that the consequence of continued cyber attacks against us outweigh the benefit.’ (Takala 2015) However, if we take the view that cyber deterrence should really concern itself only with large-scale attacks, the picture is more positive. Indeed, Valeriano and Maness (2015) have identified considerable levels of restraint in state cyber behaviour. This could be due to a lack of confidence in the strategic utility of cyber attack. It may also reflect the development of norms against aggressive forms of cyber behaviour and the efficacy of deterrence. Indeed, norms increasingly form part of ‘complex deterrence’, within which military and non-military elements operate together. In cyberspace, although a settled understanding of universal rules of behaviour is still lacking, norms appear to be crystalising around acceptable forms of intrusion rather than a blanket non-use position (Stevens 2012, 25). This may explain the continuance of lowlevel probes whilst large attacks have trailed off.

#### Grid collapse won’t cascade – impossible

Chris Marciano 16, utilities worker and researcher, “Could terrorists shut down the United State's entire power grid?”, https://www.quora.com/Could-terrorists-shut-down-the-United-States-entire-power-grid

Unlikely. First off, there are three separate grids in the US: the Eastern Interconnect, the Western Interconnect, and Texas (called ERCOT). Yes, Texas is its own entity. Don't act surprised. You can take an electron and run it from Louisiana to Maine, but you can't go to Houston or San Francisco. Several changes were made due to the Northeast Blackout of 2003. The grid operates on a principle of redundancy to avoid cascading failures. When a power line fails, the electrons near-instantaneously go to other lines. If the addition of those electrons cause these lines to overload and fail, the failures will continue like a domino effect. The operators of the grid, using fancy software, manage the grid so that no single failure leads to a cascading failure. If one failure does occur, they will make necessary changes to prevent another single failure from causing a cascading failure; that could include a starting reserve generation in particular areas (even if that generating resource is more costly) or by turning off the power of select areas.

#### No Russia war – they won’t risk it

Amy F. Woolf 20, Specialist in Nuclear Weapons Policy in the Foreign Affairs, Defense, and Trade Division of the Congressional Research Service at the Library of Congress, received a Master’s in Public Policy from the Kennedy School of Government at Harvard University in 1983, “Russia’s Nuclear Weapons: Doctrine, Forces, and Modernization”, https://fas.org/sgp/crs/nuke/R45861.pdf

One analyst has postulated that Russia may actually raise its nuclear threshold as it bolsters its conventional forces. According to this analyst, “It is difficult to understand why Russia would want to pursue military adventurism that would risk all-out confrontation with a technologically advanced and nuclear-armed adversary like NATO. While opportunistic, and possibly even reckless, the Putin regime does not appear to be suicidal.” 144 As a study from the RAND Corporation noted, Russia has “invested considerable sums in developing and fielding long-range conventional strike weapons since the mid-2000s to provide Russian leadership with a buffer against reaching the nuclear threshold—a set of conventional escalatory options that can achieve strategic effects without resorting to nuclear weapons.”145 Others note, however, that Russia has integrated these “conventional precision weapons and nuclear weapons into a single strategic weapon set,” lending credence to the view that Russia may be prepared to employ, or threaten to employ, nuclear weapons during a regional conflict.

#### Russia war won’t escalate

Amos Zeeberg 18, MA in Science Journalism from Boston University, BA from Harvard University, Contributing Editor at Nautilus Magazine, Freelance Science Journalist Based in Tokyo, “Why Hasn’t the World Been Destroyed in a Nuclear War Yet?,” Nautilus Magazine, 1/15/2018, <http://nautil.us/blog/-why-hasnt-the-world-been-destroyed-in-a-nuclear-war-yet>

But after all these nuclear near-misses, one starts to wonder if it really is plain dumb luck. The Nash equilibrium accurately describes a certain kind of rational, perfectly logical approach to choices under conflict. And exactly in keeping with game theorists’ advice, the USSR and U.S. went to great lengths to make sure their arsenals would be feared as legitimate threats. Yet each time they had an opportunity to make good on those threats—to launch a crushing response to an apparent attack or mercilessly exploit a weakness, as many armchair analysts recommended—something held them back: a disobedient soldier, a circumspect engineer, an optimistic leader. The two nations were engaged in a battle of wills, staring each other in the eyes, and they both blinked. Repeatedly.

Maybe, when millions of lives hang in the balance, people are not so rationally cold-hearted as those old game-theory models imply. Or maybe they’re using a different kind of rationality.