# Neg – OCOs 3 – BFHR

### notes

Thanks a ton to Sam Gordon and Paul Wallace for their work this wave! Please email [khirn10@gmail.com](mailto:khirn10@gmail.com) with any comments or concerns.

Many cyber affs---including OCOs and space---clearly have interactions with the ‘Article 5’ debate. I figured that 1acs should have the option of explicitly designing their plan to include an attempt at pressuring NATO to agree on appropriate Article 5 thresholds for what constitutes an armed attack with regards to cybersecurity. The aff/neg file is thus designed as a supplement, with defensible and distinct impact mods both for and against changing the threshold.

The DAs in this file are essentially deterrence and assurance, the links assuming the aff attempts to establish some cyberattacks as falling short of meeting the threshold of ‘armed attack’. The “Lower A5 Threshold” DA is meant for a hypothetical aff that **lowered** the Article 5 threshold, functionally saying “all cyberattacks are armed attacks and we will respond accordingly.” The aff material in “OCOs 3” doesn’t support this angle, but I could envision somewhat putting it together.

## Case

### Say No/Solvency---1NC

#### NATO will say no:

#### Revising Article 5 requires absolute consensus---that’s impossible on cyber

Jordan ‘14 [Klara; September 4; Senior Fellow and Assistant Director of the Atlantic Council’s Cyber Statecraft Initiative, LL.M from the Law School at the University of Groningen, Masters in Interdisciplinary European Studies from the Institute of Advanced European Studies, Law Degree from Matej Bel University; National Interest, “Would NATO Go to War Over a Cyberattack?,” https://nationalinterest.org/print/feature/would-nato-go-war-over-cyberattack-11199]

Deliberations on thresholds triggering Article 5 could prove particularly thorny, given the transatlantic divide in views on what consequences are necessary to constitute an armed attack.

For example, the United States may be willing to consider a lower threshold than its less eager European allies for whom only grave uses of force are considered an armed attack. A state’s view of this threshold may well depend on whether it is the victim of an attack or a member called upon to fulfill its collective-defense obligation.

Additionally, Article 5 does not define the nature of that commitment. The treaty allows a member state to take whatever action it deems appropriate to assist an attacked ally—it decides how it will respond in collective defense. A member state may interpret its obligation to respond expansively or in a far more limited manner. So by viewing its Article 5 obligation in a limited way, a member could determine that it is not required to respond with kinetic force to assist an attacked ally, even in cases of destructive cyberevents.

Given the capability, doctrinal and policy divide between NATO members in the cyberarena, an ally might limit its response to entirely nonkinetic measures, such as rerouting Internet traffic through its national network, monitoring networks for future attacks, crisis-management support or diplomatic statements on behalf of the attacked ally.

On the other hand, if NATO determines a cyberattack amounts to an armed attack and invokes Article 5, and undertakes responsive action against an aggressor, member states are not limited to cyber-responses alone; they may also choose to employ kinetic force in the collective defense of the attacked member state. Adoption of this cyberpolicy provides NATO states a wider range of potential options with which they may respond in cases of destructive cyberattacks. NATO allies may respond with cyber- or kinetic tools, or a combination of both, a fact that may help to ensure an Alliance-wide response.

Regardless of the political weight presently attributed to NATO’s expected policy statement, law and policy are inextricably intertwined in the interpretation of Article 5, and the subtleties of its real-world application may make it difficult for the organization to offer the assurances certain allies are seeking with respect to their defense against cyberattacks. As a result, the policy could fall far short of its intended goals.

NATO states could, however, decide to make adoption of its new cyberpolicy a true game changer, to ensure that it becomes a useful framework for addressing the rapidly changing security challenges posed in the cyber-realm.

NATO nations might begin this process by reexamining the threshold requirement for Article 5 application in response to cyberattacks. States could agree, for example, that although some cyberevents may well cause consequential kinetic results (and some of a truly horrific nature), in the cyberworld, requiring kinetic consequences in order to trigger application of the collective-defense requirement does not fully reflect the types of serious crises cyberattacks can trigger.

They could determine, rather, that the appropriate Article 5 threshold in response to cyberevents might also be triggered by the far more likely consequences of large-scale economic disruption with corresponding national- and international-security implications.

This, of course, would require all twenty-eight members to reconsider their long-established views on what constitutes an armed attack under international law, and to achieve consensus on a far more forward-leaning approach. This would, no doubt, be a hugely difficult undertaking. Nevertheless, the development of international law is a continuous process, and states and international organizations should move to adapt it to help meet changing threats.

#### Numerous allies are wedded to ambiguous cyber strategies and will refuse

Eilstrup-Sangiovanni ’18 [Mette; 2018; Reader in International Relations and a Fellow of Sidney Sussex College at Cambridge University, PhD in Political Science from the European University Institute; Philosophy & Technology, “Why the World Needs an International Cyberwar Convention,” Volume 31, Number 3]

The Cult of the (Cyber) Offensive

International security scholars and military officials widely agree that cyberspace favors offensive operations (see Nye 2015a, b; Lonergan 2016; Sheldon 2011; Libicki 2009, 32–33; Clarke and Knake 2010; Vanca 2013; Saltzman 2013, 43; Lindsay 2015, 52; Lucas 2017, 127). According to traditional offense/defense theory, when offense holds the advance it is relatively easier to ‘move forward, destroy and conquer territory’ than to protect and defend it (Jervis 1978; Evera and Stephen 1984; Glaser and Kaufman 1998).Footnote10 Cyber experts list three main reasons why offensive strategies have an upper hand in cyberspace. First, as Sheldon observes, “attacks in cyberspace occur at great speed…putting defenses under immense pressure, as an attacker has to be successful only once, whereas the defender has to be successful all of the time” (Sheldon 2011, 98). Second, the prospect of launching attacks with relative anonymity (and therefore impunity) lowers the expected cost of offensive strategies in cyberspace (see Sheldon 2011, 98; Lindsay 2015). Third, physical distance is relatively inconsequential in the virtual world. Cyberattacks can emerge practically from anywhere, providing significant latitude for attackers to seize the initiative and catch defenders by surprise (Nye 2010; Sheldon 2011, 98). Another way of stating this point is that cyber technologies lead to great improvements in the mobility and reach of force—both factors held to increase offensive advantage (see Glaser and Kaufman 1998, 62).

The International relations (IR) theory points to four main strategic implications of offensive dominance. First, when offense is strong relative to defense, it becomes imperative for states to react quickly and resolutely to emerging threats, since even a small initial shift in the ratio of capabilities can cause a decisive shift in actors’ ability to prevail in a conflict (van Evera 1984, 64). In a cyber context, the compulsion to act and react fast is further amplified by the changing vulnerability of most cyber targets. Cyber weapons consist of complex software designed to exploit vulnerabilities residing in other software, such as computer operations systems or industrial control systems (Lucas 2017, 7). Unlike most conventional targets, a given cyber target may therefore only be vulnerable—and a cyber weapon aimed at that target only potentially effective—until the point at which a string of code is fixed or the target is replaced (DOD 2006, 3). The implication, according to many cyber experts, is that, “if you do not act quickly, you may not be able to act at all” (Vanca 2013, 26. See also Buchanan 2016; Lonergan 2016; Lindsay 2015, 56).

A second implication of offensive advantage is to encourage arms racing. As Glaser and Kaufman (1998, 48) explain, when offense is strong, states are likely to find that equally sized forces are inadequate to support a defensive strategy. Instead, they are likely to conclude that they require a substantial lead in military force to defend against attacks. This triggers a dynamic of competitive arms building, whereby even states that merely wish to defend the status quo strive to build up their military arsenals at a faster pace than their competitors in order to secure an adequate defense.

A third effect of offensive advantage is to increase rewards for striking first, thereby increasing the probability of preemptive or preventive attacks (Jervis 1978; van Evera 1984). In the cyber domain, incentives to attack enemies preemptively arise partly from the fact that actions in cyberspace move so fast that they leave little time for targeted states to mount a defense (Clarke and Knake 2010). The motivation to strike first may be further reinforced by the prospect of using carefully targeted cyber-strikes to neutralize an enemy’s conventional defense systems and thereby limit its retaliatory capacity (Saltzman 2013, 44). Indeed, many military strategists believe that preemptive strikes in the cyber domain are likely to bring decisive advantages on the conventional battlefield (see, e.g., Clarke and Knake 2010).

Fourth, according to IR theory, when offense is strong relative to defense, the ability to deter attacks (as opposed to seeking to defend against them) becomes vital. Logically, in a strategic environment that is thought to favor offensive operations, the ability to deter aggressors hinges crucially on the ability to signal or demonstrate superior offensive capabilities. Hence, according to traditional offense/defense theory, the surest way to achieve effective strategic cyber deterrence is to develop strong offensive capabilities, which promise crushing retaliation against would-be attackers.

To sum up, conventional IR theory points to four strategic implications of cyber offensive advantage: (1) an emphasis on fast action, (2) a tendency towards arms-racing, (3) strong incentives for preemptive attacks, (4) a focus on boosting deterrence through enhancing offensive capabilities. These implications of cyber offensive advantage are not merely “theoretical.” The importance of taking fact action is emphasized in leading national cyber security strategies. According to the US “National Military Strategy for Cyberspace,”

Cyberspace affords commanders opportunities to make decisions rapidly, conduct operations, and deliver effects at speeds that were previously incomprehensible. In addition, increasing the speed of the policy and decision-making process potentially will yield greater effectiveness of cyberspace capabilities. (US DOD 2006, 4).

The perceived need to boost offensive capabilities as a means to strengthen deterrence is also clearly articulated in many strategic documents and in public statements by defense officials.Footnote11 Admiral Michael S. Rogers, Commander of the US Military Cyber Command, has repeatedly pointed to the need to “increase our capacity on the offensive side to get to that point of deterrence.”Footnote12 Similarly, in a press conference in April 2015, US Air Force Chief of Staff Mark Welsh described the Pentagon’s goal of developing cyber weapons that could inflict “blunt force trauma” on an enemy in order to deter aggressors (see Ewing 2015). The Trump Administration has also signaled an aggressive cyber position. During his presidential campaign, Donald Trump repeatedly vowed to expand America’s offensive cyber capabilities—a commitment that has been followed up by plans for a 15% increase in military cyber-security spending in the DOD’s 2017 budget (see Gady 2017).Footnote13

Other nations appear to be drawing similar conclusions regarding the need to adopt more offensive cyber postures. Russia, Iran, and North Korea all have military units specifically dedicated to offensive cyber operations (NY Times 2016). Since 2005, China has begun to incorporate offensive computer network operations into its military exercises, primarily in comprehensive first strikes against enemy networks (Salzman 2013, 51), and the Chinese have recently admitted the existence of purely offensive cyber units in the PLA (according to Raud 2016, 20–21). The Germans have publicly disclosed that they are developing offensive cyber weapons (Limnéll 2013) as are Argentina and France. Even Denmark and the Netherlands have launched programs to develop cyber offensive capabilities (Paletta, Yadron and Valentino-Devries 2015).

In short, current political and military leaders focus overwhelmingly on improving their countries’ cyber offensive capabilities and appear to premise national cyber security strategies on a firm belief that defensive strategies are insufficient to deter enemies in cyberspace. This strategic environment is strongly reminiscent of the “Cult of the Offensive” that swept Europe in the decades prior to World War I.Footnote14 Much like political and military leaders prior to WWI, today’s decision-makers appear to display a “highly exaggerated faith in the efficacy of offensive military strategies and tactics” (Van Evera 1984). And, much like political and military planners prior to WWI, they tend to discount the power of political factors (including the rule of international law) which may favor defenders.

#### Nobody agrees – attribution alone collapses the aff

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.

### AT: Caroline/Proportionality/Imminence---1NC

#### The plan’s criteria are useless, gutting norms and causing escalation

Titiriga Remus 13 Assistant professor Inha Law School, 100 Inharo, Nam-gu Incheon 402-751, Korea. "Cyber-attacks and International law of armed conflicts; a “jus ad bellum” perspective." https://media.neliti.com/media/publications/28802-EN-cyber-attacks-and-international-law-of-armed-conflicts-a-jus-ad-bellum-perspecti.pdf

The opposing side argues that the reference to ‘inherent’ right of self-defense preserves ancient customary law, which allowed the anticipatory action.33 Proponents of a broad reading of self-defense invoke the 1837 Caroline incident and suggest that in the nuclear era States cannot be expected to wait for a ‘first strike’. However the majority of scholars reject the precedent value of the Caroline incident based on the fact that it precedes the actual interdiction for the use of force. 34They warn of the risk of escalation that results from accepting anticipatory actions. We think that the latter reason should prevail in the case of cyber-attack and as such, anticipatory self defense should be clearly banned. ii) Interceptive self defense If an armed attack is incipient or is on the verge of beginning, the intended victim may not wait powerlessly for the inevitable blow. The attack can be legitimately intercepted. In fact interceptive (different from anticipatory) self-defense seems to be acceptable under the Charter.35 The theme of interceptive self-defense is pertinent to a computer attack when the intrusion into a computer network has been discovered, although it is not yet lethal to persons or destructive of property (using Schmitt’s analysis). The issue is to determine whether the intrusion may reasonably be seen as a first step of an unavoidable and developing ‘armed attack’. This is a very difficult matter of evaluating and interpreting information available at the time of action (including warnings, intelligence reports and other data). 4. New Horizons and Challenges In the following section we will lance a debate about possible use of cyber means as self-defense or over the boundaries of the classical international paradigm (armed force or armed attack). There are numerous theoretical and practical challenges to be relived in this exploratory topic. 4.1 Computer Attacks as Means of Self Defense If a preceding armed attack (or a computer attack qualified as ‘armed attack’ –according to Schmitt’s analysis) occurred, the possibility to use the computer attacks as legitimate defense seem obvious (legitimate defense allows the use of all military means against an aggression therefore the cyber means should be included). However there are two substantive constraints for the right of self-defense: the criteria of necessity and proportionality. In the Nicaragua case, the International Court of Justice acknowledged the ‘inherent’ right of self-defense as part of customary law. The Court recognized the two criteria, ‘necessity’ and ‘proportionality’, as additional requirements under Article 51.36 i) ‘Necessity’ ‘Necessity’ means that no alternative way of redress may be available and the target should be a military one, in agreement with the rules of International humanitarian law (“jus in bello”). Likewise, ‘necessity’ requires that the timing between the armed attack and the recourse to self-defense to be reasonably short, taking into account the need to carry out investigations and/or negotiations, or to make military preparations (this is an upper time limit while the above discussed interceptive self-defense concerned the lower time limit). ii) ‘Proportionality’ ‘Proportionality’, on the other hand, supposes that the use of self-defense will be weighed against initial armed attack(s), not only in terms of gravity/intensity, but also in terms of duration, location, and range of selected targets. And here lays a real problem for cyber-attack qualifying as self-defense. Computer attacks are naturally uncertain as to the outcome they produce, making difficult to estimate deliberate and collateral damage. In fact the consequences of a cyber-attack may be both direct and indirect, and in some cases the indirect consequences can be higher than direct consequences.37 As result it is very difficult to fulfill the criteria of proportionality in case of a self-defense by way of cyber-attacks. The risk of escalation should prevent this use of cyber-attacks in the present international framework. An eventual solution may be revealed by technological breakthroughs that will allow controlling the outcome of cyber-attacks. But this kind of technological evolution is far from being assured yet. 4.2 Difficulties on the Boundaries of Classical Paradigm: Cyber Means Not Qualifying as “Armed Force” or “Armed Attack” Much more appealing might be an analysis of the use of cyber-attacks in response to an initial act (a computer network attack) not achieving the threshold of “armed attack” (Schmitt’s criteria). i) Computer network attacks not achieving the threshold of “armed attack” If an initial (cyber) attack does not reach the threshold of an”armed attack” there is no right of selfdefense. We should examine the case of a computer attack used in retaliation short of the right to selfdefense. This situation is not purely hypothetical since there are plans to use computer attacks as counter offensive instruments. For example Col. Charles W. Williamson 38 argued that an Air Force-controlled ‘botnet’ could be a cost-effective mean to protect military networks. He envisioned collecting computers that would otherwise be discarded and remove their hard drives by making them available to launch attacks against foreign-based computers targeting American military facilities. To prevent collateral damage this ‘botnet’ would have built-in filters preventing US military and government computers from being targeted. We think that Schmitt’s threshold of an “armed attack” by cyber means (and the corresponding right to self-defense) is not attained in the example above. At this point we are considering a non-military ‘retaliation’. However this kind of action brings up tremendous risks for cyber escalation linked to the obvious indiscriminate nature of computer attacks. All those affected by this computer retaliation may react with devastating (deliberate and collateral) effects to networks. This outcome could, by aggregation and escalation, finally trigger a classical armed conflict. The dangers are too high to consider this kind of action. i) The exception of espionage and the challenge of multi-purpose nature of cyber means If there is no destructive outcome (lacking the threshold in Schmitt’s analysis) the cyber means could be covered by the espionage exception in interstate relations. These are harmful actions (not illegal from the point of view of armed conflict) that each state use constantly. Nevertheless some problems related to the nature of cyber means remain unclear. Cyber means are by nature multi-purpose tools (‘weapons’). The methods used for computer network exploitation are similar to those used for computer network attack, but configured for different objectives. For example the Wall Street Journal claimed 39 that some agents from China and Russia, along with several other countries, had infiltrated computer systems charged with managing electricity in the US. They left behind software which could be used to control or disable electric grids of the country. Security experts stated that while the incident showed gaps in the US security infrastructure in time of conflict, such an attack could have catastrophic effects. In this case, a cyber-activity (intelligence-gathering) can easily become, if undetected, the ground for a future cyber-attack. In situations like this, the only solution for the offended State is to use its own cyber exploitation or cyber defense instruments while the use of computer attacks in retaliation would be the least reasonable choice (even less reasonable than in the above example of cyber retaliation to a previous computer attack not qualifying as “armed attack”). This is another example where classical armed conflict framework seems unable to cover certain cyber means characteristics.

### AT: Hybrid War---1NC

#### Non-cyber hybrid war thumps Baltic conflict

Fisher 15 [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.

#### The plan accelerates Russian cyber probing---adversaries will test redlines and circumvent escalation thresholds

Łukasz Kulesa 19, Deputy Head of Research at the Polish Institute of International Affairs (PISM). "The Future of Deterrence: Effectiveness and Limitations of Conventional and Nuclear Postures." https://carnegieeurope.eu/2019/11/28/future-of-deterrence-effectiveness-and-limitations-of-conventional-and-nuclear-postures-pub-80440

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.

#### Russian cyber probes produce a European SOI

David Takacs 17, Associate Fellow at Slovak Security Policy Institute. "Ukraine‘s deterrence failure: Lessons for the Baltic States." DOI 10.1515/jobs-2017-0001

Russia and its revisionist behaviour present the Baltic States with a multitude of threats, making deterrence a top priority in the Baltic Region. Not only does Moscow wish to extend its sphere of influence to include what it describes as ‘near abroad’, it must carefully protect its own model of ‘sovereign democracy’ at home. Prior to Russian involvement, Ukraine was getting close to signing an association agreement with the European Union (EU) and it was feared that ‘democratic change in brotherly Ukraine could spread to Russia’. Transforming Ukraine to a western democracy was seen as a threat to the Russian regime and was thus stymied at its source (Snegovaya, 2014). However, the Baltic States have already been fully integrated into NATO and the (EU) and have been stable democracies for over two decades now. So what is the nature of the threat that Russia presents to the Baltic States?

Putin is using hybrid tactics as a means of achieving his objectives of a politically restructured Europe. These include massive pro-Russian propaganda and misinformation campaigns, using economic levers, intimidation, or the employment of cyber warfare elements. In Ukraine in 2014, Russia has once again demonstrated its resolve to use both military and non-military means to create and fuel conflicts in pursuit of its wider geopolitical interests. The Kremlin is busily trying to regain its sphere of influence over nations that were formerly part of the Soviet Union, and the Baltic States’ governments are continuously being reminded to stay alert. In addition, NATO frontier allies face much more significant threats due to their proximity to the potential aggressor (Grygiel and Mitchell, 2016, p. 166). Thus, what NATO needs most to deter Russia is ‘to demonstrate robust political solidarity’ within the alliance (NATO Parliamentary Assembly Report, 2015, pp. 4-6). There has been a significant increase in Russian probing activities to gauge NATO’s commitment to the Baltic States over the past two years. Grygiel and Mitchell (2016, p. 43) define Russian probing as a ‘lowmintensity and low-risk test aimed at gauging the opposing state´s power and will to maintain security and influence over a region’. In case of the Baltic States, probing is aimed at the US and the strongest European countries, their power and their will to back up their most exposed allies. As mentioned by Grygiel and Mitchell (2016, p. 122), ‘there is a strong correlation between the existence of alliances in a given region and the effectiveness of deterrence against a threatening power’. Building on the allies’ fear of abandonment and US fear of entrapment in local conflicts, Russia is aiming to hinder their relationships which could ultimately provide Moscow with more room for probing and manoeuvring in the Baltic Region.

Hybrid or conventional?

#### Global war

Dr. Hal Brands 18, Henry A. Kissinger Distinguished Professor of Global Affairs at the Johns Hopkins School of Advanced International Studies, Charles Edel, Senior Fellow and Visiting Scholar at the U.S. Studies Centre at the University of Sydney and is the author of Nation Builder: John Quincy Adams and the Grand Strategy of the Republic, The Disharmony of the Spheres, https://www.commentarymagazine.com/articles/hal-brands/the-disharmony-of-the-spheres/

To see this, just work backward from the present. During the Cold War, a bipolar balance did help avert actual war between Moscow and Washington. But even in Europe—where the spheres of influence were best defined—there were continual tensions and crises as Moscow tested the Western bloc. And outside Europe, violence and proxy wars were common as the superpowers competed to extend their reach into the Third World. In the 1930s, the emergence of German and Japanese spheres of influence led to the most catastrophic war in global history. The empires of the 19th century—spheres of influence in their own right—continually jostled one another, leading to wars and near-wars over the course of decades; the Peace of Amiens between England and Napoleonic France lasted a mere 14 months. And looking back to the ancient world, there were not one, but three Punic Wars fought between Rome and Carthage as two expanding empires came into conflict. A world defined by spheres of influence is often a world characterized by tensions, wars, and competition.

The reasons for this are simple. As the political scientist William Wohlforth observed, unipolar systems—such as the U.S.-dominated post–Cold War order—are anchored by a hegemonic power that can act decisively to maintain the peace. In a unipolar system, Wohlforth writes, there are few incentives for revisionist powers to incur the “focused enmity” of the leading state. Truly multipolar systems, by contrast, have often been volatile. When the major powers are more evenly matched, there is a greater temptation to aggression by those who seek to change the existing order of things. And seek to change things they undoubtedly will.

The idea that spheres of influence are stabilizing holds only if one assumes that the major powers are motivated only by insecurity and that concessions to the revisionists will therefore lead to peace. Churchill described this as the idea that if one “feeds the crocodile enough, the crocodile will eat him last.”

Unfortunately, today’s rising or resurgent powers are also motivated—as is America—by honor, ambition, and the timeless desire to make their international habitats reflect their own interests and ideals. It is a risky gamble indeed, then, to think that ceding Russia or China an uncontested sphere of influence would turn a revisionist authoritarian regime into a satisfied power. The result, as Robert Kagan has noted, might be to embolden those actors all the more, by giving them freer rein to bring their near-abroads under control, greater latitude and resources to pursue their ambitions, and enhanced confidence that the U.S.-led order is fracturing at its foundations. For China, dominance over the first island chain might simply intensify desires to achieve primacy in the second island chain and beyond; for Russia, renewed mastery in the former Soviet space could lead to desires to bring parts of the former Warsaw Pact to heel, as well. To observe how China is developing ever longer-range anti-access/area denial capabilities, or how Russia has been projecting military power ever farther afield, is to see this process in action.

The reemergence of a spheres-of-influence world would thus undercut one of the great historical achievements of U.S. foreign policy: the creation of a system in which America is the dominant power in each major geopolitical region and can act decisively to shape events and protect its interests. It would foster an environment in which democratic values are less prominent, authoritarian models are ascendant, and mercantilism advances as economic openness recedes. And rather than leading to multipolar stability, this change could simply encourage greater revisionism on the part of powers whose appetite grows with the eating. This would lead the world away from the relative stability of the post–Cold War era and back into the darker environment it seemed to have relegated to history a quarter-century ago. The phrase “spheres of influence” may sound vaguely theoretical and benign, but its real-world effects are likely to be tangible and pernicious.

Fortunately, the return of a spheres-of-influence world is not yet inevitable. Even as some nations will accept incorporation into a Chinese or Russian sphere of influence as the price of avoiding conflict, or maintaining access to critical markets and resources, others will resist because they see their own well-being as dependent on the preservation of the world order that Washington has long worked to create. The Philippines and Cambodia seem increasingly to fall into the former group; Poland and Japan, among many others, make up the latter. The willingness of even this latter group to take actions that risk incurring Beijing and Moscow’s wrath, however, will be constantly calibrated against an assessment of America’s own ability to continue leading the resistance to a spheres-of-influence world. Averting that outcome is becoming steadily harder, as the relative power and ambition of America’s authoritarian rivals rise and U.S. leadership seems to falter.

### AT: I-Law Internals---1NC

#### NATO won’t shape I-law.

Aurel 1AC Sari 19, Senior Lecturer in Law, University of Exeter; Director, Exeter Centre for International Law; Fellow, Supreme Headquarters Allied Powers Europe; Fellow, Allied Rapid Reaction Corps, “The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats,” Harvard National Security Journal, Volume 10, <https://harvardnsj.org/wp-content/uploads/sites/13/2019/06/Mutual-Assistance-Clauses-of-the-North-Atlantic-and-EU-Treaties.pdf>

The legal challenges that hybrid threats present for collective security guarantees have been recognized at the highest political level. At their Warsaw summit held in July 2016, NATO’s member states confirmed their readiness to assist each other at any stage of a hybrid campaign and to counter hybrid warfare as part of collective defense.294 They also underscored that the North Atlantic Council “could decide to invoke Article 5 of the Washington Treaty.”295 They repeated these points at their Brussels summit in July 2018.296 By drawing an express link between hybrid warfare and collective defense, NATO leaders signaled their resolve not to allow Article 5 to be hollowed out.297 Still, their declarations of intent strike a rather conservative note. Whilst they accept that NATO may assist an Ally at any stage of a “hybrid campaign,” it is only in cases of “hybrid warfare” that they foresee a potential role for Article 5. This is not an unreasonable position to take. As we saw earlier, recourse to the use of force to counter hybrid threats falling below the threshold of an armed attack is neither permissible nor necessarily appropriate. A pledge to invoke the mutual defense commitment in response to every type of hybrid threat would be a promise to use the proverbial sledgehammer to crack a nut. It would be unrealistic and therefore lack credibility in the eyes of hybrid adversaries.298 By accepting that the role of Article 5 is confined to situations of hybrid warfare, the Warsaw and Brussels Summit Declarations avoid such empty gestures. However, in the same breath they also concede that the application of Article 5 is contingent on the legal threshold between warfare and peace, and thus vulnerable to subversion along the lines discussed in the preceding sections.

It may be tempting to deal with the problem of legal thresholds by attempting to escape them altogether, but this is not a feasible strategy. Even if the contracting parties were to revise Article 5 NAT and Article 42(7) TEU to avoid references to “armed attack” and “armed aggression,”299 they would remain bound by the rules governing the use of force under the UN Charter and customary international law. Although the member states of NATO and the EU make up an influential part of the international community, it is not within their ability to adjust these general rules of international law unilaterally. In any event, lowering the threshold for the use of force in order to facilitate the application of Article 5 and Article 42(7) would come with significant costs, since it would loosen the legal restrictions for all states, including hostile powers. The applicable thresholds therefore cannot be unilaterally modified at will and without the risk of unraveling key elements of the international legal order as it currently stands.

A more promising approach is to strengthen legal interoperability among NATO and EU nations. One line of effort is to reduce legal gray zones,300 for example by narrowing disagreements over the gap that lies between the definition of force and armed attack. This could prepare the ground for developing a shared understanding of what kind of hybrid threats may trigger the applicability of Article 5 NAT and Article 42(7) TEU. Given that the assessment of any security threat depends heavily on its context, it may prove somewhat sterile to build such a consensus in the abstract. Drawing on war-gaming and exercises may offer a more fruitful way forward. Bearing in mind how attractive the use of proxies is to a hybrid state adversary,301 developing a common approach to attribute their activities to the sponsoring state also merits attention. Although many aspects of the rules governing the attribution of wrongful acts are settled, certain questions could benefit from a joint posture.302 NATO and EU nations should also strengthen their collective mechanisms for unmasking attempts at plausible deniability in order to deny its use as a hybrid instrument,303 as illustrated by their united response to the Skripal incident and to Russian cyber operations.304

#### No norm consensus, compliance, or enforcement.

Ferry 18 Jean Pisani-Ferry, Economics Professor with Sciences Po of Paris and the Hertie School of Governance of Berlin, former campaign director for Emmanuel Macron and Commissioner-General of France Stratégie, the Founding Director of the think tank Bruegel. [Should we give up on global governance? Policy Contribution 17, October 2018, https://bruegel.org/wp-content/uploads/2018/10/PC-17-2018.pdf (table 1 omitted)]//BPS

C. Obsolescence of global rules and institutions Although the previous argument primarily rests on the broad pattern of international trade and finance, the adverse effects of external liberalisation can be compounded by inadequate governance. As far as trade is concerned, two cases in point are, first, inertia in the categorisation of countries, especially the fact that emerging countries, including China, still enjoy developing country status in the WTO; and, second, failures to enforce the adequate protection of intellectual property (an issue on which the EU recently joined the US and filed a complaint at the WTO against Chinese practices; see European Union, 2018). These grievances, and others concerning subsidies or investment, are not new: they were clearly spelled out by policymakers from the Obama administration (see for example, Schwab, 2011, and Wu, 2016). The underlying concern is that the systemic convergence on a market economy template that was expected from participation in the WTO has failed to materialise. The rules and institutions of global trade have brought shallow convergence but not the deeper alignment of economic systems that was hoped for. More generally, existing rules and institutions were conceived for a different world. This is very apparent in the trade field: the GATT/WTO framework dates from what Baldwin (2016) has called the “first unbundling” of production and consumption. They were not designed for the “second unbundling” of knowledge and production that gave rise to the emergence of global value chains. For decades, the implicit assumption behind the structure of trade negotiations has been that nations have well-defined sectoral trade interests: they are either exporters or importers. But in a world of global value chains, they are both importers and exporters of similar products simultaneously. Even if the principles of multilateralism remain valid, important features of the rules and institutions in which they are embedded are increasingly outdated. In the same way, opening to capital movements was supposed to result in net financial flows from savings-rich to savings-poor countries. What has happened instead is a massive increase in gross flows resulting in the interpenetration of financial systems and the coexistence of sizeable external assets and liabilities. The consequence has been the emergence of a global financial cycle (see for example Rey, 2017) and of policy dilemmas that are quite different from those arising in a simple Mundell-Fleming framework, in which interdependence takes place through net inflows and outflows of capital. Developments in the climate field further illustrate the point. The 1997 Kyoto Protocol was negotiated under the assumption that the bulk of greenhouse gas emissions would continue to originate in the advanced countries. But by the time the Protocol was meant to enter into force, it was clear already that the hypothesis was deeply wrong. The exemption of developing countries from emissions reductions was one of the reasons why the US did not ratify the treaty. The failed Copenhagen agreement of 2009 was an attempt to replicate Kyoto on a global scale, but there was no consensus for such an approach. Rules can be reformed and institutions can adapt. But this is a long and demanding process, especially when it requires unanimity, when participating countries have diverging interests and when changes require ratification by parliaments where there is no majority to support them. Global rules therefore exhibit a strong inertia that often prevents necessary adaptations. Trade rules, amendments to which require unanimity, are a case in point. Institutions are nimbler and can adapt to changing priorities or perspectives on interdependence. The IMF for example has succeeded in adjusting to major changes in the international economic regime and major shifts in the intellectual consensus. But even institutions face limitations to their ability to keep up with underlying transformations. This is one of the reasons why solutions to emerging problems have often been looked for outside the existing multilateral, institution-based governance framework (Table 1). D. The imbalances of global governance A further reason for popular dissatisfaction with global governance is its unbalanced nature. The deeper international integration becomes, the broader the scope of policy its management should cover, and the more acute the tension between the technical requirements of global interdependence and the domestically-rooted legitimacy of public policies. This is most apparent in the field of taxation. International tax optimisation by multinationals has become an issue of significant relevance and it is estimated that 40 percent of their profit is being artificially shifted to low-tax countries – with major consequences for national budgets (Tørsløv et al, 2018). But the fact that taxation remains at the core of sovereign prerogatives limits the scope and ambition of initiatives conducted at international level. The result, which can be regarded as an illustration of Rodrik’s trilemma, is that global coordination in tax matters falls short of what equity-conscious citizens regard as desirable and, at the same time, exceeds what sovereignty-conscious citizens consider acceptable. The imbalances of global governance are by no means limited to the taxation field. The same can be found in a series of domains, for example biodiversity and the preservation of nature. E. Increased complexity The final obstacle to multilateral solutions has to do with the sheer complexity of the challenges global governance has to tackle. In recent decades channels of international interdependence have both multiplied and diversified. They now link together countries with significantly differing levels of technical, economic or financial development. Because they have developed outside the scope of negotiated rules and established institutions, some of channels of interdependence also escape the reach of international agreements to an unprecedented degree. This is especially, but not only, the case of the internet and the multiple networks that rely on it. The world does not fit anymore the usual representation whereby individual nations trade goods, capital and technology. Even putting aside geopolitical consequences and assuming a shared commitment to openness and multilateral solutions, such complexity is bound to test the limits of existing international governance arrangements.

### AT: Gunboat Diplomacy---1NC

#### The U.S. is an alt-cause to gunboat diplomacy.

***1AC author*:** Patrick C. R. Terry 19, dean of the faculty of law at the University of Public Administration in Kehl, Germany, “The Return of Gunboat Diplomacy: How the West has Undermined the Ban on the Use of Force,” Harvard National Security Journal Volume 10, <https://harvardnsj.org/wp-content/uploads/sites/13/2019/02/Return-of-Gunboat-Diplomacy.pdf>

Although incompatible with Article 51 and not supported by sufficient state practice, a tendency is discernible whereby the United States and some of its allies, such as the U.K., Australia, and Israel are attempting to establish preventive self defense as yet another legal recourse to the use of force. The disadvantages and dangers of this strategy are manifold. The main weakness of “forcible counter-proliferation” is its ability to undermine stability in international relations and the rule of law.278 Its supporters seem to believe that it is possible to restrict the legality of such actions to cases where the United States or close allies deem them necessary—which is unrealistic and incompatible with sovereign equality.279 Once preventive self-defense is legal, there is no reason why India could not decide that it is necessary to preventively strike Pakistan, which possesses nu- clear weapons (or vice versa). Extended to other WMD, there are many more volatile situations which would seemingly justify the use of force280 and today’s ally is often tomorrow’s “rogue state,” and vice versa (Iran and Iraq being prime examples).281 Many western proponents of preventive self-defense also seem to believe that a state viewed by the United States and its allies as “rogue” is universally recognized as such, which is not the case.282 To others, the rule of law seems to be equivalent to U.S. rule, a view often confirmed when U.S. actions are claimed to have created new international law without any analysis of the practice or views of other states.283 It is, however, unlikely that other powerful states, such as China, Russia, or India will accept this U.S.-centric view. In conclusion, “preventive” selfdefense is not lawful, nor should it be. Nevertheless, many western states seek to undermine its ban.

### AT: Miscalc/Lashout---1NC

#### Ambiguity gives operational flex in crises – prevents underreactions and solves adversary restraint

Roggeveen 17 – Barbara Roggeveen research assistant at the Slavic Department of the University of Amsterdam, “NATO Needs an Offensive Cybersecurity Policy,” 8/8/17, https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-an-offensive-cybersecurity-policy/

Although NATO has been working toward a more comprehensive cybersecurity policy, there are two major challenges with its current strategy. The current plan places cyberattacks within the scope of Article 5 of the North Atlantic Treaty and the concept of collective defense, thus, creating high thresholds for engagement. In addition, it allows for mainly defensive and reactive measures, leaving less room for preventive or offensive operations.

NATO’s approach to cybersecurity can be traced back to early steps taken at the 2014 Wales Summit, in which NATO included cyber defense in its core tasks of collective defense. At the Warsaw Summit two years later, NATO recognized cyberspace as a “domain of operations,” reaffirming its defensive mandate with regard to cyber threats.

The Warsaw Summit Communiqué states that recognizing cyberspace as a domain of operations will “support NATO’s broader deterrence [of] and defense [against cyber threats],” and NATO promised to continue integrating cyber defense “into operational planning [to ensure] a better management of resources, skills, and capabilities.”

Armed attack-threshold

The designation of cyberspace as a domain of operations has far-reaching implications. As decided upon by Allied countries in the Tallinn Manual 2.0, such a label allows NATO to act only against those cyberattacks that qualify as an “armed attack.” In the case of cyberattacks, however, opponents often do not seek physical destruction. Of late, cyberattacks have moved further away from traditional warfare in pursuit of subtler influences , sometimes involving coercive political pressure. On July 28, the US Congress voted for new sanctions on Russia for its meddling in the 2016 US presidential election in favor of then-candidate US President Donald J. Trump.

By placing cyberattacks within the doctrine of collective defense, NATO limits its response to those cyberattacks that reach the armed-attack threshold, making it extremely difficult for NATO members to effectively address cyberattacks that do not qualify as such.

Whether a cyber operation constitutes an “armed attack” also depends on the parties involved. Traditionally, the right to collective defense could only be invoked in case of an armed attack undertaken by one state against another. NATO’s Strategic Concept allowed for a wider definition, stipulating that “the North Atlantic Treaty covers any armed attack on the territory of the Allies, from whatever direction or source.” Although this allows NATO to take defensive action against cyberattacks carried out by non-state actors, there is still some uncertainty within the community of allied countries as to when collective defense against non-state actors is permissible. One of the biggest challenges in this case remains attribution. It is often difficult to trace cyberattacks back to one specific organization.

From defensive to offensive capabilities

Currently, NATO’s cybersecurity strategy is strictly defensive. The NATO Computer Incident Response Capability (NCIRC) protects NATO’s own networks, and NATO supports allied members in their individual cyber defenses through intelligence gathering and sharing, the employment of high-readiness cyber defense teams, the development of targets for allied countries to facilitate national cyber defense capabilities, and investment in education, training, and exercise.

As James A. Lewis, director of the Strategic Technologies Program at the Center for Strategic and International Studies, wrote for the Tallinn Papers, a series of publications from the NATO Cooperative Cyber Defence Centre of Excellence, “a cyber defensive orientation is the equivalent of a static defense, defending fixed positions rather than maneuvering, and conceding initiative to opponents.”

Defensive measures might hold off an individual cyberattack, but they do not address the underlying threat. Although the protection of NATO members’ national networks should be a priority, the most effective way to provide sustainable and long-term protection against cyberattacks is through offensive capabilities and the destruction of opponent networks and systems.

While individual member states can take certain steps toward achieving this objective—the United States, for example, has already employed strong offensive cyber capabilities, such as Stuxnet—a collective NATO doctrine would provide allied countries with the necessary guidelines regarding proportionality and subsidiarity when employing offensive cyber capabilities. NATO’s cybersecurity policy should provide a clear framework to address the relatively uncharted territory of offensive cyber operations.

Recommendations

Current developments in the field of cybersecurity require a more proactive approach. In order to counter cyber threats, NATO should pursue a broader and more dynamic operational framework than that of collective defense. As the cyber capabilities of NATO’s opponents grow more sophisticated, the Alliance should adopt a cybersecurity policy that can effectively counter these threats.

### AT: PMCs---1NC

#### Russian PMCs are lagging behind

Soldat, a group of military experts, 1/29/18

(Soldat, “The Market is Divided PMCs, Russia Lags Far Behind”, https://soldat.pro/en/2018/01/29/5414/)

He agreed, that private military companies will be difficult to regain market share. "The world market is fully captured by the US and the UK. percent 95 PMC's market belongs to those countries. They perform a variety of functions - ranging from security and ending with accompaniment of strings... Try kerf on the market in any African country, where all captured, intercepted. We are already lagging behind many other countries. The market is divided. This business,it's not only fighting, yet, eg, protection of oil fields. Well, We have based on fierce competition incorporated. It's hard to compete with the US. If they enter into a contract of some, eg, for the protection, during the day can be aircraft of military transport aircraft to transfer several hundred cars. We have the possibility of, of course, modestly", - expert predicts, specifying, that the possibility of Russian and foreign PMCs until incomparable.

## Strategic Ambiguity Good

### 1nc - turn

#### Squo solves – locks in strategic ambiguity which is essential to deterrence – motivates adversaries’ self-restraint - non-article 5 responses solve their offense

Michaela Prucková 22 - Masaryk University/NATO CCDCOE Law Branch. (“Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO,” CCDCOE, 2022, <https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/> ) PJW

In reporting on the unfolding events in Ukraine, media and social platforms have repeatedly discussed as novel the possibility of Article 5 of the North Atlantic Treaty being triggered by a cyber attack on one or more Member States. This article presents a brief overview of the topic and explains that the possibility a cyber attack could lead to the invocation of Article 5 has been established since 2014; hence it is not a novelty and definitely not a response to the latest events on NATO’s eastern flank.

NATO’s cornerstone

Article 5 of the North Atlantic Treaty, NATO’s founding document, stipulates that:

‘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-defence recognised 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.

Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.’

As one of the core provisions of the Alliance, Article 5 confirms solidarity amongst Member States (Allies) in the event of an armed attack, which can be summarised as one for all, all for one in the spirit of Alexandre Dumas’s musketeers. Collective defence does not involve merely using armed forces and sending military units; rather, it binds Allies to provide **possible** and appropriate help to the affected Party.

In NATO’s history, Article 5 has been invoked only once, after the 9/11 terrorist attacks on the United States in 2001. That decision, first, showed solidarity with the US after the attacks and, second, enabled the country and the Alliance to take further steps in responding to them.

It is therefore clear that invocation of Article 5 is not an everyday measure but a major political decision on which all 30 Allies have to agree.

Article 5 in connection with cyberspace

The cyber agenda is not new to the Alliance’s portfolio; the first reference to cyber attacks appeared in the Prague Summit Declaration of 2002 (Para. 4). This type of public document reflects the outcomes of debates and decisions made at the highest political level of NATO Member States.

Since 2002, the cyber agenda started to increasingly appear in NATO’s documents until 2014 when the Wales Summit Declaration acknowledged for the first time the possibility of cyber attacks triggering Article 5. However, the relevant section (Para. 72) focuses on the potential attack’s effects and magnitude; it does not question a cyber attack’s ability to invoke Article 5 and is couched in terms of when, not if. In 2014, no one denied that operations in cyberspace could be equal in impact to conventional attacks.

At the next NATO summit in 2016, the Allies went even further by declaring cyberspace a new operational domain, taking its place alongside air, land and sea (Para. 70). The Warsaw Summit Communiqué thus reaffirmed cyberspace as part of NATO’s core task of collective defence, following the proclamation of 2014. The possibility of the invocation of Article 5 in reaction to a cyber attack was reiterated in 2021 in Para. 33 of Brussels Summit Communiqué. **On all those occasions, evaluation on a case-by-case basis was the guiding principle.**

The same applies to space and hybrid warfare. Space was declared the fifth domain of operations during the foreign ministers’ meeting in 2019 in the London Summit Declaration (Para. 6). The affirmation that attacks to, from or within space may invoke Article 5 was also reaffirmed two years later in the Brussels Summit Communiqué (Para. 33). As for hybrid warfare, the statements that it may invoke Article 5 have appeared, for example, in Para. 72 of Warsaw Summit Communiqué (2016) or Para. 31 of Brussels Summit Communiqué (2021).

A game-changing cyber attack

We need to keep in mind that cyber attacks have been a ‘persistent challenge‘ for years to NATO, with Russia being a stable originator of limited cyber activities, avoiding further escalation until now. None of the cyber incidents Allies has thus far experienced has led to the invocation of Article 5 and neither has the Alliance stated openly what level or damage the triggering attack would have to cause.

Even though this possibility is sometimes criticised for being a vague statement without clearly drawn lines, **it is also logical.** As NATO Secretary-General Jens Stoltenberg has stated, both the extent of such an attack and the Allied response under Article 5 ‘**must remain purposefully vague**‘. Hence, the Alliance does not provide potential adversaries with knowledge of the threshold between an everyday cyber attack (see, for example, the live map of ongoing attacks by FireEye) and an armed attack in cyberspace. This **uncertainty serves as a deterrent** and can motivate a potential adversary to exercise self-restraint in their malicious cyber activities and avoid launching a large-scale attack that could cross the blurred threshold. Such a position of strategic ambiguity is reflected in the documents which discuss evaluation on a case-by-case basis.

Put simply, **NATO does not want to weaken its position by revealing its red lines** and reaction measures in cyberspace. However, we are not entirely blind here. The Alliance has acknowledged, for example, that cyber attacks similar to the ones Estonia experienced in 2007 could lead to Article 5 invocation today.

Since the required gravity and impact of a game-changing cyber attack remain unclear, discussions emerge stirred by the events in Ukraine on what Russian actions in cyberspace aimed at NATO could or would lead to the invocation of Article 5. For example, Michael Schmitt provides an analysis of potential scenarios of Russia’s cyber operations and their interpretation under international law, not limiting the scope of events only to armed attack.

To summarise, responses to cyber attacks, attacks to, from or within space, and hybrid warfare are part of NATO’s collective defence and can, under certain circumstances, lead to invoking Article 5 of the North Atlantic Treaty. Both cyber and hybrid activities can be met with a range of proportional responses by NATO Member States, which can coordinate, for example, economic or diplomatic measures **without having to invoke Article 5**. This was stated in Para. 31 of the Brussels Summit Communiqué and by the Secretary-General himself during Cyber Defence Pledge Conference in 2018.

Threats of cyber attacks have featured in NATO policies since 2014. This understanding has developed as a natural response to the evolution of the threat landscape and is not a novelty of the events in Ukraine or an artificial tool aimed at increasing the current geopolitical tensions.

#### The plan removes flexibility and encourages adversary probing -- current Article 5 threshold properly responds to armed attacks

Z’hra **Ghavam 16** - Lieutenant Commander in the United States Navy with a B.S. from the United States Naval Academy. (“NATO’s Preparedness for Cyberwar,” September 2016, <https://www.hsdl.org/?abstract&did=801548> )

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.

#### The plan accelerates Russian cyber probing---adversaries will test redlines and circumvent escalation thresholds

Kulesa 19 [Lukasz; Nov 28; Deputy Head of Research at the Polish Institute of International Affairs (PISM); "The Future of Deterrence: Effectiveness and Limitations of Conventional and Nuclear Postures,” https://carnegieeurope.eu/2019/11/28/future-of-deterrence-effectiveness-and-limitations-of-conventional-and-nuclear-postures-pub-80440]

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.

### 2nc ov

#### Identifying cyber as an Article V issue creates arbitrary thresholds for armed attacks which can be exploited by adversaries – maintaining strategic ambiguity along with developing offensive capabilities is key to deterrence – turns the case

Roggeveen 17 – Barbara Roggeveen research assistant at the Slavic Department of the University of Amsterdam, “NATO Needs an Offensive Cybersecurity Policy,” 8/8/17, https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-an-offensive-cybersecurity-policy/

Although NATO has been working toward a more comprehensive cybersecurity policy, there are two major challenges with its current strategy. The current plan places cyberattacks within the scope of Article 5 of the North Atlantic Treaty and the concept of collective defense, thus, creating high thresholds for engagement. In addition, it allows for mainly defensive and reactive measures, leaving less room for preventive or offensive operations.

NATO’s approach to cybersecurity can be traced back to early steps taken at the 2014 Wales Summit, in which NATO included cyber defense in its core tasks of collective defense. At the Warsaw Summit two years later, NATO recognized cyberspace as a “domain of operations,” reaffirming its defensive mandate with regard to cyber threats.

The Warsaw Summit Communiqué states that recognizing cyberspace as a domain of operations will “support NATO’s broader deterrence [of] and defense [against cyber threats],” and NATO promised to continue integrating cyber defense “into operational planning [to ensure] a better management of resources, skills, and capabilities.”

Armed attack-threshold

The designation of cyberspace as a domain of operations has far-reaching implications. As decided upon by Allied countries in the Tallinn Manual 2.0, such a label allows NATO to act only against those cyberattacks that qualify as an “armed attack.” In the case of cyberattacks, however, opponents often do not seek physical destruction. Of late, cyberattacks have moved further away from traditional warfare in pursuit of subtler influences, sometimes involving coercive political pressure. On July 28, the US Congress voted for new sanctions on Russia for its meddling in the 2016 US presidential election in favor of then-candidate US President Donald J. Trump.

By placing cyberattacks within the doctrine of collective defense, NATO limits its response to those cyberattacks that reach the armed-attack threshold, making it extremely difficult for NATO members to effectively address cyberattacks that do not qualify as such.

Whether a cyber operation constitutes an “armed attack” also depends on the parties involved. Traditionally, the right to collective defense could only be invoked in case of an armed attack undertaken by one state against another. NATO’s Strategic Concept allowed for a wider definition, stipulating that “the North Atlantic Treaty covers any armed attack on the territory of the Allies, from whatever direction or source.” Although this allows NATO to take defensive action against cyberattacks carried out by non-state actors, there is still some uncertainty within the community of allied countries as to when collective defense against non-state actors is permissible. One of the biggest challenges in this case remains attribution. It is often difficult to trace cyberattacks back to one specific organization.

From defensive to offensive capabilities

Currently, NATO’s cybersecurity strategy is strictly defensive. The NATO Computer Incident Response Capability (NCIRC) protects NATO’s own networks, and NATO supports allied members in their individual cyber defenses through intelligence gathering and sharing, the employment of high-readiness cyber defense teams, the development of targets for allied countries to facilitate national cyber defense capabilities, and investment in education, training, and exercise.

As James A. Lewis, director of the Strategic Technologies Program at the Center for Strategic and International Studies, wrote for the Tallinn Papers, a series of publications from the NATO Cooperative Cyber Defence Centre of Excellence, “a cyber defensive orientation is the equivalent of a static defense, defending fixed positions rather than maneuvering, and conceding initiative to opponents.”

Defensive measures might hold off an individual cyberattack, but they do not address the underlying threat. Although the protection of NATO members’ national networks should be a priority, the most effective way to provide sustainable and long-term protection against cyberattacks is through offensive capabilities and the destruction of opponent networks and systems.

While individual member states can take certain steps toward achieving this objective—the United States, for example, has already employed strong offensive cyber capabilities, such as Stuxnet—a collective NATO doctrine would provide allied countries with the necessary guidelines regarding proportionality and subsidiarity when employing offensive cyber capabilities. NATO’s cybersecurity policy should provide a clear framework to address the relatively uncharted territory of offensive cyber operations.

Recommendations

Current developments in the field of cybersecurity require a more proactive approach. In order to counter cyber threats, NATO should pursue a broader and more dynamic operational framework than that of collective defense. As the cyber capabilities of NATO’s opponents grow more sophisticated, the Alliance should adopt a cybersecurity policy that can effectively counter these threats.

#### Lack of consensus turns the case – conflicting standards produce unclear thresholds that undercut deterrence.

Tertrais ’16 [Bruno; Deputy Director of the Foundation for Strategic Research, member of the committees of White Papers on Defence and National Security, former Special Assistant to the Director of Strategic Affairs at the Ministry of Defense; April 2016; “Article 5 of the Washington Treaty: Its Origins, Meaning and Future”; <http://www.jstor.com/stable/resrep10238>; NATO Defense College, No. 130] \*Edited in brackets for reading clarity.

The Alliance has made progress in deterring and protecting against such threats. Protecting against a limited ballistic strike from the Middle East was the rationale for NATO’s ballistic missile defense program. It is today an operational capability. The cyber threat is now recognized as having the potential to be considered, under some circumstances, an “armed attack.”16 But faced with a limited attack, NATO should not expect that Article 5 will be automatically, swiftly and unanimously declared (and the history of the past 25 years highlights the relevance of these doubts). If coming from Russia, it should be expected that several member states will hesitate before taking steps that may commit them to war with Moscow. This includes not only a “Northern contingency” (in the Baltic region or in the High North), but also a scenario where Russia forcefully responds on Turkish territory to what it would, rightly or wrongly, see as provocation by Ankara.

Attribution will be a problem in many instances; even assuming that this issue is solved, some member countries might hesitate in acknowledging the adversary’s responsibility, especially if the latter – as should be expected – embarks on massive propaganda aimed at influencing their public opinions.

Finally, a 30 plus-country alliance (if two or more countries joined) would be less likely to reach consensus on the urgency to declare Article 5 faced with a limited attack than it would have been when NATO included only half that number (which was the case during most of the Cold War). As a result, “what might count locally as an intolerable assault on the Baltic States’ sovereignty may not be seen in Brussels as an ‘armed attack’ for Article 5 purposes. [...] All the strength of the world’s mightiest military alliance will not amount to much if its members cannot agree when an aggressor has actually stepped over the line.”17

NATO should expect that its potential aggressors are smart. Having learned from the history of warfare and terrorism, an adversary could organize fake civilian accidents, launch false flag operations, embark on sabotage, commit acts of terrorism, abduct foreign citizens, claim a “right of hot pursuit” on Alliance territory under a false pretext, etc.18

Incursions of security forces and militia (so-called “little green men”) – a subset of what Russia calls “hybrid warfare” – are the hardest to deter and defend against. Northern European security analysts are right to ask the following question: “to what extent is NATO’s legal framework ready to deal with modern warfare? [...] Supposing a Crimea-like situation occurs in Narva, Estonia, for example. Can Article 5 be called on if there is no armed attack, but instead, what Russia would call a ‘democratic right of self-determination of the same nature as Kosovo and Crimea’?”19 It would be impossible to declare that any form of externally-induced political destabilization is an “armed attack.” A positive answer to the question asked would be impossible to reach unanimously and would stretch the definition of an “armed attack” to the implausible.

Legal history provides a useful guide to what an armed attack is in international law. The International Court of Justice (ICJ), in its seminal Nicaragua decision (1986), stated that it includes “the sending of or on behalf of a State of armed bands, groups, irregular or mercenaries” provided that said State has “effective” control [over] them. The International Criminal Tribunal for Yugoslavia, for its part, judges that “overall” control is sufficient.

#### And, the aff produces reluctance to invoke Article V early in a crisis. That “wait-and-see” posture complicates crisis escalation management later.

Murauskaite et al. ’19 [Egle Murauskaite, David Quinn, Catarina P. Thomson, Devin H. Ellis, Jonathan Wilkenfeld, Erik Gartzke; Senior Non-resident Fellow with the ICONS Project at the University of Maryland; 5/10/19; “Extended Deterrence Dilemmas in the Grey Zone: Trans-Atlantic Insights on Baltic Security Challenges”; <https://content.sciendo.com/view/journals/jobs/5/2/article-p5.xml>; Journal on Baltic Security, Vol. 5, Issue 2]

The first exercise was conducted in fall of 2016, in support of U.S. SOCEUR, and involved 29 expert respondents. The scenario vignette explored a series of suspicious Russia-linked incidents against Latvia: a cyberattack against the energy grid, an explosion in a Russian-language middle school, and staged protests in Riga. As Baltic, American, and Western European experts addressed these crises, several important findings emerged. The first was that both Latvia and its neighbour Lithuania delayed asking for Western assistance as long as possible – U.S. and/or NATO assistance in handling Russian interference was likely seen as the ultimate trump card to be called upon only at the darkest hour (which any individual grey zone crisis hardly qualified as, though their cumulative impact was approaching the threshold). The problem was that it significantly complicated escalation management, depriving allied decision-makers of a series of tools that could help de-escalate the conflict early and giving rise to more possibilities for the adversary to sow discord and ambiguity among the allies. The second important insight was that the EU played a significantly more important role than NATO in managing the grey zone crises – turning to NATO resources was seen as too escalatory a step. The third significant insight was that although the experts agreed at the outset on the importance for NATO and the EU to maintain a united front, during any particular crisis there was a tendency to conduct bilateral talks with Russia, trying to resolve the situation without involving the target state (i.e. Latvia) directly – which inevitably backfired.

### at: ambiguity dangerous

#### Even if they win ambiguity is dangerous, it is on balance beneficial – alternatives collapse deterrence by allowing adversaries to operate under critical thresholds

Davis 19 – Susan Davis, NATO Parliamentary Assembly, “NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence,” 4/18/19, https://www.nato-pa.int/download-file?filename=sites/default/files/2019-04/087\_STC\_19\_E%20-%20NATO.pdf

60. 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, but also poses distinct challenges.

61. 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 treading lightly. A similarly vague deterrence posture arguably worked well during the Cold War. However, ambiguity on where the threshold lies could indeed lead an opponent who is sufficiently comfortably with taking risks, to continuously exploit the ‘grey zones’, test the defender’s resolve, and conduct ever more daring cyber attacks.

62. 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. Arguably, the solution for such attacks cannot be found in deterrence, but rather in clearly defined policy response for hybrid operations. Despite its best efforts, the Alliance continues to struggle to develop such options. Setting specific thresholds without strong options for hybrid operations would only encourage more of them. Moreover, the Allies could also find it hard to agree on and perhaps also credibly commit to a specific threshold. Thus, on balance, the policy of ambiguity on thresholds makes sense.

63. 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. While NATO would retaliate in a proportional manner, it could do so through similar cyber attacks, air strikes, or worse. 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?

64. On balance, 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. That being said, in practice, this so-called cross-domain deterrence can be complicated, problematic, and difficult to control (Nye, 2017). For example, proportional response in the mind of the defender might look escalatory to the attacker.

### 2nc - uniqueness

#### Strategic ambiguity is explicit and consistent – no red lines

**Pearson, et al 22** – James Pearson is a European Cyber Correspondent for Reuters. Jonathan Landay is a National Security Correspondent at Thomson Reuters. (“Cyberattack on NATO could trigger collective defence clause – official,” Reuters, 02/28/2022, <https://www.reuters.com/world/europe/cyberattack-nato-could-trigger-collective-defence-clause-official-2022-02-28/> ) PJW

LONDON/WASHINGTON, Feb 28 (Reuters) - A cyberattack on a NATO member state could trigger Article 5, its collective defence clause, a NATO official said on Monday, amid concerns that chaos in cyberspace around Russia's invasion of Ukraine could spill over into other territories. The military alliance has for years made clear that a serious cyberattack could trigger the clause, but such a scenario has so far been largely hypothetical. "Allies also recognise that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as an armed attack," the official told Reuters. "**We will not speculate on how serious a cyberattack would have to be** in order to trigger a collective response. Any response could include diplomatic and economic sanctions, cyber measures, or even conventional forces, depending on the nature of the attack," the official said. Whether or not a cyberattack met the threshold of an attack large enough to trigger Article 5 was a "political decision for NATO Allies to make," they added. Britain and the United States have warned of potential cyberattacks on Ukraine which could have international consequences should, for example, malicious software designed to target networks in Ukraine start to spread elsewhere. read more There has also been concern among cybersecurity experts that Russia could team up with some of the gangs and people who release malicious software, such as malware used to hold Colonial Pipeline to ransom in the United States last year. U.S. Senate Intelligence Committee Chairman Mark Warner said there were no clear guidelines on how NATO (North Atlantic Treaty Organization) should respond, should such an attack take place. "These are things that have been in hypothetical discussion for a decade, but because we've not come to any universal conclusion on what those standards should be, what level of attribution is needed, we're kind of in a very grey area," he told Reuters. He posed the hypothetical case of a Russian cyberattack on Ukraine that impacts NATO member Poland, triggering power outages that result in hospital patients dying or knocking out traffic lights, causing fatal road accidents involving U.S. troops deployed there. "The West may have wanted **strategic ambiguity** in this area, and that **may still be the right choice**," he added. "But have we sufficiently made clear to the Russians the red lines on cyber or frankly to the NATO public, the American public, on red lines on cyber? I don't think we've done that."

#### The squo is goldilocks -- locks in strategic ambiguity over both cyber thresholds and responses as unofficial policy -- but there’s a strong norm against activating Article 5 against non-violent attacks.

Lynch '18 [Justin; 7/10/18; Associate Editor at Fifth Domain, contributor to the New Yorker, Foreign Policy, the Atlantic; "Cyber ambiguity: NATO’s digital defense in doubt amid unstable alliances," https://www.fifthdomain.com/international/2018/07/09/cyber-ambiguity-natos-digital-defense-in-doubt-amid-unstable-alliances/]

Today, the alliance counts cybersecurity as one of its core missions. It has placed a new cyber research center in the heart of the Baltic nation.

But amid what is viewed as a sustained campaign of Russian digital warfare on the West and the trans-Atlantic alliance ― whose foundations are being questioned through a surge of populism ― the very future of NATO’s cyber strategy is left intentionally murky.

During a May speech, NATO Secretary General Jens Stoltenberg said he is often asked under what circumstances the organization would trigger Article 5 in the case for a cyberattack.

Article 5 is the alliance’s principle of collective self-defense; an attack on one member nation is considered an attack on all member nations.

“My answer is: We will see. The level of cyberattack that would provoke a response must remain purposefully vague, as will the nature of our response,” Stoltenberg said. “It could include diplomatic and economic sanctions, cyber responses, or even conventional forces, depending on the nature and consequences of the attack.”

Questions over how NATO will respond to a cyberattack come as the alliance takes steps to bolster its digital protocols. In its joint air power strategy, unveiled in late June, NATO added cyberwarfare to its joint operations programs. The document boasts of the historic threat the organization faces: “For the first time since the end of the Cold War, the Alliance has to be able to conduct operations.”

In 2014, the alliance said for the first time that a cyberattack could trigger the organization’s collective-defense mechanism. It has proven a successful deterrent to combat large-scale digital attacks like the reported Russian cyber assault on Estonia in 2007, said Sorin Ducaru, a former assistant secretary general of NATO. But he added that the alliance has to be more creative in deterring medium- and low-grade cyberattacks “because that is the world we are living in.”

For Estonia, an aggressive NATO cyber policy could be the difference between the smooth withdrawal of cash or a disturbing “error” sign flashing on an ATM screen. An Estonian intelligence report from earlier this year predicts Russia will continue its campaign of aggression in Eastern Europe and the Baltic states through a combination of cyberattacks and information warfare.

When it comes to digital threats, “each country has faced them alone. NATO has not adopted a unified response,” former Estonia President Toomas Hendrik Ilves said during a May conference.

Today, nations are still loath to share information on cyberattacks, Ilves said, recounting a story about how as president he reported a hack on Estonia to NATO. “The response was: ‘Oh, you, too.’ I don’t think that’s how we should be doing things.”

Ilves is among those who have called for a cyber NATO ― an alliance of nations cooperating in digital defense.

The top civilian of Estonia’s Ministry of Defence also told Defense News that international cooperation could help thwart cyberattacks.

“I think people are realizing that we need international cooperation, and without international cooperation we simply cannot succeed in this new domain,” Jonatan Vseviov said.

Yet a bolstered NATO cyber response could mean a wave of new tension with Russia and China, which are seen as two of the alliance’s biggest digital challengers.

It is unclear under existing NATO rules how the alliance could be more aggressive in response to cyberattacks, said Alex Crowther, a senior research fellow at the National Defense University.

“In order for Article 5 to be voted on, it has to be something major. It pretty much has to be an armed attack or a use of force as discussed in the U.N. Charter. The most commonly adopted point of view is that people have to be hurt or killed, or property is damaged or destroyed,” Crowther told Fifth Domain, a sister publication of Defense News. “I have met people who say that the only attack that meets that criteria was the Stuxnet attack because it caused damage to Iranian centrifuges.”

Even the hack on Estonia did not meet the criteria for triggering the principal of collective self-defense, Crowther added.

### 2nc – uq – at: “cumulative”

#### “Cumulative” language changes nothing because it’s not defined – case-by-case is still the norm

Stefan **Soesanto 21** - Senior Researcher in the Cyber Defense Team at the Center for Security Studies (CSS) at the ETH Zurich. (“When Does a ‘Cyber Attack’ Demand Retaliation? NATO Broadens Its View,” Defense One, 06/30/2021, <https://www.defenseone.com/ideas/2021/06/when-does-cyber-attack-demand-retaliation-nato-broadens-its-view/175028/> ) PJW

In the 14 years since NATO first declared that a “cyber attack” could amount to an assault requiring collective action, alliance members have never made it quite clear what would constitute such an attack. But now they appear to be broadening the still-hazy definition.

Since the Wales Summit of 2014, analysts have largely worked under the assumption that a cyberattack would have to be as destructive as a kinetic attack to reach the legal threshold that would trigger defensive actions. This view was reinforced throughout the years by NATO’s use of the grammatical singular, i.e., “a cyberattack,” and the equivalency drawn between a kinetic attack and the effects and scale of a cyberattack.

At the Cyber Defense Pledge Conference in 2018, for example, NATO Secretary General Stoltenberg said, “NATO leaders agreed that a cyber-attack could trigger Article 5 of our founding treaty. Where an attack on one Ally is treated as an attack on all Allies.” As recently as June 7, Stoltenberg told the Atlantic Council: “In a way it sends a message that a kinetic attack can of course cause a lot of damage, and so can of course a cyberattack. It does not matter whether it is a kinetic attack or a cyberattack. We will assess as allies when it meets the threshold for triggering Article 5.”

With the publication of the NATO Brussels Summit Communique on June 14, the alliance fundamentally re-conceptualized how and what kind of adversarial activities can lead to crossing the threshold of an armed attack. The most important change: the insertion of the word “cumulative.”

According to paragraph 32 of the Communique, allies now recognize that “the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack.” Asked to clarify the insertion of the term ‘cumulative,’ the NATO press office responded that (a) the term was indeed used deliberately, and (b) the reason for using it is because the alliance has recognized that the cyber threat landscape is evolving, and that several low impact cyber incidents by the same threat actor can have the same impact as a single destructive cyberattack. The Estonian Ministry of Defense added via email that “it is paramount that we would also take into account long-term cyber operations and attacks that might cause cumulative damage equal to what a single cyber-attack could cause.”

The Communique itself still battles with the grammatical singular of “a cyberattack,” saying, “We reaffirm that 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**.” But gone is the sole equivalence to a kinetic attack. In addition, the alliance now also recognizes the impacts of “ransomware incidents and other malicious cyber activity targeting our critical infrastructure and democratic institutions, which might have systemic effects and cause significant harm.”

This means that NATO is finally inching away from cyberattacks as the metric of choice, and will hopefully move toward the more relevant unit of cumulative cyber activities – or in other words adversarial cyber campaigns. It is also positive to see that the threat of ransomware is receiving recognition as a security threat within the alliance. And it is good that NATO starts considering systemic effects resulting from malicious cyber activities – of which some might occur outside the alliance’s geographic area of responsibility. The 2012 attack against Saudi Aramco for example, could have posed a systemic threat to the majority of alliance members if oil and gas shipments were severely disrupted over a longer period of time.

But it remains unclear how NATO’s “cumulative” approach will work. What falls into this accumulation? Non-state ransomware campaigns? Non-destructive state-sponsored cyber espionage activity? And do these adversarial cyber activities have to occur in parallel, within a limited time, or are they continuously accumulated?

NATO’s press office has said the move toward “cumulative cyber activities” **should not be seen as lowering the threshold for triggering Article 5**, because (a) there is no clearly defined threshold to begin with due to NATO’s strategic ambiguity, and (b) triggering Article 5 will be discussed by the alliance members on a case-by-case basis – meaning **ultimately it is a political decision**. This argumentation is of course debatable and hinges upon how member states will calculate cumulative cyber activities and which member state will push for a precedent.

### 2nc – ambiguity good

#### Ambiguity deters attacks -- clarification encourages attackers and causes alliance disputes.

Davis '19 [Susan; 4/18/19; General Rapporteur to the NATO parliamentary Assembly Science and Technology Committee; "NATO in the Cyber Age: Strengthening Security & Defense, Stabilizing Deterrence," https://www.nato-pa.int/download-file?filename=sites/default/files/2019-04/087\_STC\_19\_E%20-%20NATO.pdf]

60. 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, but also poses distinct challenges.

61. 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 treading lightly. A similarly vague deterrence posture arguably worked well during the Cold War. However, ambiguity on where the threshold lies could indeed lead an opponent who is sufficiently comfortably with taking risks, to continuously exploit the ‘grey zones’, test the defender’s resolve, and conduct ever more daring cyber attacks.

62. 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. Arguably, the solution for such attacks cannot be found in deterrence, but rather in clearly defined policy response for hybrid operations. Despite its best efforts, the Alliance continues to struggle to develop such options. Setting specific thresholds without strong options for hybrid operations would only encourage more of them. Moreover, the Allies could also find it hard to agree on and perhaps also credibly commit to a specific threshold. Thus, on balance, the policy of ambiguity on thresholds makes sense.

63. 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. While NATO would retaliate in a proportional manner, it could do so through similar cyber attacks, air strikes, or worse. 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?

64. On balance, 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. That being said, in practice, this so-called cross-domain deterrence can be complicated, problematic, and difficult to control (Nye, 2017). For example, proportional response in the mind of the defender might look escalatory to the attacker.

#### The plan gives adversaries impunity to confidently act below the threshold -- case-by-case evaluation is intentional and advantageous.

Canbolat and Sezgin '16 [Mustafa and Emrah; December 2016; PhD in Management Science from McMaster University, Associate Professor of Operations Management and Business Analytics at the State University of New York; MBA as an International Military Officer from the Naval Postgraduate School, Senior Program Manager at Amazon; "Is NATO Ready for a Cyberwar?" https://www.hsdl.org/?view&did=810939]

One of the most discussed issues in the international arena after the 9/11 attacks was the Digital Disaster scenario that could be experienced in a member country (Bicakci, 2014). Many countries have incorporated cyber security strategies in their national security strategies in order to address cyber-attacks that could threaten the state. The role of NATO in the case of a serious cyberattack against a member country has been a conundrum.

Due to the difficulty of attributing a cyber-attack, NATO appears to have a pragmatic cyber security posture that handles each attack on a case-by-case basis (Burton, 2015). However, NATO officially stated that “NATO will consider (and potentially implement) a collective Article 5 response to cyber-attacks against NATO members, just as it did in response to the terrorist attacks on 9/11” (Burton, 2015, p. 308). Nevertheless, the threshold for the cyber-attacks that could invoke Article 5 is not certain. The head of NATO’s Emerging Security Challenges division, Jamie Shea stated that “[w]e are keeping that ambiguous so a potential aggressor does not get the idea they can carry out cyber-attacks up to a certain level with impunity” (Ashford, 2014, para. 8). Even though setting a specific and certain threshold would make it easier for NATO to determine when to invoke Article 5 against a cyber-attack, keeping it ambiguous gives an advantageous flexibility to the alliance regardless of the attack or adversary (Jones, 2015).

Article 5 was purposely left vague to give NATO more flexibility to assess a threat and determine a response. Therefore, it is also uncertain what kind of a response NATO would give against a cyber-attack. Would it be a cyber or a kinetic operation against the adversary if Article 5 were triggered? The answer to this question is deliberately left ambiguous, reinforcing NATO’s position that it will evaluate cyber-attacks on case-by-case basis.

#### Closing the window of escalation encourages adversaries -- their choice of grey-zone threats signals sensitivity to escalation.

Takahashi '19 [Sugio; 1/9/19; Chief of Policy Simulation at the National Institute of Defense Studies, MA in Political Science from Waseda University; "Development of gray-zone deterrence: concept building and lessons from Japan’s experience," The Pacific Review, Vol. 31, Issue 6, p. 787-810]

Third aspect of gray zone deterrence is that deterring states should never close the window for escalation. The main reason why the challengers use gray zone threats to change the status quo is that, first, they are discontent with the status quo and, second, they recognize their inferiority in conventional military challenge (Mazzar, 2015). The challenger may choose gray zone creeping expansion, rather than conventional military challenge, because the cost of conventional military challenge would easily exceed potential gain. Therefore, they may refrain from launching the challenge in the first place if they realize that their expansion has plausible risk of escalating to military conflict. The tripwire definitely has an effect that the challenger estimates higher possibility for escalation. If deterring states absolutely refrain from escalating countermeasures, the challenger side can continue gray zone creeping expansion eternally without taking any risk accompanied with escalation. In order to stop them, the deterring side needs to develop robust posture to win the possible war in the case of escalation, and make the challengers recognize the possibility of unfavorable military conflict. The critical role of military force, which cannot be substituted by other toolkit of statecraft, exists in this aspect of gray zone deterrence. And in this context, war-fighting capabilities still have an irreplaceable role to play.

#### ambiguity’s necessary to respond to unpredictable threats with maximum flexibility.

Jones '15 [Ken; March 2015; MS in Cyber Systems and Operations from the Naval Postgraduate School; "Cyber War: The Next Frontier for NATO," https://calhoun.nps.edu/bitstream/handle/10945/45201/15Mar\_Jones\_Ken.pdf?sequence=1&isAllowed=y]

To answer this question, it is important to look at the first (and only) time NATO invoked an Article 5 response; namely, following the 9/11 attacks on the United States. When the partners of the alliance first wrote the Washington Treaty, it was initially to deter the Russians from expanding and to deter nuclear warfare at the onset of the Cold War. Article 5 is purposefully vague to give NATO considerable room to maneuver. Before the 9/11 attacks led by Al Qaida, it would have been nearly impossible for anyone, anywhere, including the framers of the Washington Treaty, to imagine such an attack. Likewise, at the 2014 summit in Wales, NATO announced that it would and could invoke an Article 5 response to a cyber-attack, and that the ambiguity would stand.158 NATO’s Ambassador Sorin Ducaru, NATO’s assistant secretary general for “emerging security challenges,” made the following remarks:

[T]here’s no predetermined threshold…there was a conscious decision by the allies in this policy that there is benefit in keeping flexibility and ambiguity…article 5 was by design something that should be invoked politically by [member] nations in a specific context, on a case by case basis…article 5 was never designed to be triggered by a certain threshold. The only time it was invoked was after 9/11, which was a scenario that had never been contemplated by the founding partners.159 In this same vein, Christopher Painter, the U.S.’ State Department cyber coordinator said:

The NATO leaders’ declaration that international law including the UN Charter, the Law of Armed Conflict, international humanitarian law, etc. applies in cyberspace just like it does in the physical world…[t]his is a clear statement that this is not a lawless space. There was some doubt before. There was some thought you had different rules entirely for the cyber world than the physical world, which made no sense and in fact would be very destabilizing.160

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.

#### Strategic ambiguity necessary for offensive and defensive military flexibility

**Taddeo 17** - Associate Professor and Senior Research Fellow at Oxford and the Programme Director of the DPhil in Information, Communication and the Social Sciences at the Oxford Internet Institute (Mariarosaria, “Deterrence by Norms to Stop Interstate Cyber Attacks, “ Minds and Machines, September 17, <https://link.springer.com/content/pdf/10.1007/s11023-017-9446-1.pdf>) //nt-sg

In this scenario, state actors make policy decisions to protect their abilities to launch cyber attacks. ‘Strategic ambiguity’ is one of such decisions. According to this policy, states decide neither to define and nor inform the international community about their red lines—thresholds that once crossed would trigger state response—for non-kinetic cyber attacks (Taddeo 2011). Strategic ambiguity has often been presented as a way to **confuse the opponents** about the consequences of their cyber attacks. As the US National Intelligence Officer for Cyber Issues officer put it:

Currently most countries, including ours, don’t want to be incredibly specific about the red lines for two reasons: **You** **don’t want to invite people** to do anything they want below that red line thinking they’ll be able to do it with impunity, and secondly**, you** **don’t want to back yourself into a strategic corner** where you have to respond if they do something above that red line or else lose credibility in a geopolitical sense.

By fostering ambiguity, state actors also **leave open** for themselves a wider room for manoeuvring. Strategic ambiguity allows state actors to deploy cyber attacks for military, espionage, sabotage, and surveillance purposes **without being constrained** by their own policies or international red lines. This makes ambiguity a dangerous choice, one that is strategically risky and politically misleading.

#### Ambiguity solves deterrence.

Ziolkowski 15 – Dr Katharina Ziolkowski, a government director in the legal department of the Ministry of Defense. [NATO and cyber defence, Chapter 20 of *the Research Handbook on International Law and Cyberspace*, edited by Nicholas Tsagourias and Russell Buchan, Research Handbooks in International Law series, Elgaronline]

(i) Collective Self-Defence

The core task of NATO is collective self-defence. Article 5 of the North Atlantic Treaty states:

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-defence recognised 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.

In the past, it was debated whether or not this provision applied to malicious cyber activities. Neither a legal definition nor a universally accepted definition of the term ‘armed attack’ exists, and the term is open to interpretation. NATO Member States consider that malicious cyber activities can potentially constitute an ‘armed attack’ and trigger the right to collective self-defence. In the NATO Strategic Concept of 2010 they declared that ‘[c]yber attacks […] can reach a threshold that threatens national and Euro{Atlantic prosperity, security and stability’ and committed itself to continuing to fulfil its essential core tasks, inter alia, to ‘deter and to defend against […] emerging security challenges’, including cyber threats.46

Some authors47 assert that the Alliance needs to specify which malicious cyber activities will likely be deemed to constitute an ‘armed attack’ and judge the lack of such a declaration as a deficiency of the organization. However, the absence of such a specification can be considered as a politically wise and therefore favourable option. Drawing ‘red lines’ with regard to interpretations of key international security terms such as ‘armed attack’ is not always sensible. Retaining strategic ambiguity may maintain or support a deterrent effect. Accordingly, there is no ‘check-list’ specifying the level of tolerance of the 28 Member States with regard to traditional (e.g. kinetic) military activities directed against an Ally, and thus claiming the necessity of such a ‘check-list’ with regard to malicious cyber activities is unconvincing. Furthermore, the decision as to whether an armed attack is present will always be highly political and will never occur outside of a certain political context. Therefore, the determination whether a certain situation is or is not covered by Article 5 can only be undertaken on a case-by-case basis after comprehensive consultation between and by consensus of the organization’s 28 Member States, taking into consideration the political and security environment as well as all facts and circumstances of the case.

#### Ambiguity good.

Canbolat & Sezgin 16 – Mustafa Canbolat and Emrah Sezgin, Master’s Thesis. [Is NATO ready for a cyberwar? Naval Postgraduate School, http://hdl.handle.net/10945/51662

Due to the difficulty of attributing a cyber-attack, NATO appears to have a pragmatic cyber security posture that handles each attack on a case-by-case basis (Burton, 2015). However, NATO officially stated that “NATO will consider (and potentially implement) a collective Article 5 response to cyber-attacks against NATO members, just as it did in response to the terrorist attacks on 9/11” (Burton, 2015, p. 308). Nevertheless, the threshold for the cyber-attacks that could invoke Article 5 is not certain. The head of NATO’s Emerging Security Challenges division, Jamie Shea stated that “[w]e are keeping that ambiguous so a potential aggressor does not get the idea they can carry out cyber-attacks up to a certain level with impunity” (Ashford, 2014, para. 8). Even though setting a specific and certain threshold would make it easier for NATO to determine when to invoke Article 5 against a cyber-attack, keeping it ambiguous gives an advantageous flexibility to the alliance regardless of the attack or adversary (Jones, 2015).

Article 5 was purposely left vague to give NATO more flexibility to assess a threat and determine a response. Therefore, it is also uncertain what kind of a response NATO would give against a cyber-attack. Would it be a cyber or a kinetic operation against the adversary if Article 5 were triggered? The answer to this question is deliberately left ambiguous, reinforcing NATO’s position that it will evaluate cyber-attacks on case-by-case basis.

### 2nc – link

#### Squo solves – plan makes cyber deterrence dependent on Article 5 which guarantees miscalc

Dr. Jamie **Shea 18** - Senior Fellow for Peace, Security and Defence at Friends of Europe and former Deputy Assistant Secretary General for emerging security challenges at NATO. (“Cyberspace as a Domain of Operations What Is NATO’s Vision and Strategy?” MCU Journal vol. 9, no. 2, Fall 2018, <https://apps.dtic.mil/sti/pdfs/AD1068701.pdf> ) PJW

To reach these objectives, the alliance needs to become more involved in resilience, mapping its vulnerabilities, and exercising comprehensive business continuity plans. The counterhybrid support teams that the recent NATO summit decided to establish, together with the advisory support teams and lists of trusted suppliers managed by NATO’s Civil Emergency Planning Committee, can help allies ensure and demonstrate the resilience of their critical infrastructures.21 Memoranda of understanding also have been concluded between the NATO staff and 24 of its allies. They provide for points of contact and the sending of cyber rapid reaction teams and enhanced technical measures provided by the NATO Computer Incident Response Capability (NCIRC) Technical Centre to stricken allies upon request. These services help allies deal with specific incidents and collectively harness the diversity of the alliance when it comes to recovery options. This comes together with persistent cyberspace defense, which is not just the theoretical capacity to defend but the actual willingness to respond to all the many and regular cyber attacks **below the Article 5 threshold**. If NATO is **only willing to act once this red line has been clearly crossed**, and if it then has only heavy military forces with which to respond, it **risks miscalculation** by an aggressor regarding NATO’s resolve and unity. **NATO may end up deterring itself more than the aggressor** through fear of escalation and of an outright kinetic conflict. Here, strategic communications have a role to play in demonstrating that NATO is able to wield equivalent force in cyberspace as in the other domains. Increasing the visibility of cyber defense and highlighting the way in which cyber is being integrated into large-scale military exercises, such as the Trident Juncture or Trident Javelin series, conveys a message of capability and resolve. These efforts will not only dissuade would-be aggressors from attempting to intimidate any individual ally but also increase public confidence that NATO is addressing the evolving cyber threat. Some recent opinion pieces in the U.S. media, in particular calling for a “Cyber NATO,” have shown a lack of awareness of just how much effort NATO is actually making in this area.22 In fact, the alliance is already on its third Cyber Defence Policy and associated Cyber Action Plan since 2002.

#### Ambiguity key for maximum flexibility and effective deterrence

Mowchan 12 – Lieutenant Colonel in the US Army and an instructor at Center for Strategic Leadership (John, “On the Razor’s Edge: Establishing Indistinct Thresholds for Military Power in Cyberspace” United States Army War College, 4-23-12, https://apps.dtic.mil/sti/pdfs/ADA568852.pdf) //nt-sg

Ambiguous Thresholds. Ambiguous thresholds offer **several advantages** for employing military power following a hostile cyber-attack against government networks.

First, not establishing red lines allows government leaders the **flexibility** to tailor response options based on the hostile act, the **perpetrator** (state or non-state), its **effects** in the physical and digital world, and how they relate to the current state of affairs in the international system. As such, the employment of military power against a state-based threat would be much different than one against a non-state actor that conducted the same type of attack thus validating the necessity for ambiguous thresholds. For example, in 2009 individuals in China and Russia penetrated computer networks that operate parts of the U.S. electrical power grid. These individuals reportedly inserted malware that could destroy infrastructure components. Although the identities of the perpetrators or their associations with the Russian and Chinese governments were not disclosed, it validates the point that response options must be tailored since a **response** against hackers or hacktivists would be **different** from a response against the Chinese or Russian governments.

A second advantage is that the U.S. **does not disclose** all facets of its strategy to its adversaries. If cyber threat actors know what the U.S. will do in response to particular hostile acts in cyberspace, they will **adjust** their strategic approaches, **modify** their doctrine, and **develop** new cyber tactics, techniques or procedures that **skirt the red line**. Because neither the national nor the defense strategy for cyberspace explicitly defines a hostile act in cyberspace or how exactly the U.S. will respond, this leaves it open to interpretation. In 2009 General Kevin Chilton, Commander U.S. Strategic Command, stated, "I don’t think you take anything off the table when you provide [response] options to the president. **Why would we constrain ourselves** on how we would respond [to hostile acts in cyberspace]?" Such an approach is **no different** than how the U.S. addresses hostile acts **in the other global domains**. Hostile actions in cyberspace should be **no different**.

Finally, ambiguous thresholds **keep the adversary guessing** on how the U.S. will respond. As was brought out by one unidentified military official, “If you shut down our power grid, **maybe** we will put a missile down one of your smokestacks,” Again, ambiguity in when, how, and to what extent to use military power gives political and military leaders **maximum latitude** in developing a response.

#### Ambiguous red-lines force adversaries to self-restrain

Rehn 11 – Lieutenant Colonel in the US Army, U.S. Army Cyber Command Chief Technology Officer, and Director of the ARCYBER Technical Warfare Center (Steven, “Don’t Touch My Bits or Else!” US Army War College, 3-23-11, <https://apps.dtic.mil/sti/pdfs/ADA560247.pdf>) //nt-sg

\*\*edited for gendered language\*\*

Having a somewhat vague public policy is not necessarily **detrimental** in deterrence. Some ambiguity **complicates the cost analysis** an adversary undergoes to determine whether or not to pursue an attack. Hence, an adversary is **likely to refrain** from any action that may possibly invoke nuclear punishment even if ~~he doesn’t~~ [they don’t] necessarily know **exactly what level** of action does not invoke a nuclear response. **The mere threat** of a possible nuclear retaliation is enough to deter ~~his~~ [their] action

### 2nc – cyber probes impact

#### Russian cyber probes undermines NATO SOI

Takacs ’17 [David; 2017; Associate Fellow at Slovak Security Policy Institute. "Ukraine‘s deterrence failure: Lessons for the Baltic States." DOI 10.1515/jobs-2017-0001]

Russia and its revisionist behaviour present the Baltic States with a multitude of threats, making deterrence a top priority in the Baltic Region. Not only does Moscow wish to extend its sphere of influence to include what it describes as ‘near abroad’, it must carefully protect its own model of ‘sovereign democracy’ at home. Prior to Russian involvement, Ukraine was getting close to signing an association agreement with the European Union (EU) and it was feared that ‘democratic change in brotherly Ukraine could spread to Russia’. Transforming Ukraine to a western democracy was seen as a threat to the Russian regime and was thus stymied at its source (Snegovaya, 2014). However, the Baltic States have already been fully integrated into NATO and the (EU) and have been stable democracies for over two decades now. So what is the nature of the threat that Russia presents to the Baltic States?

Putin is using hybrid tactics as a means of achieving his objectives of a politically restructured Europe. These include massive pro-Russian propaganda and misinformation campaigns, using economic levers, intimidation, or the employment of cyber warfare elements. In Ukraine in 2014, Russia has once again demonstrated its resolve to use both military and non-military means to create and fuel conflicts in pursuit of its wider geopolitical interests. The Kremlin is busily trying to regain its sphere of influence over nations that were formerly part of the Soviet Union, and the Baltic States’ governments are continuously being reminded to stay alert. In addition, NATO frontier allies face much more significant threats due to their proximity to the potential aggressor (Grygiel and Mitchell, 2016, p. 166). Thus, what NATO needs most to deter Russia is ‘to demonstrate robust political solidarity’ within the alliance (NATO Parliamentary Assembly Report, 2015, pp. 4-6). There has been a significant increase in Russian probing activities to gauge NATO’s commitment to the Baltic States over the past two years. Grygiel and Mitchell (2016, p. 43) define Russian probing as a ‘lowmintensity and low-risk test aimed at gauging the opposing state´s power and will to maintain security and influence over a region’. In case of the Baltic States, probing is aimed at the US and the strongest European countries, their power and their will to back up their most exposed allies. As mentioned by Grygiel and Mitchell (2016, p. 122), ‘there is a strong correlation between the existence of alliances in a given region and the effectiveness of deterrence against a threatening power’. Building on the allies’ fear of abandonment and US fear of entrapment in local conflicts, Russia is aiming to hinder their relationships which could ultimately provide Moscow with more room for probing and manoeuvring in the Baltic Region.

Hybrid or conventional?

#### Global war

Brands ’18 [Dr. Hal; 2018; Henry A. Kissinger Distinguished Professor of Global Affairs at the Johns Hopkins School of Advanced International Studies, Charles Edel, Senior Fellow and Visiting Scholar at the U.S. Studies Centre at the University of Sydney and is the author of Nation Builder: John Quincy Adams and the Grand Strategy of the Republic, The Disharmony of the Spheres, https://www.commentarymagazine.com/articles/hal-brands/the-disharmony-of-the-spheres]

To see this, just work backward from the present. During the Cold War, a bipolar balance did help avert actual war between Moscow and Washington. But even in Europe—where the spheres of influence were best defined—there were continual tensions and crises as Moscow tested the Western bloc. And outside Europe, violence and proxy wars were common as the superpowers competed to extend their reach into the Third World. In the 1930s, the emergence of German and Japanese spheres of influence led to the most catastrophic war in global history. The empires of the 19th century—spheres of influence in their own right—continually jostled one another, leading to wars and near-wars over the course of decades; the Peace of Amiens between England and Napoleonic France lasted a mere 14 months. And looking back to the ancient world, there were not one, but three Punic Wars fought between Rome and Carthage as two expanding empires came into conflict. A world defined by spheres of influence is often a world characterized by tensions, wars, and competition.

The reasons for this are simple. As the political scientist William Wohlforth observed, unipolar systems—such as the U.S.-dominated post–Cold War order—are anchored by a hegemonic power that can act decisively to maintain the peace. In a unipolar system, Wohlforth writes, there are few incentives for revisionist powers to incur the “focused enmity” of the leading state. Truly multipolar systems, by contrast, have often been volatile. When the major powers are more evenly matched, there is a greater temptation to aggression by those who seek to change the existing order of things. And seek to change things they undoubtedly will.

The idea that spheres of influence are stabilizing holds only if one assumes that the major powers are motivated only by insecurity and that concessions to the revisionists will therefore lead to peace. Churchill described this as the idea that if one “feeds the crocodile enough, the crocodile will eat him last.”

Unfortunately, today’s rising or resurgent powers are also motivated—as is America—by honor, ambition, and the timeless desire to make their international habitats reflect their own interests and ideals. It is a risky gamble indeed, then, to think that ceding Russia or China an uncontested sphere of influence would turn a revisionist authoritarian regime into a satisfied power. The result, as Robert Kagan has noted, might be to embolden those actors all the more, by giving them freer rein to bring their near-abroads under control, greater latitude and resources to pursue their ambitions, and enhanced confidence that the U.S.-led order is fracturing at its foundations. For China, dominance over the first island chain might simply intensify desires to achieve primacy in the second island chain and beyond; for Russia, renewed mastery in the former Soviet space could lead to desires to bring parts of the former Warsaw Pact to heel, as well. To observe how China is developing ever longer-range anti-access/area denial capabilities, or how Russia has been projecting military power ever farther afield, is to see this process in action.

The reemergence of a spheres-of-influence world would thus undercut one of the great historical achievements of U.S. foreign policy: the creation of a system in which America is the dominant power in each major geopolitical region and can act decisively to shape events and protect its interests. It would foster an environment in which democratic values are less prominent, authoritarian models are ascendant, and mercantilism advances as economic openness recedes. And rather than leading to multipolar stability, this change could simply encourage greater revisionism on the part of powers whose appetite grows with the eating. This would lead the world away from the relative stability of the post–Cold War era and back into the darker environment it seemed to have relegated to history a quarter-century ago. The phrase “spheres of influence” may sound vaguely theoretical and benign, but its real-world effects are likely to be tangible and pernicious.

Fortunately, the return of a spheres-of-influence world is not yet inevitable. Even as some nations will accept incorporation into a Chinese or Russian sphere of influence as the price of avoiding conflict, or maintaining access to critical markets and resources, others will resist because they see their own well-being as dependent on the preservation of the world order that Washington has long worked to create. The Philippines and Cambodia seem increasingly to fall into the former group; Poland and Japan, among many others, make up the latter. The willingness of even this latter group to take actions that risk incurring Beijing and Moscow’s wrath, however, will be constantly calibrated against an assessment of America’s own ability to continue leading the resistance to a spheres-of-influence world. Averting that outcome is becoming steadily harder, as the relative power and ambition of America’s authoritarian rivals rise and U.S. leadership seems to falter.

## Assurance

### 1nc – assurance module

#### The plan shreds assurance

Baldor '18 [Lolita; 10/3/18; Associated Press reporter, citing Katie Wheelbarger, the principal deputy assistant defense secretary for international security affairs; "US to offer cyberwar capabilities to NATO allies," <https://www.fifthdomain.com/international/2018/10/03/us-to-offer-cyberwar-capabilities-to-nato-allies/>]

Acting to counter Russia’s aggressive use of cyberattacks across Europe and around the world, the U.S. is expected to announce that, if asked, it will use its formidable cyberwarfare capabilities on NATO’s behalf, according to a senior U.S. official.

The announcement is expected in the coming days as U.S. Defense Secretary Jim Mattis attends a meeting of NATO defense ministers on Wednesday and Thursday.

Katie Wheelbarger, the principal deputy assistant defense secretary for international security affairs, said the U.S. is committing to use offensive and defensive cyber operations for NATO allies, but America will maintain control over its own personnel and capabilities.

The decision comes on the heels of the NATO summit in July, when members agreed to allow the alliance to use cyber capabilities that are provided voluntarily by allies to protect networks and respond to cyberattacks. It reflects growing concerns by the U.S. and its allies over Moscow’s use of cyber operations to influence elections in America and elsewhere.

"Russia is constantly pushing its cyber and information operations," said Wheelbarger, adding that this is a way for the U.S. to show its continued commitment to NATO.

NATO Secretary-General Jens Stoltenberg told reporters on Wednesday that the inclusion of offensive cyber operations in alliance missions "is just one of many elements in our strengthened NATO cyber defenses." And he said that it's important to have cyber capabilities that can be used against the Islamic State group to destroy the networks they use for recruiting, financing and communicating.

He said that the British and Denmark have also agreed to make cyber contributions to NATO and he expects other allies will follow.

"We have seen an increasing number of cyber-attacks. They are more frequent, they are more sophisticated," Stoltenberg said. "We see cyber being used to meddle in domestic political processes, attacks against critical infrastructure. Cyber will be an integral part of any future military conflict."

Wheelbarger told reporters traveling to NATO with Mattis that the move is a signal to other nations that NATO is prepared to counter cyberattacks waged against the alliance or its members.

Much like America's nuclear capabilities, the formal declaration of cyber support can help serve as a military deterrent to other nations and adversaries.

The U.S. has, for some time, considered cyber as a warfighting domain, much like air, sea, space and ground operations. In recent weeks the Pentagon released a new cybersecurity strategy that maps out a more aggressive use of military cyber capabilities. And it specifically calls out Russia and China for their use of cyberattacks.

China, it said, has been "persistently" stealing data from the public and private sector to gain an economic advantage. And it said Russia has use cyber information operations to "influence our population and challenge our diplomatic processes." U.S. officials have repeatedly accused Moscow of interfering in the 2016 elections, including through online social media.

"We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of a crisis or conflict," the new strategy states, adding that the U.S. is prepared to use cyberwarfare along with other military weapons against its enemies when needed, including to counter malicious cyber activities targeting the country.

The document adds that the Pentagon will "work to strengthen the capacity" of allies and partners.

NATO has moved cautiously on offensive cyber capabilities. At the Warsaw Summit in 2016, allies recognized cyberspace as a warfighting domain. It has said that a computer-based attack on an ally would trigger NATO's commitment to defend its members. And last year the alliance agreed to create a new cyber operations center. But the focus has always been on defending NATO networks and those of its members, not offensive cyberwar.

#### Spills over.

Keifer, 11—Project Manager, Advanced Systems and Concepts Office, Defense Threat Reduction Agency (Michael, “Assuring South Korea and Japan as the Role and Number of U.S. Nuclear Weapons are Reduced,” <https://fas.org/irp/agency/dod/dtra/assuring.pdf>, dml)

For both the ROK and Japan, economic and cultural ties with the United States are strong and well established. The United States and its two key allies in the region share common values and cultural ties that are well ingrained. However, assuming the Chinese economy continues to expand, U.S. leaders may have to find innovative ways to ensure that this dimension of the relationship with Northeast Asian allies remains strong. Allies typically find common economic interests to be a tangible expression of a healthy bilateral relationship and, therefore, reassuring.

Allies in Northeast Asia are sure to watch closely any new developments in the NATO alliance and draw comparisons and contrasts. Therefore, as U.S. officials implement the new Strategic Concept in NATO and its implications for extended deterrence, it will be important to bear in mind how statements and actions will be perceived in Seoul and Tokyo.

#### Extinction.

Tanter ’17 [Richard; April 1; Senior Research Associate at the Nautilus Institute, Honorary Professor in the School of Political and Social Sciences at the University of Melbourne; The Asia-Pacific Journal, “Donald Trump’s Japanese and South Korean Nuclear Threat to China: A tipping point in East Asia?” Vol. 15, No. 2, Issue 7, <https://apjjf.org/-Richard-Tanter/5025/article.pdf>]

But in the longer run, apart from the direct risks of such an event for the U.S. itself, its East Asian alliance network, now in its seventh decade, founded on Japanese and Korean acceptance of U.S. nuclear primacy and a U.S. nuclear umbrella, would change dramatically, bringing with it, for better or worse, the end of U.S. hegemony in East and Southeast Asia (http://nautilus.org/napsnet/napsnet-special-rep orts/playing-the-japan-nuclear-card-did-the-ussecretary-of-state-reverse-five-decades-of-usnon-proliferation-policy/). Whether occurring on a Gaullist or British model, the foundations of Korean and Japanese relations with the United States would be irrevocably altered. Even leaving aside the obvious questions about the DPRK, in the event of a nuclearized Japan and South Korea, clearly the mathematical risks of nuclear war initiated in East Asia would be very much greater than even the current risks of India-Pakistan nuclear conflict. Regional nuclear security planning would be woven with multiple valences of possible perceived nuclear threats. The calculus of China-U.S. nuclear relations immediately becomes much more complex, with China facing two new potential threats, nominally at least coordinating with the U.S., in addition to the older concerns about India and Russia. For the United States, a nuclear-armed, fully ‘normalized’ Japan would never be the undoubted loyal lapdog of by then likely postUnited Kingdom Little England. And the calculations of a nuclear-armed South Korea and Japan about each other would start and finish in historically-conditioned suspicion.

At a global level, the U.S. opening the door to Japanese and Korean nuclear weapons could not fail to encourage a cascade of regional races to nuclear weapons, not only in the Western Pacific but in the Middle East, in Latin America, and quite possibly in Africa. The risks of regional nuclear war, with all its now thoroughly documented (http://www.psr.org/assets/pdfs/two-billion-at-ri sk.pdf) catastrophic environmental and climate consequences (http://www.readcube.com/articles/10.1002/201 3EF000205), would be both manifold and far higher than at present.

### 2nc – prolif impact

#### The entire world will be blanketed via miscalc -- extinction.

Cirincione **’20** [Joe; March 20; Former Vice President for National Security at the Center for American Progress; Responsible Statecraft, “Why Letting Our Allies Get Nuclear Weapons Is A Bad Idea,” https://responsiblestatecraft.org/2020/05/20/why-letting-our-allies-get-nuclear-weapons-is-a-bad-idea/]

There is nothing automatic about the nuclear domino theory, and it has been successfully countered in some regions, but the theory is generally correct. The Soviet Union got the bomb because, as Stalin told his scientists after Hiroshima, “The balance has been broken. Build the bomb. It will remove the great danger from us.” Britain and France got the bomb because the Soviets (and the U.S.) had it. China did the same, then India got the bomb because China did; Pakistan because India did.

Nuclear competition in Asia would not end if South Korea decided to build a nuclear arsenal. Others in the region would likely follow suit. Japan, Taiwan, perhaps Vietnam. Similarly, a Saudi bomb would likely beget an Iranian bomb, a Turkish bomb and even an Egyptian bomb. Far from making the region — and the United States — safer, these arms races would blanket the globe with nuclear tripwires, each primed to unleash unprecedented destruction at the slightest twitch.

Where you stand determines what you see. Kennedy and the other presidents stood atop the chain of command, and their own experiences with that awful responsibility (particularly with the near-miss of the Cuban Missile Crisis) colored how they saw nuclear politics. They recognized the limitations of theory in a world characterized by imperfect information and the frictions of human interaction. They understood what the nuclear theorists could not — that more countries having nuclear weapons would only increase the risk of their use, not lessen it.

Three months before the Cuban Crisis, Kennedy’s Secretary of Defense, Robert McNamara, gave a speech in Ann Arbor, Michigan where he laid out this danger. “The mere fact that no nation could rationally take steps leading to nuclear war does not guarantee that a nuclear war cannot take place,” he said. “Not only do nations sometimes act in ways that are hard to explain on a rational basis, but even when acting in a ‘rational’ way they sometimes, indeed disturbingly often, act on the basis of misunderstandings of the true facts of a situation. They misjudge the way others will react, and the way others will interpret what they are doing.”

Any attempt to rationalize nuclear relationships — treating adversaries like two sides of a balanced equation — removes the human factor: the tendency towards irrationality and error. In a world with just a handful of nuclear states, that factor has already nearly led to apocalypse. In a world with a dozen more, those risks would go up exponentially.

It does not have to be this way. For over 50 years, since the signing of the Nuclear Non-Proliferation Treaty, successful diplomacy, security assurances, and global norms have largely kept nuclear proliferation at bay. The nightmare scenario of dozens of nuclear states has so far been averted, in no small part through the conscious and continual effort of American presidential administrations of both parties. Yes, there will always be those who advocate for more nuclear weapons in more hands. But the forces of restraint, and with it, survival, have prevailed and can continue to prevail if U.S. policy leads the way.

#### They get the bomb in months.

Steff **’16** [Reuben; 2016; Senior Lecturer in International Relations and Global Security at the University of Waikato; Strategic Thinking, “Strategic Thinking, Deterrence and the US Ballistic Missile Defense Project: From Truman to Obama,” p. 139-140]

Commentators like Samuel Huntington and Zbiegniew Brezinski asserted that a world without US primacy would be a world of violence and disorder, less democracy and economic growth; American primacy facilitates global peace.1 Thus BMD was cast as inherently defensive; it enables the US to protect the global commons and international economic system that benefits all nations as the US assumes the role of a global-ordering superpower.2 Bush administration officials supported this position, in line with Hegemonic Stability Theory, holding that BMD could restore the freedom of action that would be lost in the second nuclear age, by allowing America to retain the capability to project power.3 There is some support for the nuclear age thesis. Firstly, nine states have nuclear weapons and apparently 49 countries have the know how to construct them.4 Secondly, to reduce greenhouse gases, many states may soon judge it prudent to construct nuclear power plants. Thirdly, states like Japan, Germany and South Korea have latent nuclear weapons potential and could apparently militarize their program in the space of a few months; Myanmar was suspected of having a covert program; Russia helped Iran build its Bushehr power plant and many states around the Persian Gulf are considering developing civilian programs. Syria also had a covert nuclear program until an Israeli strike in 2007.5 Finally, the IAEA is tasked with the contradictory mission of promoting the spread of nuclear energy for peaceful purposes and inhibiting its diversion to military purposes. These goals are not mutually exclusive as the former provides a path towards weaponization.6

#### Independent of the NPT -- allied prolif causes nuke war through accidents and terrorism.

McKenzie **’20** [Reuben; 2016; Independent Journalist Based in New Zealand; Defense One, “America’s Allies Are Becoming a Nuclear-Proliferation Threat,” https://www.defenseone.com/threats/2020/03/americas-allies-are-becoming-nuclear-proliferation-threat/164057/]

The consequences of proliferation among allies are dire. Miller explained that “the more countries with nuclear weapons, the more likely that a weapon gets used. That could be a deliberate attack, accident or nuclear terrorism.” Crucially, “the U.S. has adopted a strong stance against proliferation [because] we’re very worried about cascades or tipping points. If one [ally] gets nuclear weapons, it gives others incentives to do the same”.

### 2nc – assurance ov

#### Link turns case.

Jones 15 – Ken M. Jones, Naval Postgraduate School, Master’s Thesis. [Cyber war: the next frontier for NATO, Form Approved OMB No. 0704–0188, http://hdl.handle.net/10945/45201]

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.

#### Externally, strong NATO’s key to coordinate response to a laundry list of existential threats.

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

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

Now consider the alternative. American withdrawal from NATO would be a grave error. Not only would it surrender the above advantages and undo existing progress in Europe. It would also have negative long-term implications globally pertaining to America’s foremost long-term strategic challenge: namely, the People’s Republic of China. As Beijing extends its influence worldwide, U.S. disengagement from NATO would send the signal that the United States is an unreliable friend. America’s allies and partners in the Indo-Pacific would have to rethink the integrated security architecture we have painstakingly built since Eisenhower’s day. This is not to mention the obvious and immediate tactical and operational military advantages that would accrue to Russia in Europe, shifting the balance of power against the United States.

### 2nc – assurance link

#### The strength of Article V is breadth – U.S. activation is key AND coordination exists now.

Tucker 19 – Patrick Tucker is technology editor for Defense One. [NATO Getting More Aggressive on Offensive Cyber, 5-24-2019, https://www.defenseone.com/technology/2019/05/nato-getting-more-aggressive-offensive-cyber/157270/]

In the latest signal NATO is adopting a tougher posture against cyber and electronic attacks, Secretary General Jens Stoltenberg this week said that the defensive alliance will not remain purely defensive.

Stoltenberg told attendees at the Cyber Defence Pledge conference in London, “We are not limited to respond in cyberspace when we are attacked in cyberspace.”

NATO members have already “agreed to integrate national cyber capabilities or offensive cyber into Alliance operations and missions,” he said. But the parameters of a NATO response to cyber attacks remains undefined. In 2015, Stoltenberg said that a cyber attack against one member nation could trigger an Article 5 collective response by all members. Yet only once has a collective response ever been invoked, at the request of the United States following the attacks of September 11, 2001. NATO is a defensive organization, so what an offensive cyber posture looks like remains something of a mystery. An Article 5 response can take many different forms.

That’s the strength of the article, according to NATO Deputy General Secretary Rose Gottemoeller. However, while an Article 5 response can be unpredictable, it must be coordinated, which can be tricky with many different partners in possession of many different capabilities.

At an event in May, Gottemoeller said NATO was in the processes of establishing a new innovation board to “bring together all of the parts of and pieces of NATO that have to wrestle with these new technologies to really try to get a flow of information. Many of you having served in any international institution or government, you know how things can get stove-piped. So we are resolved to break down those stove-pipes, particularly where innovation is concerned,” she said.

NATO is building a cyber command that is scheduled to be fully operational in 2023 and will coordinate and conduct all offensive cyber operations. Until then, whatever NATO does offensively, it will rely heavily on the United States and the discretion of U.S. commanders, according to Sophie Arts, program coordinator for security and defense at the German Marshall Fund, who explains in this December report.

“Yesterday’s remarks indicate that NATO’s leadership is thinking more seriously about buttressing the alliance’s deterrence posture in cyberspace and address threats that fall under the threshold of an Article 5 violation,” she told Defense One.

“This tracks recent shifts in strategy adopted by several NATO allies, including the United States, which integrate offensive cyber operations as an important tool to proactively address growing instances of cyber interference from hostile actors.”

#### Maintaining ambiguous commitments is vital to assurance -- allies purposefully agreed to allow totally flexibility.

Kofman **’**16 [Michael; 2016; Analyst at CNA Corporation and Fellow at the Wilson Center’s Kennan Institute; War on the Rocks, “Fixing NATO Deterrence In The East Or: How I Learned To Stop Worrying And Love NATO’s Crushing Defeat By Russia,” https://warontherocks.com/2016/05/fixing-nato-deterrence-in-the-east-or-how-i-learned-to-stop-worrying-and-love-natos-crushing-defeat-by-russia/]

NATO’s best answer to compellence is strategic flexibility and ambiguity of response. While Article V dictates the defense of a member, it doesn’t stipulate what that defense must be, how it should take shape, or where it will be applied. With U.S. forces in place, NATO members can be assured that Article V will be triggered, but what happens next should be left a question mark. The more NATO emphasizes the Russian threat and argues for fixed forces in place, the less capably it can defend a challenge to its credibility as an alliance. Anyone can count the order of battle and the balance of forces. By introducing ambiguity in its potential response once Article V has been declared, NATO reduces the chance it can easily be manipulated into a credibility test. The objective should be shrouding a Baltic high-end fight in incalculable risk for Russia while maintaining uncertainty and strategic flexibility with air and naval assets.

#### The plan shreds assurance.

Stoltenberg 18 – Jens Stoltenberg, NATO secretary general and the former prime minister of Norway. [How NATO Defends Against the Dark Side of the Web, 9-6-18, https://www.wired.com/story/how-nato-defends-against-the-dark-side-of-the-web/]

If cyberattacks were physical attacks, using bombs or missiles instead of computer code, they could be considered an act of war. But instead, some are using software to wage soft-war with very real, and potentially deadly, consequences.

For almost 70 years, NATO has been the bedrock of transatlantic security, whether on land, at sea, or in the air. The same is now true in cyberspace. A cyberattack can now trigger Article 5 of NATO'S founding treaty, which states that an attack on one Ally is an attack on all Allies.

The level of cyberattack that would provoke NATO into a response under Article 5 must remain purposefully vague, as will the nature of our response. A clearly defined threshold only invites attacks immediately beneath it. That is the logic of deterrence. But NATO’s response could include diplomatic or economic sanctions, a digital counter attack, or even conventional force, depending on the nature and consequences of the attack. NATO will always follow the principle of restraint and act in accordance with international law.

Two years ago, NATO leaders pledged to invest more in cyber defense. Since then, almost every Ally has upgraded its cyber defenses, and we see countries like France, Britain and the United States investing heavily in their cyber defenses. NATO is helping all Allies to work together, to pool their knowledge and help each other.

NATO shares information about technological threats in real-time—as we did with the EU, nations and private companies during the WannaCry attack. We are integrating national cyber capabilities into NATO planning and operations. We have Cyber Rapid Reaction teams on standby to assist Allies 24 hours a day, while exercises, research, and training are led by the NATO Center of Excellence for Cyber Defense in Estonia, established after a huge cyberattack took down the websites of Estonian banks, media, and government bodies in 2007.

Being strong in cyberspace is now as important for our deterrence efforts as having strong conventional forces. Deterrence is about making the potential costs of an attack too high and the potential gains of an attack too low.

By agreeing that a cyberattack can trigger an Article 5 response by all Allies, the potential cost of action by an aggressor is high. But we must also lower the potential gains of any attack. Even the most advanced system is only as secure as its users. Some of the biggest cyberattacks have only been possible because of human error—picking up an infected USB drive placed in a parking lot and plugging it into a computer, say, or clicking on a bad link in a phishing email. It is time for us to wake up to the potential dangers.

In the Second World War, the saying was “loose lips sink ships.” Today it is using weak passwords, failing to update software programs, or opening unfamiliar emails. Simple things. But if we get them right, we go a long way to protecting ourselves.

The digital revolution has made our lives better. But, like in the physical world, there are dangers. NATO and NATO Allies are doing everything possible to keep our nations and our people safe, including in cyberspace.

#### Allies want more assertive cyber postures, NOT less.

Schneider & Herr 18 – Jacquelyn Schneider, Cyber Conflict Studies Professor at the U.S. Naval War College. Trey Herr, visiting fellow at the Hoover Institution. [Sharing is Caring: The United States’ New Cyber Commitment for NATO, 10-10-20, https://www.cfr.org/blog/sharing-caring-united-states-new-cyber-commitment-nato]

Given the recent blockbuster headlines about alleged Chinese snooping on server hardware sold to major technology companies and the latest joint-denunciation of Russian cyber operations, you could be forgiven for having missed an important NATO-related development. The Associated Press reports that the U.S. Defense Department will announce a new commitment to use offensive and defensive cybersecurity capabilities on behalf of NATO allies.

The new commitment is notable given how cybersecurity has long been treated as an exceptional domain of operations, and cyber capabilities reserved as strategic national assets to be shared with only the closest of allies. With this announcement, the Pentagon is suggesting that cyber capabilities might be used alongside conventional weapons with allies and indeed, equal weight appears to be given to offensive and defensive operations. Perhaps most significantly, the announcement moves NATO partners closer to what has been a tight coterie of U.S.-favored signals intelligence partners such as the United Kingdom, New Zealand, Australia, and Canada.

The DoD announcement is a sign of the continued, if nascent, normalization of cybersecurity under the current administration and in Europe. Even where offensive cyber operations may not rise to the level of war, they provide decision-makers with options to influence the geopolitical environment. This aligns with recent trends in the U.S. military to integrate cyber capabilities into maneuver units and large exercises, and reflects the shift towards more risk acceptant and offensive measures to counter cyberattacks found in the 2018 DoD Cyber Strategy.

Moving cyber capabilities into the same strategic frame as conventional weapons, especially with NATO, reflects a shift in institutional cyber arrangements within the United States and the growing power of the military relative to the intelligence community. For the United States, cyber capabilities have always had a complicated relationship with the intelligence community, in particular the National Security Agency (NSA). When Cyber Command stood up in 2010 as a sub-unified combatant command within the Department of Defense, it moved into the NSA’s headquarters, staffed its management ranks with longtime NSA employees, borrowed networks and technical capabilities, and to this day shares a dual-hatted commander. In the immediate years after the command was created, it was logical that the structure of partnerships with allies looked more like the special signals intelligence relationships formed around the NSA rather than traditional alliance networks in NATO and Asia. The recent announcement aligns cyber operations more closely with Department of Defense missions, which are more likely to posture capabilities for deterrent effects, than intelligence missions, which view capabilities as assets to be carefully husbanded.

Treating cybersecurity capabilities more like conventional arms and less like national assets also helps drive the integration of cyber operations into the planning and execution of a broader array of conventional military missions. Early cyber operations were largely conventional espionage and surveillance activities supercharged by the spread of computing and the internet. In the United States, this led to the creation of large and complex software tools, carefully guarded by the intelligence community as national assets (sometimes unsuccessfully). The DoD’s announcement indicates a move towards treating at least some of these capabilities, along with their supporting infrastructure, more like conventional armaments and making them available for broader use; a model closer to Central or Special Operations Command and less like the National Security Agency.

The Pentagon’s new commitment also reflects changes in how Europe talks about cybersecurity and characterizes the Russian threat. The last two years have seen a trend toward more open discussion of offensive cyber operations and the possibility of the alliance adopting more assertive postures to counter cyber operations against its members. After years of devastating ransomware attacks and cyber-enabled information attacks, NATO members are more willing to explore cyber triggers to Article 5. They have also been more willing to articulate the cyber threat against the alliance. In addition to last week’s denunciation by Dutch, UK, and U.S. authorities, Russian state actors are widely suggested to be responsible for an increasingly brazen series of operations, including targeting German government ministries, French and British TV stations, and more.

#### Limitations buck the trend – honoring collective defense requests is key to cyber-assurance.

Piret Pernik 14 {Piret Pernik is a Researcher of Strategy Branch of the NATO CCDCOE. Her main research areas are cyber security strategies and policies, horizon scanning and analysis of cyber threats, and the development of military cyber organizations. September 2014. “Improving Cyber Security: NATO and the EU.” https://icds.ee/wp-content/uploads/2010/02/Piret\_Pernik\_-\_Improving\_Cyber\_Security.pdf}//JM

Development of the approaches of NATO and the EU The principal focus of NATO’s cyber defence approach has always been the protection of its own headquarters, agencies, and operations. The Alliance has been improving its cyber defence capabilities since 1990s. The first well-known cyber incident against NATO took place in 1999 during NATO’s operation “Allied Force” in Kosovo when hacker groups from Russia and Serbia disrupted NATO’s internal systems.14 Few years later, at the Prague Summit in 2002, cyber security appeared for the first time on NATO’s political agenda with NATO declaring to “strengthen our capabilities to defend against cyber attacks.”15 In the same year, the North Atlantic Council (NAC) approved a Cyber Defence Programme and as part of this, the NATO Computer Incident Response Capability (NCIRC) - NATO’s emergency team to prevent, detect and respond to cyber incidents - was created.16 The cyber attacks against Estonia in 2007 that disabled its governmental, media and financial websites and the Russia-Georgia war in 2008 that included military offence against Georgian military forces and cyber attacks against Georgian webpages17 helped NATO to realize how it was behind in cyber space. Subsequently, the Alliance’s focus broadened from the security of its own networks to that of its member states.18 In January 2008 NATO approved its first Policy on Cyber Defence stressing “the need for NATO and nations to protect key information systems […]; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack.”19 In the same year, it established the Cyber Defence Management Authority (CDMA) to coordinate cyber defence, review capabilities and conduct appropriate security risk management across the Alliance. It also accredited the Cooperative Cyber Defence Centre for Excellence (CCD COE) with the main objectives to improve the interoperability of NATO and enhance cyber awareness, education, and training efforts. In 2009 cyber defence was rendered an integral part of NATO exercises. In 2010 the Lisbon Summit addressed cyber defence capabilities gaps including improvements to the NCIRC, and in the same year the Emerging Security Challenges Division was created within NATO International Staff with a mandate to analyse among other asymmetrical threats cyber threats. The Defence Policy and Planning Committee/Cyber Defence (from 2014 titled the Cyber Defence Committee) was also established to provide political-level guidance and oversight. In 2011 the Cyber Defence Management Board (CDMB, supplanted CDMA), which consists of NATO cyber experts at the political, military, operational, and technical levels was set up. Its purpose is to coordinate cyber defence activities throughout NATO and associated agencies, and to facilitate implementation of NATO’s cyber defence policies and capabilities.20 In June 2011 a revised Cyber Defence Policy was approved, confirming the resolve to protect NATO’s networks and assist member states in the event of cyber attack. It also commanded the establishment of two cyber Rapid Response Teams (RRTs) by the end of 2012 with a core of six professionals that can be deployed within 24 hours to a member state.21 Any NATO nation under cyber attack could request the team’s assistance through the CDMB22, the deployment must be approved by the North Atlantic Council (which may be politically challenging). The policy also defined minimum requirements to national networks critical to NATO’s core tasks and assistance to the Allies to achieve the minimum levels of security. Additionally, the Defence Policy and Planning Committee in Reinforced format (DPPC(R)) was set up to oversee the work of CDMB and manage the overall planning process, including cyber capabilities.23 In 2012 the NATO Communications and Information Agency (NCIA) was established.24

### at: no spillover

#### Spills over to all alliances.

Fitzsimmons 19 – Michael Fitzsimmons, research staff at the Institute for Defense Analyses, served previously with the US Army War College and the Office of the Secretary of Defense, PhD in international security from the University of Maryland. [Horizontal Escalation: An Asymmetric Approach to Russian Aggression?” Strategic Studies Quarterly 13.1. Spring 2019]

Also, deterrence and escalation outcomes in a regional crisis with Russia are critically important to the US beyond the direct local consequences of any conflict, grave as they may be. The US commitment to NATO’s collective defense is the lynchpin of American alliance commitments globally. Hence, even otherwise minor crises are likely to have long-term effects for US power and global security, in terms of demonstrating strengths, weaknesses, and levels of resolve in American defense of its stated commitments abroad.11

#### Reputational costs ensure the link.

Brown 17 – J Wellington Brown, MA Thesis at the School of Advanced Air and Space Studies. [Indispensable Nation: US Security Guarantees and Nuclear Proliferation, June, https://www.hsdl.org/?view&did=813351]

Defense agreements carry great reputational costs for US credibility. Beyond an implicit notion of public goods, the United States has made an explicit commitment to come to the defense of another state. To renege on these commitments would not only damage the United States’ reputation, but in the case of collective security agreements, it would undermine the entire collective security institution. These institutions, such as NATO, serve not only as collective defense against external threats, but also promote stability and reduce the security dilemma among members of the alliance. The United States’ interest in this regional stability is the basis of its credibility in upholding collective security agreements.

#### Link magnitude is huge.

Dodge 16 – Michaela Dodge, M.S in Defense and Strategic Studies, former Publius Fellow at the Claremont Institute. [A ‘No First Use’ Nuke Strategy Would be a Disaster for the US, 7-27-16, https://www.dailysignal.com/2016/07/27/if-the-obama-administration-adopts-a-no-first-use-nuclear-strategy-it-could-cripple-us-security/]

The second problem with the no first use policy is that about 30 nations around the world, close U.S. allies like Japan or NATO allies, rely on U.S. nuclear weapons for their own security. They rely on the United States to deter their nuclear-armed neighbors. North Korea habitually threatens South Korea with annihilation. North Korea’s ballistic missiles can reach Japan, another close U.S. ally. Russia is pursuing increasingly aggressive revisionist policies on the European theater. U.S. nuclear weapons have kept nuclear programs of allies at bay—and that is a very good thing as the complexity of the nuclear environment and thus the potential for miscalculation increases the more nuclear-armed countries exist. Facing dangerous neighbors and lacking U.S. assurances vis-à-vis devastating non-nuclear attacks, these countries would be undoubtedly more inclined to pursue their own nuclear weapons capabilities, complicating or thwarting U.S. nonproliferation efforts.

#### It triggers European proliferation.

Axe ’18 [David; July 2018; War and politics correspondent, citing the Atlantic Council’s Eurasia Center, the Arms Control Association, and Bruce Blair of Princeton University; The Daily Beast, “The Risk to the World: Massive Nuclear Proliferation,” <https://www.thedailybeast.com/the-risk-to-the-world-massive-nuclear-proliferation>]

"The loss of U.S. reliability to deter aggression against NATO Europe would prompt France and the U.K. to expand their nuclear capabilities and Germany and other non-nuclear countries to consider building their own nuclear arsenals despite strong public opposition," Blair said.

Some European officials are already thinking in those terms. In 2017, Jaroslaw Kaczynski, chairman of Poland’s ruling Law and Justice Party, called for Europe to build up a combined nuclear arsenal as powerful as Russia's own arsenal. Conservative German parliamentarian Roderich Kiesewetter [endorsed](https://www.economist.com/europe/2017/03/04/germans-are-debating-getting-their-own-nuclear-weapon) the idea.

If the United States were to leave NATO, Europe could build its own deterrent under the umbrella of a diminished NATO structure, or opt for a new structure based on the European Union. In the last decade or so, the E.U. has begun to establish a rudimentary military organization, but has deployed troops only rarely – and then mostly in Africa on peacekeeping duties.

The realignment could get complicated. Albania, Canada, Iceland, Norway and Turkey are in NATO, but aren't in the E.U. Austria, Finland, Ireland, Malta and Sweden are in the E.U., but aren't in NATO. Ireland, for one, is strictly opposed to nuclear weapons. "There are European Union members with nuclear capabilities, but how those capabilities would be employed outside of a NATO context – it's never been fleshed out," Simakovsky said.

#### That cascades.

Kroenig 15 – Matthew Kroenig, International Relations Professor and Chair at Georgetown University. [The History of Proliferation Optimism: Does It Have a Future? 38(1-2), Taylor & Francis]

Further Proliferation

Nuclear proliferation poses an additional threat to international peace and security because it causes further proliferation. As former Secretary of State George Schultz once said, ‘proliferation begets proliferation’65 When one country acquires nuclear weapons, its regional adversaries, feeling threatened by its neighbor’s new nuclear capabilities, are more likely to attempt to acquire nuclear weapons in response. Indeed, the history of nuclear proliferation can be read as one long chain reaction of proliferation.

Of course, reactive proliferation does not always occur. In the early 1960s, for example, US officials worried that a nuclear-armed China would cause Taiwan, Japan, India, Pakistan, and other states to acquire nuclear weapons.66 In hindsight, we now know that they were correct in some cases, but wrong in others. Using statistical analysis, Philipp Bleek has shown that reactive proliferation is not automatic, but that rather, states are more likely to proliferate in response to neighbors when three conditions are met (1) there is an intense security rivalry between the two countries, (2) the potential proliferant state does not have a security guarantee from a nuclear-armed patron (3) and the potential proliferant state has the industrial and technical capacity to launch an indigenous nuclear program.67 In other words, reactive proliferation is real, but conditional. To be sure, as Barry Posen has argued, Egypt, Saudi Arabia, and Turkey all have primitive nuclear infrastructures and it would be difficult for any of them to build nuclear weapons overnight.68 In addition, Turkey is a member of NATO and Saudi Arabia enjoys a close security partnership with the United States and these states might prefer to lounge in the shade of America’s nuclear umbrella rather than build independent arsenals. On the other hand, one or more of these states, much like the United Kingdom and France in the early days of the Cold War, might decide that America’s nuclear protection is insufficient. With a decade’s worth of dedicated nuclear development, any of these states could conceivably become nuclear powers. Just because reactive proliferation takes time, does not mean that it is not a problem. If Iran enters the nuclear club, therefore, it is likely that some, but not all, of the countries that we currently worry about will eventually become nuclear powers.

We should worry about the spread of nuclear weapons in every case, therefore, because the problem will likely extend beyond that specific case. As Wohlstetter cautioned decades ago, proliferation is an N+1 problem.69

In sum, nuclear proliferation gives us many reasons to fear the spread of nuclear weapons to additional states. While it is important not to exaggerate the above threats, it would be an even greater sin to underestimate them and, as a result, not take the steps necessary to combat the spread of the world’s most dangerous weapons.

### at: no prolif

#### Unilateral revision ensures prolif.

Lanoszka **’18** [Alexander; 2018; Assistant Professor Department of Political Science Balsillie School of International Affairs University of Waterloo; Cornell Studies in Security Affairs, “Atomic Assurance: The Alliance Politics of Nuclear Proliferation,” p. 149-157]

How do alliances curb potential or actual cases of nuclear proliferation, if at all? Many scholars argue that alliances are effective tools for bridling the nuclear ambitions of states. When allies do try to acquire nuclear weapons, their alliance relationships serve as conduits for the guarantor to coerce a nonproliferation outcome. In this book, I show that such optimism about the role military alliances play is overstated. Alliances can deter nuclear proliferation if they marry written pledges of support with compatible foreign policy and defense doctrines as well as in-theater conventional deployments. Yet alliances are prone to severe adjustments that can unsettle the ally. When guarantors make major unilateral changes to the security relationship, through undesirable doctrinal announcements or troop withdrawals, abandonment fears intensify. The affected ally becomes so doubtful of its received guarantees that it becomes more likely to engage in nuclear proliferation–related behavior. Unfortunately for the guarantor, curbing such behavior once it has started is very difficult. It requires fixing the broken security guarantee that prompted the nuclear interest in the first place. Nonmilitary tools like economic sanctions may be the best coercive instruments available, but their viability depends on the extent to which the ally relies on the guarantor. Simply put, alliances are better for deterring potential than for preventing actual nuclear proliferation.

The empirical cases support this argument. Table 2 summarizes the main findings. Fears of abandonment in West Germany intensified after July 1956 amid rumors that the Eisenhower administration would reduce the size of the US Army by a third. Shortly thereafter, West Germany joined France and Italy in a short-lived and unsuccessful effort to develop nuclear weapons. Throughout the subsequent decade, Bonn deflected calls for it to make clear nonproliferation pledges while obtaining enrichment and reprocessing capabilities. Its alliance with the United States certainly constrained its decision-making, but arguments that distinct coercion episodes prompted West German leaders to renounce nuclear proliferation are overstated. Domestic politics and prestige considerations were important factors as well.

Japan followed a somewhat similar trajectory. It began evaluating the strength of its received security guarantees more fastidiously following China’s nuclear device detonation in late 1964. Yet Japan did not begin making serious moves in investing in nuclear technology until the prospect of American withdrawal from Vietnam and even East Asia became highly likely at the end of the decade. Similarly to West Germany, Japan did not have an actual program dedicated to the production of an indigenous nuclear weapons capability. But like that of West Germany, Japan’s stance toward nuclear nonproliferation remained dubious. When Japan finally ratified the NPT, it did so largely because of domestic politics. Ideational arguments about the inherent value of the bomb were also influential. The United States provided assurances when asked to do so but had largely refrained from efforts to compel Japan into making nonproliferation commitments. Nevertheless, some controversy ensued not long after NPT ratification regarding activities at a Japanese reprocessing plant.

South Korea had a clear intent to acquire nuclear weapons. Despite South Korea’s weathering various provocations by North Korea, what triggered South Korea to seek nuclear weapons was Nixon’s unexpected announcement that the United States would withdraw one US Army division from the peninsula. Thankfully for Washington, South Korea depended on the United States for economic and technological goods, thus rendering South Korea vulnerable to American efforts in suppressing the program in 1976. Still, South Korea’s interest in nuclear weapons was not entirely snuffed out. Some speculate that the program went further underground. Whatever the truth, safeguard violations did occur in the 1980s.

Although I have not studied them at the same level of detail, the five smaller cases further corroborate the argument. Great Britain and France both sought nuclear weapons in part because of having to fight alone and without American support. What distinguishes Great Britain from France is that Great Britain came to depend on American technology for its nuclear deterrent. Great Britain still retains operational independence, but the French nuclear arsenal is fully autonomous from the United States. For its part, Norway remained satisfied with the security provided by the United States, so much so that it rejected having much of an American conventional military presence until the 1980s when it accepted pre-positioned gear from the US Marine Corps. Only very briefly at the beginning of the Cold War did Norwegian military leaders consider nuclear weapons. By contrast, Australia wanted more alliance goods but had no guarantor—whether the United States or Great Britain—that would supply them. On the basis of its security fears, Australia had a nuclear weapons program that it eventually renounced following a change in government. Alliance coercion arguably played no part. Finally, Taiwan began its attempt to produce nuclear weapons once it sensed that the geopolitical tide was turning against it. The United States gradually seemed more open to accommodating China, which had by that point come to possess nuclear weapons. What ensued was a cat-and- mouse game that spanned about two decades. The United States used different levers to ensure that Taiwan would not go nuclear, but its success in restraining Taiwan’s ambitions appears to have had more to do with intelligence than with sanctions per se.

The takeaway of this book is that alliances are better for deterring states from engaging in nuclear proliferation–related behavior than for compelling states to give up their nuclear weapons programs. In this chapter, I address the implications for theory and policy. In so doing, I outline possible avenues for future research as well as how my analysis sheds light on contemporary policy problems.

Theoretical Implications

My argument has several theoretical implications for how we should think about key questions in international relations theory. First, I show that my analysis bears on a contemporary debate in international relations regarding how beliefs about credibility are formed. Second, I argue that scholars are wrong to divide the study of nuclear weapons from that of conventional military power. Third, I add to the growing scholarship on the effectiveness of coercion in international relations by considering the alliance politics of nuclear proliferation.

THE BASIS OF CREDIBILITY

One major debate among international relations scholars concerns the basis of credibility: what makes threats—and, for that matter, promises—believable? A dominant school of thought holds that assessments of credibility turn on situational considerations like the war-fighting capabilities and geopolitical stakes involved behind the threats or promises that states make to one another.1 Policy makers are thus foolish to believe that they can develop reputations on the basis of their historical record for keeping or breaking commitments. This perspective has received criticism. For one, past actions communicate—intentionally or not—the interests that states have, whereas situational assessments depend partly on the historical record. 2 For another, this school of thought has mischaracterized the work of Thomas Schelling, which it has held responsible for the belief that commitments are so interdependent that reputations for keeping commitments are necessary for deterrence. Schelling instead argued that past actions matter in cases where states are continuously negotiating with each other, not in all coercive bargaining encounters.3

My findings further challenge the perspective that current, ahistorical calculations of power and interest determine credibility. I find that in attending to the foreign policy doctrines and conventional military deployments of their guarantors, allies accord importance to the local military effectiveness of their guarantors. Still, some actions undertaken by the guarantor can provide information as to its interests and foreign policy interests, especially if those actions include major and unfavorable military redeployments. In brief, my findings blur the distinction between reputation, on the one hand, and current calculations like power and interest, on the other hand. To be sure, I do not offer a systematic test as to the sources of alliance credibility. I examined narrowly how abandonment fears intensify so as to make states more likely to engage in nuclear proliferation–related behavior. Scholars should thus focus more on alliance credibility as a dependent variable.

NUCLEAR WEAPONS AND CONVENTIONAL MILITARY POWER

States form judgments about the security guarantees that they receive with reference to the conventional military capabilities that their guarantor could muster on their behalf for defense and deterrence purposes. The reason why allies look to the conventional capabilities of their guarantor is that they value deterrence-by- denial as much as they do deterrence-by- punishment, if not more. Indeed, from the perspective of allies like West Germany and especially South Korea, nuclear weapons are partly a means for offsetting the conventional superiority of adversaries, especially when those same adversaries possess nuclear weapons as well.

Unfortunately, scholars separate the study of nuclear weapons from that of conventional military power. Many studies of nuclear proliferation simply assume that nuclear weapons represent a special category, even though the factors that predict which states have nuclear weapons can also predict which states would have access to fifth-generation fighter jets, third-generation advanced tanks, ballistic missile capabilities, and so forth.4 In social scientific parlance, these studies neglect an important endogeneity problem, whereby conventional and nuclear weapons systems are related to each other. States that experience unfavorable alterations in their received security guarantees might opt for nuclear weapons, because they cannot develop sufficient conventional military capabilities for deterring an adversary in time. Some states, like Great Britain and France, acquire nuclear weapons because they already have most leading military technologies. Interestingly, the best works on conventional deterrence and military power neglect the nuclear dimension altogether.5 To take one example, excluding the role nuclear weapons have played in the Arab-Israeli conflict—as John Mearsheimer has done—could lead to mistaken understandings of how deterrence in general succeeds.6

THE EFFECTIVENESS OF COERCION

The core message of this book is that military alliances are better at preventing nuclear proliferation than stopping it once it has started. I have presented evidence that apparent success stories of alliance coercion are less than what they appear. What does this finding mean more generally for international relations scholarship?

Schelling famously wrote that compellence is harder than deterrence because the former seeks to change the status quo, whereas the latter seeks to maintain it. Much of the recent literature seems to support this maxim, notwithstanding the difficulties in empirically distinguishing deterrence from compellence.7 Drawing on data regarding compellent threats, Todd Sechser observes that strong states have trouble compelling weaker states because those weaker states worry that capitulation would lead to new demands. Their very strength leads strong states to underappreciate these reputational concerns.8 Using similar data, Todd Sechser and Matthew Fuhrmann show that nuclear weapons rarely confer any bargaining leverage on its possessors, since they are useless for territorial conquest and involve high costs as tools for punishment.9 Dianne Chamberlain finds that because using military force has become less costly for the United States, weak adversaries discount its threats.10 Dan Altman argues that states do not even bother with coercion at all in making territorial gains—they grab what they want rather than dispute a proposed territorial division in a crisis.11 Some disagreement exists among scholars. Kyle Beardsley and Victor Asal write that “the possession of nuclear weapons helps states to succeed in their confrontations with other states even when they do not ‘use’ these weapons,” whereas Matthew Kroenig argues that nuclear superiority confers an advantage in crisis bargaining.12

All these studies, however, focus on coercive bargaining between adversaries rather than between allies. When scholars examine military or nonmilitary threats that states make to their allies, the issue-area under dispute usually revolves around nuclear proliferation.13 My case studies show that alliance coercion in this domain is often difficult for the United States to do effectively. That is not to say that alliance coercion is never effective. Such a view would be sorely mistaken. Rather, my argument is that its effect is more subtle and indirect than commonly presumed. Still, a more general or comparative study of intra-alliance coercion would benefit international relations scholarship—one that encompasses other issues such as wartime coalition participation and peacetime burden-sharing. 14 Many empirical questions still need an answer. For example, is alliance coercion more effective in some issue areas than in others? Why or why not?

THE NUCLEAR SOURCES OF AMERICAN PRIMACY

The case studies also suggest that to understand the preponderant role of the United States in international politics, we should not overlook the nuclear dimension. Unfortunately, many existing theories of hierarchy and hegemony often view the world in largely conventional military terms, as the books of David Lake and John Ikenberry do.15 This oversight is problematic for the very reason that whatever one thinks of the global military presence of the United States, it is at least partly the product of a consistent desire to forestall nuclear proliferation. Daniel Deudney adds that “unipolarity, to the extent it still exists, is made much easier and more durable by nuclear weapons” because the deterrent effects they generate help stabilize interstate relations and inhibit encroachment and counterbalancing.16 Nuclear proliferation undercuts hegemony because it negates American power projection capabilities.

Claiming that nonproliferation has been as much a goal of American grand strategy as openness and containment might be a slight overstatement, however. 17 Sometimes other foreign policy goals get in the way—the Kennedy administration discovered this tension when it came to value nuclear nonproliferation while voicing its frustrations with the defense and monetary policies of West Germany. On occasion foreign policy goals are complementary so as to reinforce each other: quashing Taiwan’s nuclear ambitions was important for Sino-American relations. Moreover, the United States has good reason not to enshrine nuclear nonproliferation as an overriding priority that trumps all other foreign policy objectives: states would have an incentive to manipulate American interest in nonproliferation. Accordingly, despite what realists say about the lack of a central enforcer of rules in the international system, states would be able to “dial 911” for help by signaling some intent to acquire nuclear weapons.18 But partly because the United States has conflicting foreign policy interests, this option remains problematic for allies to use.

The nuclear dimension of American global leadership might, then, be more complicated than what seems to be the case at first glance. If the United States views nonproliferation as a goal unto itself, then it might be an offensive realist: that is, it uses whatever means to secure regional—if not global—hegemony at the expense of other states.19 In contrast, if nonproliferation is a goal that is either subordinate or complementary to other interests, then the United States might be a defensive realist. In other words, it might not see nuclear proliferation as problematic per se and can in fact be open to it, but it sometimes works hard to forestall it lest the spread of nuclear weapons would complicate other foreign policy objectives.20

GREAT POWER MANAGEMENT OF WEAKER STATES

This book addresses how American security guarantees can forestall nuclear proliferation. It does not investigate how the security guarantees of other major powers—namely, the Soviet Union and China—can affect the nuclear interest of their own security partners.

My argument has implications for understanding nuclear proliferation and nonproliferation within non-American alliance systems. Consider first the Soviet Union and its alliances.21 Romania was the only Warsaw Pact member out of seven to covet nuclear weapons, whereas both East Asian allies—China and North Korea— made efforts to acquire nuclear weapons in the Cold War with varying degrees of success. Despite the contiguity of the Soviet Union with all those countries, its security guarantees to them varied in quality. For better or for worse, none of these countries held the Soviet geopolitical interest and hosted Soviet armed forces to the same extent, if at all, as the industrialized Northern Tier of the Warsaw Pact (Poland, East Germany, and Czechoslovakia). 22 Romania might have been a member of the Warsaw Pact, but it perceived a growing disconnect between its security interests and those of the Kremlin between the late 1950s and early 1960s. In particular, it did not wish to be consigned to being the soft agricultural underbelly of the Soviet bloc.23 Moreover, the Soviet Union accorded so much significance to its holdings in Central and Eastern Europe that it cared less about developments in East Asia. Chinese and North Korean leaders might have reached this conclusion in the 1950s when the Soviet Union appeared disinterested in the fate of its communist partners during the Korean War.24 Those countries thus discounted Soviet support early and decided to develop nuclear weapons. And so the dynamics outlined in this book could very well be applicable to the Soviet context.25

My argument bears insights for how China has managed the North Korean proliferation problem. Interestingly, North Korea began considering whether to acquire nuclear technologies shortly after China withdrew its forces from North Korea in 1958.26 North Korea had good reason to discount Chinese security guarantees, formalized as they were with a 1961 mutual defense treaty. After all, China came to North Korea’s aid in the Korean War only when American-led forces approached the Yalu River. As Jonathan Pollack writes, Pyongyang “faced four decades of continuous nuclear threat . . . without a countervailing nuclear retaliatory threat of its own or allied nuclear deployments on its own territory.”27

But what has China done about North Korea? A common refrain is that China can and should do more to curb its ally’s destabilizing ambitions, especially since China is the main source of North Korea’s trade, food, arms, and energy.28 Despite how scholars sometimes argue that guarantors seek to prevent nuclear proliferation in order to preserve their standing and power projection capabilities, China appears exceptional in having shielded its ally from multilateral sanctions for the most part. One can argue that it has even free-ridden on American efforts to restrain Taiwan and South Korea without doing much of the same toward North Korea. However, my analysis yields two notes of caution. The first is that China might have perceived that reversing North Korea’s nuclear program was not in China’s interest, especially if China’s worries about regime stability, refugee flows, and a reunified Korea are legitimate. The second is that experts might be overestimating China’s ability to restrain its ally, especially when North Korea has by now developed certain missile capabilities and thermonuclear weapons. To be sure, Beijing could have at least forbidden North Korean citizens from receiving training in China—scientists who probably went on to participate in advanced weapons development in their native country.29 Still, in the improbable event that North Korea renounces its nuclear weapons, it would likely do so for non-alliance reasons.

Policy Implications

The policy implications of this study seem grim. Not only does the denuclearization of North Korea seem fantastical, but also any move toward acquiring nuclear weapons on the part of an ally would be extraordinarily difficult for the United States to reverse. The policy community should take small comfort in how American decision makers have restrained the ambitions of South Korea, Taiwan, and West Germany. The successes of those decision makers were at best overstated.

Yet there are upsides. One is that the United States can deter nuclear weapons interest among its allies. Given how vital strong security guarantees are toward this end, American decision makers thankfully have a say. More specifically, they can recalibrate doctrines and deployments so as to shape perceptions of credibility. Ally leaders appear to refer to these metrics in their own nuclear decision-making. We should thus remember that it is of the utmost importance that American defense planners take the time to think about the effects of their moves from more than just a budgetary or rational perspective. Having Marines in Okinawa might make little tactical or operational sense, but shifting them thousands of miles away could still be destabilizing. Symbols matter, and they may matter more from the perspective of allies than from the perspective of Washington.30 Nevertheless, the symbolic nature of such deployments should not be overstated. Allies value them because they believe such forces can put up a fight against an adversary should deterrence fail. In a world of anti-access and area denial (A2/ AD) military technology, a United States that practices offshore balancing might experience overwhelming difficulties in entering a theater of operations so as to aid an ally under siege. An onshore presence makes the United States look more capable and resolved to allies and adversaries alike.31 That said, withdrawing forces unilaterally might be counterproductive when it comes to having an ally bear a greater share of the collective defense burden. If the ally feels threatened by a nuclear-armed aggressor, then it might arm itself in ways that are to the detriment of the guarantor’s own interests.

Another upside is that decoupling does not make nuclear proliferation inevitable. 32 Because North Korea is developing capabilities so that it could strike the continental United States with nuclear weapons, some observers fear that Washington would become less likely to defend South Korea and Japan in order to avoid being attacked. Accordingly, those two allies sense that their interests are becoming decoupled from that of the United States and so would strive to secure themselves nuclear weapons of their own. Yet this fear is overstated. For one, they have already endured decoupling throughout the Cold War and after the Soviet Union and China had acquired survivable second-strike capabilities. For another, my analysis suggests that decoupling need not translate to nuclear proliferation as long as those allies believe that the United States would fight on their behalf and deny adversaries battlefield success. Providing hostages for the sake of extended deterrence is insufficient. Having aligned doctrines and in-theater deployments capable of inflicting harm on the adversary can influence such beliefs in a positive direction.

Perceptions of credibility are malleable, but we must be careful not to overstate idiosyncratic factors. Many analysts and experts worry that President Donald Trump’s unique style of communication can undercut deterrence and destabilize alliance relations. For example, in an excellent overview of his attitudes toward nuclear weapons, Jeffrey Michaels and Heather Williams caution that his use of social media could lead to misperceptions and miscalculations by friends and foes alike.33 According to this argument, an errant tweet would undermine American credibility. My analysis suggests that such concerns may be slightly exaggerated. A tweet is but one signal among many. Allies like South Korea and Poland will pay more attention to the military basis of their received commitments than to Twitter accounts in going about their nuclear decision-making.

#### Nuclear war.

Axe **’18** [David; July 16; MFA from the University of South Carolina; The Daily Beast, “The Risk to the World: Massive Nuclear Proliferation,” https://www.thedailybeast.com/the-risk-to-the-world-massive-nuclear-proliferation]

More realistically, the Americans leaving NATO would force European countries that currently lack nuclear arms to toss aside the 1968 Non-Proliferation Treaty and rush to acquire them, all in order to deter the Russians without the Americans' help.

The treaty's disintegration could then lead to countries all over the world pursuing their own nukes. "Trump is increasing the chances of the bomb spreading and the key treaty keeping the lid on such proliferation collapsing," says Blair.

Unconstrained nuclearization is one nightmare scenario that is becoming increasingly plausible as Trump escalates his criticism of the 69-year-old North Atlantic alliance. For three quarters of a century, American nukes have made it unnecessary for many European countries to possess nukes of their own.

Because of that, these countries could safely sign on to the Non-Proliferation Treaty, bolstering international efforts to limit nuclearization all over the world. "Among the benefits of NATO, a key one is that it has helped to prevent the spread of nuclear weapons," Kingston Reif, an analyst with the Arms Control Association, told The Daily Beast.

But that was long before Trump’s rise as a political force. In 2017, the former reality-T.V. star declared NATO "obsolete." In Brussels on July 11, Trump again questioned the organization's usefulness. "What good is NATO?" he asked. The next day at a meeting of NATO leaders, Trump threatened that he might "do his own thing" if alliance members didn't immediately increase their military spending.

Trump's words sent a chill through European capitals. The United States is by far the biggest military spender in NATO and, according to Mark Simakovsky, a fellow with the Atlantic Council's Eurasia Center, the "glue" that holds the alliance together. "Don't forget, there are huge divisions in Europe," Simakovsky said.

NATO's 29 member states range from illiberal Turkey, Hungary and Poland on the alliance's eastern flank to stalwarts France and Germany at the heart of the continent and the restive United Kingdom in the west.

At present just two non-U.S. NATO states – the U.K. and France – possess nuclear weapons. France fields around 300 nukes. The U.K., around 215. By contrast, the United States maintains an arsenal of no fewer than 3,800 atomic warheads, only slightly fewer than Russia possesses. The U.S. military keeps 180 warheads in Europe for use by its own forces and the forces of certain NATO members, most notably Germany.

Practically speaking, America is Europe's nuclear shield.

Under Article V of the NATO charter, an attack on any NATO state represents an attack on every other state – and the alliance is obligated to respond. That applies to a nuclear strike as well as conventional attack. If Russia nuked, say, Lithuania or Poland, the United States would be obligated to nuke Russia right back.

That mutual nuclear threat has helped to keep the peace in Europe since the Soviet Union exploded its first atomic bomb in a test in 1949, the same year as NATO's founding.

But with France and the U.K. possessing so few atomic warheads compared to Russia, deterrence in Europe could begin to collapse without American nukes. And that risk could drive European countries to create their own, more powerful deterrents – either collectively or individually.

"The loss of U.S. reliability to deter aggression against NATO Europe would prompt France and the U.K. to expand their nuclear capabilities and Germany and other non-nuclear countries to consider building their own nuclear arsenals despite strong public opposition," Blair said.

Some European officials are already thinking in those terms. In 2017, Jaroslaw Kaczynski, chairman of Poland’s ruling Law and Justice Party, called for Europe to build up a combined nuclear arsenal as powerful as Russia's own arsenal. Conservative German parliamentarian Roderich Kiesewetter endorsed the idea.

If the United States were to leave NATO, Europe could build its own deterrent under the umbrella of a diminished NATO structure, or opt for a new structure based on the European Union. In the last decade or so, the E.U. has begun to establish a rudimentary military organization, but has deployed troops only rarely – and then mostly in Africa on peacekeeping duties.

The realignment could get complicated. Albania, Canada, Iceland, Norway and Turkey are in NATO, but aren't in the E.U. Austria, Finland, Ireland, Malta and Sweden are in the E.U., but aren't in NATO. Ireland, for one, is strictly opposed to nuclear weapons. "There are European Union members with nuclear capabilities, but how those capabilities would be employed outside of a NATO context – it's never been fleshed out," Simakovsky said.

For Trump to even threaten to pull back America's atomic umbrella is dangerous, Simakovsky said. "What it encourages is instability."

And that instability – and the resulting mistrust between former allies – plays into the hands of Russian president Vladimir Putin. It could even, in the most extreme scenario, tempt Putin to launch his own limited nuclear strike in the context of a wider war in Europe.

In the last decade Russia has invaded two of its European neighbors – Ukraine in 2014 and the Republic of Georgia in 2008. Neither Georgia nor Ukraine is a full member of NATO, although both countries have signalled their desire to join the alliance.

The Eastern European states of Lithuania, Latvia and Estonia – all former Soviet republics – and Poland, formerly a Soviet satellite, are NATO members and view themselves as the main targets of Russia's aggression. This year, Russia deployed nuclear weapons to Kaliningrad, a Russian enclave on the Baltic Sea between Poland and Lithuania.

The Trump administration criticized the Russian deployment as "destabilizing." But the greater threat of destabilization comes from the administration itself as it continues to dismantle rhetorically a security structure that has preserved the peace – and deterred nuclear war – in Europe since 1949.

"If Putin somehow decides to cross the nuclear threshold, it won’t be because he thinks we don’t have enough nuclear weapons," Reif said. "It will be based on a political calculation that he has a greater stake in the conflict and we and our allies won’t be willing to run the risk of escalation."

The alternative is only less awful. That, in the absence of America's nuclear guarantee as part of a transatlantic alliance, Europe might build up a large nuclear arsenal of its own and supercharge global atomic proliferation. "Nothing would do more to cause nuclear anarchy than wrecking NATO," Blair said.

### at: prolif now

#### There’s no European prolif now because the NATO guarantee is strong.

Tertrais **’**19 [Bruno; July 29; Master’s Degree in Public Law of the University of Paris; Washington Quarterly, “Will Europe Get Its Own Bomb?” p. 56]

Still, as a study conducted by the European Council on Foreign Relations (ECFR) indicates, there is a continued general nuclear apathy in Europe as well as an unwillingness “to face up to the renewed relevance that nuclear deterrence ought to have in their strategic thinking.”43 The time is thus not ripe for grand initiatives that would entail the creation *ex abrupto* of a common deterrent, especially as long as NATO mechanisms are intact. As an EU scholar put it in a recent overview of the concept of “strategic autonomy:” “[T]here appears to be no Europe-wide willingness for a ‘European nuclear deterrent’ at present. In many European countries such a level of autonomy would symbolize the end of the transatlantic relationship as we know it today, pose a strategic liability for their national security, and, for many states, violate their neutrality or constitutions.”44

#### Allied prolif isn’t inevitable, but the plan flips assurances.

Lanoszka **’**18 [Alexander; 2018; International Relations Professor at the University of Waterloo; *Atomic Assurance: The Alliance Politics of Nuclear Proliferation*, “How Alliances (Mis)Manage Nuclear Proliferation,” Chapter 1]

Perhaps such pessimism is warranted amid the Teutonic shifts in international politics that attend the rise of China and the apparent decline of the United States. Yet the view that the future is unlike the past is an overstatement. American security commitments will come under stress, just as they have in the past. The difference may well be that the United States would not have the same clout over its allies as before if predictions of its relative decline are correct. If the United States had trouble suppressing the nuclear interest of industrializing allies like South Korea and Taiwan in the 1970s, then future nonproliferation efforts will be much more hard-pressed to achieve success. Nevertheless, as in the past, the United States may well continue to hold sufficiently strong military and technological capabilities over adversaries.35 As such, allies’ behavior could reflect how the United States decides to allocate its strategic attention and military resources more so than deep structural trends. Nuclear proliferation among allies is not inevitable, but the choice is for the United States to make in order to prevent it from happening.

### at: prolif slow

#### It’s on the brink.

Tertrais **’**19 [Bruno; July 29; Master’s Degree in Public Law of the University of Paris; Washington Quarterly, “Will Europe Get Its Own Bomb?,” p. 48]

But the context is now changing. If one describes the nuclear deterrence question as a matter of supply and demand, things have evolved on both ends:

– On the demand side, Russia’s new assertiveness and territorial aggression has triggered a renewed interest in Europe about the means to guarantee their existence and territorial integrity. This is true in particular not only for countries that became members of NATO at the turn of the century (such as Poland and the Baltic States) but also for EU members which are not members of NATO (Finland and Sweden) and thus do not rely on a formal U.S. guarantee, but worry about Russia. The end of the Intermediate-range Nuclear Forces (INF) treaty, as well as uncertainties about the future of the Iranian program, tensions in South Asia, and North Korean nuclear progress are additional reasons for Europe to reconsider deterrence.

– On the supply side, doubts about the reliability of the American guarantee to Europe have rarely been as strong as under the current U.S. administration. The brutality of Donald Trump’s tweets, body language and policies is unprecedented in transatlantic relations. This has led many in Europe, notably in Germany, to question the wisdom of relying solely on U.S. protection. In parallel, the European Union has consolidated its security and defense identity through the Lisbon treaty of 2009, and also taken more recent steps which were made easier by the prospect of Brexit. Also in 2009, France rejoined NATO’s military structure, a move which alleviated the suspicions of some of its partners about an alleged French intention to build a European security entity that would compete with NATO. Interestingly, while Paris was a leader in the European nuclear debate of the 1990s, this time, voices in Germany have been at the forefront.2

Thus, the time seems ripe for thinking anew about Europe’s nuclear role in securing the continent. This paper seek to dispel a certain intellectual and political confusion when one reads or hears about a “European deterrent,” a vague expression which covers a range of scenarios ranging from a declared European role for French (and possibly British) nuclear forces to a full-fledged “common Bomb” in the hands of Europe, and sometimes including a German nuclear program. Not all of them are realistic. This depends heavily on one key variable: will the current NATO nuclear arrangement continue to exist? So this paper will proceed with two sections—first on what could happen assuming the NATO arrangement continues and, second what could happen if it were to break down.

## AT: Lower A5 Threshold

### 1NC

#### Russian cyber-attacks won’t escalate now – but lowering the threshold for Article V ensures NATO vulnerabilities that Russia will exploit

Lonergan and Moller 22 - Erica D. Lonergan is an assistant professor in the Army Cyber Institute and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University. Sara B. Moller is a former Eisenhower Fellow at the NATO Defense College and will be joining the Center for Security Studies at Georgetown University later this year (Erica and Sarah, “Opinion | NATO’s Credibility Is on the Line with its Cyber Defense Pledge. That’s a Bad Idea,” Politico, 4-27-22, <https://www.politico.com/news/magazine/2022/04/27/nato-credibility-cyber-defense-pledge-russia-ukraine-00027829>) //nt-sg

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.

#### Russia will gradually push red-lines – that goes nuclear

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

Escalation: Can a NATO - Russia conflict be managed?

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

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

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

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

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

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

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

Conflict termination

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

### 2NC – Only Small Attacks Now

#### Russia only has the capacity for basic cyber-attacks

Wolff 22 - associate professor of cybersecurity policy at The Fletcher School at Tufts University (Josephine, “Why Russia Hasn't Launched Major Cyber Attacks Since the Invasion of Ukraine,” Time, 3-2-2022, <https://time.com/6153902/russia-major-cyber-attacks-invasion-ukraine/>) //nt-sg

But as the invasion continues with few signs of any sophisticated cyber conflict, it **seems less and less likely** that Russia has significant cyber capabilities in reserve, ready to deploy if needed. Instead, it begins to look like Russia’s much vaunted cyber capabilities have been **neglected** in recent years, in favor of developing less expensive, less effective cyber weapons that cause less widespread damage and are considerably easier to contain and defend against. For instance, many of the cyberattacks directed at Ukraine in the past month have been **relatively basic** distributed denial-of-service attacks, in which hackers bombard Ukrainian government websites and servers with so much online traffic that those servers cannot respond to legitimate users and are forced offline for some period of time. Denial-of-service attacks can be effective for short-term disruptions but they’re **hardly** a **new or impressive** cyber capability—in fact, they’re what Russia used to target Estonia more than a decade ago in 2007. Moreover, launching these types of attacks requires **no sophisticated technical capabilities** or discovery of new vulnerabilities, and they typically have fairly contained impacts on the specific, targeted computers. Similarly, recent reports that Belarusian hackers are trying to phish European officials using compromised accounts belonging to Ukrainian armed services members suggests that not only are these efforts relying on **fairly basic tactics** like phishing emails, they are not even being carried out by Russian military hackers directly.

#### Russia lacks the talent and will for major strikes

Lonergan et al. 22 - assistant professor in the Army Cyber Institute and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University (Erica D., “Putin’s invasion of Ukraine didn’t rely on cyberwarfare. Here’s why,” WaPo, 3-7-22, <https://www.washingtonpost.com/politics/2022/03/07/putins-invasion-ukraine-didnt-rely-cyber-warfare-heres-why/>) //nt-sg

Despite these predictions, the expected “shock and awe” Russian cyber campaign in preparation of the invasion of Ukraine **never emerged**. Moreover, while the conflict will undoubtedly evolve, cyber operations don’t appear to be playing a decisive role on the battlefield.

Surprised? We’re not. Academic research explains why cyber operations are **poor tools** of coercion — whether used independently or as part of conventional warfighting.

What clues do earlier Russian cyber operations give?

Scholarly research details Russia’s long history of cyber operations against Ukraine. Russia’s 2014 annexation of Crimea included cyber operations in parallel to kinetic ones. Distributed denial of service attacks, for instance, strategically flooded Ukrainian networks to crash operations. In 2015, Russia carried out a cyberattack against Ukraine’s power grid. And in 2017, Russia unleashed the data-wiping NotPetya virus, malware that targeted Ukrainian servers initially but quickly spread around the world.

Yet experts who inferred from Russia’s past behavior that the current conflict would be a “Cyber Pearl Harbor” moment may have been **drawing the wrong lesson**. There is little evidence that cyber operations provided Russia with an operational advantage in 2014 — let alone highly synchronized combined arms warfare. And the power grid attack — in the dead of winter — did not cause any deaths, and service was restored within hours.

Russia’s current cyber efforts have had **little impact**

Many of the recent cyberattacks aimed to fragment the trust Ukrainians have in their government — and these information operations clearly **haven’t been effective**. In mid-January, Microsoft and other monitors reported that destructive malware, “WhisperGate,” was targeting Ukrainian organizations.

#### Cyber doomsday scenarios are fantastical – states lack technical means and motive for advanced success

Rabkin and Yoo 17 - Jeremy Rabkin is Professor of Law at George Mason University and John Yoo is the Emanuel Heller Professor of Law at the University of California at Berkeley (Jeremy and John, *Striking Power*, pages 98-99, 2017) //nt-sg

There are **good reasons** to doubt that even these cyber operations will produce the nightmares drawn by Richard Clarke and other alarmists. The first obstacle is the **scale of the technical challenge**. A hostile power cannot simply aim a general-purpose cyber weapon at a target system. To take control of a network, the hackers **must custom design** a special program to penetrate the system. The developers of the cyber weapon must have a **detailed understanding of the network**, which may take **years of snooping** inside that system. If the target is disconnected from the Internet, as the Iranian nuclear facility was, the attacker must infiltrate a closed local network. That may prove feasible, but it requires **highly specialized and sophisticated intelligence**, so that attackers can infiltrate the target system by way of other computers with which it may regularly interact.

The challenge is greater still if the aim is not simply to shut down the target system but to change its operations, as with Stuxnet. The hackers must then **figure out how to disguise their program** to evade detection by network security teams. The Stuxnet virus is reported to have taken **four or five years and billions of dollars** to develop. Among other things, the developers built their own model of the Iranian nuclear facility.22 Stuxnet took over the supervisory control and data acquisition program (SCADA) of the Iranian centrifuges. As engineers have pointed out, "the complexity of SCADA systems is one of the best defenses against attack," because their complexity would prevent all but the most patient, expert, and highly informed hackers from redirecting their operations.23

To accomplish a doomsday scenario, an enemy would have to make **a huge investment in research and development** for each individual target. Enemies are **not likely to build models** of each mass transit system in the U.S. to work out the right attack program for the controls on that system. Even if they did, they could not expect that all of their efforts would **go undetected**. If even one such attack were detected or went off ahead of schedule, it would prompt **immediate security checks** on other transit systems. On the other hand, regular changes in the control systems, which might be updated for any number of reasons, could **throw off years of preparation** by the hackers. Achieving a simultaneous attack on a series of different targets would be an **amazing feat of engineering and deception**. Only a **handful** of states could spare the necessary resources to attempt such a cascade of destruction.

Apart from the technical challenge, there remains the **practical question**: Why would an adversary want to achieve such mass destruction effects through hacking? If the aim is to generate mass casualties, there are more direct and reliable ways. A hostile state could use ICBMs tipped with nuclear warheads to kill millions. By exploding a nuclear weapon in the atmosphere, an enemy could generate an electromagnetic pulse powerful enough to shut down electrical and communications networks. Aerial bombs and cruise missiles could destroy critical transportation nodes. Terrorists might even introduce poisons to a city water supply or disease agents in the food chain. The more catastrophic the desired effect of the attack, the less point there is to deliver it through computer networks.

Alarmist observers also do not explain why deterrence would not succeed with cyber weapons as it has with WMD. It is the announced policy of the United States government that it stands prepared to respond with "military force" to a cyber attack that causes loss of life or substantial damage to property.24 The United States need not try to counter each cyber attack with a comparable response in cyber space. A cyber attack could well trigger kinetic retaliation from a wide range of conventional weapons that could cause worse damage to an enemy regime. Whatever one may think about the inherent logic of cyber deterrence, the record of experience suggests that something is at work. Since September 11, 2001 terrorist attacks have killed thousands of Americans, even within the boundaries of the United States. In the same period, there have been **no U.S. fatalities attributable to cyber attacks**.

### 2NC – NATO Ineffective

#### NATO will flounder when forced to act on cyber

Ucko 10 - Adjunct fellow at the Department of War Studies at King's College London (David H., "Resetting Article 5: Toward a New Understanding of NATO's Security Guarantees," World Politics Review, 10-26-2010, https://www.worldpoliticsreview.com/articles/6838/resetting-article-5-toward-a-new-understanding-of-natos-security-guarantees)//nt-sg

The Estonian crisis demonstrated that today's attacks are **unlikely to be** the **unambiguous,** military and territorial attacks imagined during the Cold War, and that NATO, as a military alliance, **remains ill-equipped** to operate in less-traditional domains or against less-readily identifiable actors. Similar conclusions can be drawn from NATO's sole invocation of Article 5, on Sept. 12, 2001. NATO's response then centered on Operation Eagle Assist, the deployment of Airborne Early Warning aircraft (AWACS) to protect U.S. airspace, and Operation Active Endeavor, the deployment of naval forces to the eastern Mediterranean "to help detect, deter and protect against terrorist activity." The alliance also pledged to share intelligence on the terrorist threat, provide overflight rights and access to ports and airfields as part of any retaliatory operations, and to assist any state whose support for these measures would prove destabilizing.

At first sight, NATO's response reflected an agile use of structures and capabilities configured for Cold War-era threats. But the first invocation of Article 5 also illustrated the **limited relevance** of its guarantees against less-conventional foes. Unlike the Soviet Union, al-Qaida was not deterred by the threat of collective NATO action. Nor were NATO's actions following Sept. 11 effective in punishing the transgressor or in forestalling future attacks. Indeed, it took **nearly a month** for NATO to confirm its invocation of Article 5 and launch Active Endeavor and Eagle Assist, as it first had to establish that the perpetrators of the attack were not domestic actors within the United States. And although the AWACS that NATO provided did free up some U.S. assets for the campaign in Afghanistan, Operation Eagle Assist was peripheral to the broader effort against al-Qaida and was terminated after a mere six months. The Mediterranean operation looked good on paper, but its relation to the al-Qaida threat was unclear, and the ships involved also operated under a limited mandate that precluded involuntary boarding of suspicious vessels.

Some European nations did deploy special forces to Afghanistan in 2001, yet even this response was a far cry, in terms of scale and effectiveness, from the type of reaction associated with Article 5. By the time the U.S. made more concrete appeals for European forces to come stabilize "postwar" Afghanistan, the mood of solidarity had already begun to wane. Having had their initial offers of assistance rebuffed by the then-bullish Bush administration, there was not much appetite in Europe to deploy, and the campaign basically had to be sold as another Balkans peacekeeping operation before European troops began arriving. By that point, the link between the Afghan campaign and the invocation of Article 5 had already substantially eroded.

In short, the threat and actual invocation of Article 5 **does not deter** less-traditional adversaries and types of attack, **nor does it provide for a swift or effective response** to these threats. As a military alliance, NATO is ill-equipped and ill-structured to deal with the security risks of terrorism, cyber attacks, political subversion and harassment (over energy or natural resources, for instance). The **ambiguity** of these acts, whether in their origins, effects, and nature, is also likely to **delay NATO decision-making** and undermine the alliance's resolve. As a result, the categorical response implied by the wording of Article 5 will be difficult, if not **impossible**, to put into practice.

#### NATO is illequipped to handle cyber escalation

Lindley-French 19 - is Senior Fellow, Institute of Statecraft, London; Director, Europe Analytica; Distinguished Visiting Research Fellow, National Defense University (Julian, Judy Asks: Is NATO Deterrence a Paper Tiger?” Carnegie Europe, 1-31-19, <https://carnegieeurope.eu/strategiceurope/78254>) //nt-sg

Paper tiger? No, more **cardboard elephant**. Thomas Schelling said that deterrence is the power to hurt as bargaining and best held in reserve. NATO has become a collective deterrent rather than a collective defender. On the eve of a short but violent war NATO would be the last place the Americans would turn to. Rather, as NATO continued to talk deterrence, Washington would put together a high-end coalition under its command to do the fighting.

NATO is too **slow of thought, decision, and foot** to fight a contemporary war. The conduct of war will become far **faster** with new technologies appearing in a **battlespace** that will **stretch across** air, sea, land, cyber, space, information, and knowledge. The **Russians understand this** and have built a thirty-day “wham, bam, thank you Vlad” war machine that would **exploit NATO’s slowness** of force generation and military mobility. NATO assumes at least thirty days of warning. Adaptation is thus buttressing deterrent value by accelerating NATO’s speed of response and extending its power to hurt. NATO could fight a short war if it had the warning, or a long war if it was given the chance. Hmmm . . .

#### Consensus ensures any Article V invocation will trigger infighting and delays

Dunivan 15 – Lieutenant Colonel in the US Army and Assistant Professor at U.S. Army Command and General Staff College (Jim, “Challenges, Capability and Will: Is NATO Relevant in the Twenty-first Century?” School of Advanced Military Studies at United States Army Command and General Staff College, 5-23-15, <https://apps.dtic.mil/sti/pdfs/AD1001278.pdf>) //nt-sg

That being said, consensus in and of itself is one of the **primary challenges** to the continued relevance of the Alliance. Consensus within NATO **constitutes compromise** among the membership for action. While the idea of consensus has always served as a fundamental and valued principle within the Alliance, it is worth noting that compromise, by its very definition of agreement through concessions or adjustment, is rarely an optimum solution. Additionally, in their report to the Secretary General to inform the development of the 2010 NATO Strategic Concept, the Group of Experts put forth that:

there is **an inherent tension** between a multimember organization that works by consensus and a military/political Alliance operating in a fluid and fast-paced security environment...However, the need to achieve agreement...can prove arduous, sometimes **leading to delays** that serve no constructive purpose. In addition, the Alliance needs to prepare for situations where rapid (indeed almost instantaneous) decision-making may be required.

While the Group of Experts was correct to identify this challenge, there has been little to **no** apparent **progress** in streamlining the overall process of collaborative decision making for the Alliance. One member of the European Union Military Staff, another organization that has membership size and consensus issues, commented that it is **hard to create a shared vision** when you have twenty-eight members sitting around the table. This combination of real or perceived less than optimal solutions derived from a **cumbersome and obstacle-laden process** presents challenges to the reliability and credibility of NATO as a relevant force of action.

### 2NC – Grey Zone Escalation

#### Putin will take advantage of NATO disunity to attack

McGee 21 - UK and European Policy and Politics Editor for CNN Digital (Luke, ANALYSIS: How the West made the most dangerous version of Putin,” CNN, 10-24-21, <https://www.cnnphilippines.com/world/2021/10/24/How-the-West-made-the-most-dangerous-version-of-Putin.html>) //nt-sg

"Putin is an **opportunist**. NATO's disunity is the **greatest gift** he can receive," says Riho Terras, former commander of the Estonian Defense Forces. "German reliance on Russian gas is a problem for those of us who share a border as it undermines unity. Brexit might be good for the UK, but it raises questions of a European army which would obviously be weaker than NATO."

Some believe that Putin's greatest asset has been hysteria and overstating of the threat he poses in some part of the West, combined with limited pushback from powerful nations, including the US, for his sincere hostility.

"Every time an opportunity appears, **he will take i**t. It happened in **Ukraine**, it happened in **Georgia**. He only understands strong messages and if we keep showing disunity he will respond in kind. **He is a streetfighter.** The West is trying to figure skate around Russia, but Putin plays ice hockey," says Terras.

#### Putin will exploit any NATO weakness he can

Tribune Editorial Board 22 - (Editorial: Biden and Europe must use the only language Putin understands: Strength,”Chicago Tribune, 1-24-2022, <https://www.chicagotribune.com/opinion/editorials/ct-editorial-biden-putin-ukraine-nato-unified-resolve-20220124-bsxoqss4rzdrncw5qlhkf3bfuq-story.html>) //nt-sg

Though brutish in so many ways, Putin also is a **chess player** who calibrates each move and countermove. With Ukraine, he has embarked on a gambit that aims to **force NATO to retreat** from Eastern Europe, former Soviet lands that ring Russia’s western edge and widely known among Russians as “the near abroad.” He’s pinning his hopes on the possibility that **NATO devolves into a scale of disunity** that allows him to reconstitute a buffer against the West.

That’s precisely why any sign of a breakdown in the West’s resolve toward Kremlin aggression would be **disastrous**. The West’s cohesion is its **primary strength**. Whether its military and financial support for Ukraine’s democratically elected government, the buildup of defenses on Russia’s western flank, or a new regime of harsh sanctions against Russia, the U.S. and Europe cannot allow any divisiveness to germinate.

### 2NC - AT: Article V = Deterrence

#### Ambiguity and diversity of threats obviates attempts at cyber deterrence

Smeets and Soesanto 20 - Dr. Max Smeets is a senior researcher at ETH Center for Security Studies and affiliate at Stanford University CISAC. Stefan Soesanto is a senior researcher in the Cyber Defense Team at the Center for Security Studies (CSS) at ETH Zurich. (Max and Stefan, “**Cyber Deterrence Is Dead**. Long Live Cyber Deterrence!” Council on Foreign Relations, 2-18-2020, <https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence>) //nt-sg

Why has the concept fallen out of fashion? The existing literature has certainly done a great job of providing a comprehensive list of reasons why deterrence in cyberspace is more difficult to achieve than deterrence in conventional domains. Cyberattacks are said to be **cheaper to execute**, while defense is hard. **Retaliation** in cyberspace is supposedly **harder to execute** as the attribution of a cyberattack necessitates **time-intensive**, all-source information, often spanning numerous networks and actors. Signaling is **equally problematic**, given the **secrecy** of cyber operations and the **difficulty** of discerning between offensive and defensive behavior. Furthermore, given the **diversity** of actors in this domain, including individuals, non-state hacking groups, and military operators, the assumption that all actors in cyberspace act rational is **not a given.**

#### Even if Article V deters conventional war – it is ineffective to combat cyber

Ross 21 - an intelligence officer with extensive expertise in signals and cyber intelligence and a graduate of the Junior Officer Cryptologic Career Program (Cameron, “Is It Time to Forget about Cyber Deterrence?” Air & Space Power Journal, Spring 2021, <https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-35_Issue-1/C-Ross.pdf>) //nt-sg

Consequently, ideas about cyber deterrence have naturally accompanied the growth of cyberspace and cyber operations. The disruptive and revolutionary nature of cyber and its potential for massive effect resembled the arrival of nuclear weapons in many ways. However, many theorists and strategists quickly noted the **challenges** to reconciling cyber with ideas of classical deterrence. During the Cold War, deterrence was straightforward. For example, it was easy to know who launched an attack; there was a significant scientific barrier to creating nuclear weapons; every bomb could be as powerful as the first; any use of a nuclear weapon crossed an acknowledged threshold; redlines were usually grounded in geography and easy to conceptualize; and motives were generally discernable and tied to strategic interests.6 Almost **none of these apply** to the world of cyber. Attribution can be **incredibly difficult** and usually takes an inordinate amount of time—if one can discern the origins of the attack at all. The low barrier to entry enables **many actors**, and what would deter each actor is almost as **varied** as the actors themselves. The use of a cyber weapon makes it less likely that it will be effective in the future as defenders patch the vulnerability. Defining substantive thresholds and redlines is **almost impossible**. Yet, despite all the barriers to effective deterrence, most authors believe it is possible and should be pursued. But is deterrence the right framework for approaching cyberspace? Perhaps the friction strategists face is indicative of the need for a **paradigm shift**.

### 2nc – only retal = war

#### Retaliation spirals and ensures conventional warfare

Hunt 16 - Group Head of Information Security at Sanne (Ash, “Tit-for-Tat: Cyber Retaliation,” Info Security Magazine, 8-22-2016, <https://www.infosecurity-magazine.com/opinions/titfortat-cyber-retaliation/>) //nt-sg

Retaliation often **engenders escalation**: something that the cyber domain facilitates with unprecedented ease. As nation states all-too-willingly adopt this tit-for-tat mentality, the prospect of attacks **spilling over** the ether into the conventional domains of war becomes **increasingly likely.**

As Russia’s revanchist activities in Ukraine show, asymmetric warfare has already begun to rear its head; its efficacy and desirability – a potent combination of cyber and tangible force – will make it the norm. Nation states should make a concerted effort to curtail a spiraling cyber arms race and ensure cooler heads prevail. Cyber’s destructive capacity and ability to destabilize international relationships deserves **constant policing and attention**.

There is a Chinese proverb; he who seeks revenge should remember to dig two graves. The international community would do well to remember this. When it comes to tit-for-tat, there are **no winners**, only pyrrhic victories.

#### Retaliation ensures larger cyber crisis

Libicki 13 – management scientist at the RAND Corporation (Martin C., “Tangled Web,” RAND Review: Vol. 37, No. 1, Summer 2013, <https://www.rand.org/pubs/corporate_pubs/CP22-2013-06.html>) //nt-sg

In their zeal to protect themselves in cyberspace, countries need to **ensure** that they do not **trigger even greater threats** beyond cyberspace, particularly military or economic forms of retaliation. At a time when the reported level of cyber incidents continues to rise and when cyber risks are perceived as growing even faster, the odds are increasing that a country will find itself in a cyber crisis. Such a crisis could take many different forms: the escalation of tensions associated with an actual, major cyberattack; the suspicion that such an attack has already occurred and must be countered; or the simple fear that an attack might soon occur and must be preempted. Cyber crises are less likely to emanate from the unavoidable features of cyberspace than from each side’s fear, often **exaggerated**, of what might result from its failure to respond. To avoid the unnecessary escalation of such crises, national cyberdefense agencies should **monitor the messages** and signals they send out about their own cyberoperations, sharpen their analyses of how potential adversaries would likely perceive the escalatory aspect of offensive strategies, and **take additional cautionary measures** to manage perceptions.

#### Following through with Article V commitments guarentees a disproportionate response

Singer and Friedman 2013 – P.W. Singer is a Strategist for the New America Foundation and a Professor of Practice at Arizona State University. Allan Friedman is the Director of Cybersecurity Initiatives at National Telecommunications and Information Administration in the US Department of Commerce (P.W. and Allan, “*Cybersecurity and Cyberwar: What Everyone Needs to Know*,” Oxford University Press, 2013, p. 137) //nt-sg

Conversely, making good on a threat in cyberspace can have **drastic impacts** on international stability. The full impact of an action taken in cyberspace is **difficult to control or predict.** Therefore, the retaliation may **spiral** beyond the intended punishment, inflicting damage over and above what would be considered a proportionate response to the breach of a threshold. This risks a minor incident triggering a tit-for-tat escalation and ‘cascading an attack in cyberspace into a much bigger conflict’. This danger is exacerbated by the risk of inadvertently punishing the incorrect actor. Incorrect attribution could trigger unnecessary escalation with a third party while the real aggressor goes unpunished and undeterred.

Thus, once such a cyber deterrence framework’s constructed, a state faces the strategic dilemma of being forced to choose between maintaining its credibility and the risks of collateral damage.

### 2nc – US retal

#### NATO countries want to use OCOs to response to cyber attacks

Emmott 17 - Diplomatic Correspondent at Reuters Brussels (Robin, “NATO mulls 'offensive defense' with cyber warfare rules,” Reuters, 11-30-17, <https://web.archive.org/web/20210304161932/https://www.reuters.com/article/us-nato-cyber/nato-mulls-offensive-defense-with-cyber-warfare-rules-idUSKBN1DU1G4>) //nt-sg

TARTU, Estonia (Reuters) - A group of NATO allies are considering a **more muscular response** to state-sponsored computer hackers that could involve using cyber attacks to bring down enemy networks, officials said.

The United States, Britain, Germany, Norway, Spain, Denmark and the Netherlands are drawing up cyber warfare principles to guide their militaries on what justifies deploying cyber attack weapons more broadly, aiming for agreement by early 2019.

The doctrine could **shift NATO’s approach** from being defensive **to confronting hackers** that officials say Russia, China and North Korea use to try to undermine Western governments and steal technology.

“There’s a **change in the (NATO) mindset** to accept that computers, just like aircraft and ships, have an offensive capability,” said U.S. Navy Commander Michael Widmann at the NATO Cooperative Cyber Defence Centre of Excellence, a research center affiliated to NATO that is coordinating doctrine writing.

Washington already has cyber weapons, such as computer code to take down websites or shut down IT systems, and in 2011 declared that **it would respond to hostile cyber acts**.

The United States, and possibly Israel, are widely believed to have been behind “Stuxnet”, a computer virus that destroyed nuclear centrifuges in Iran in 2010. Neither has confirmed it.

Some NATO allies believe shutting down an enemy power plant through a cyber attack could be **more effective** than air strikes.

“I need to do a certain mission and I have an air asset, I also have a cyber asset. What fits best for the me to get the effect I want?” Widmann said.

The 29-nation NATO alliance **recognized** **cyber as a domain of warfare**, along with land, air and sea, in 2014, but has not outlined in detail what that entails.

#### The US would have no choice but to retaliate to cyber ops

Healey 22 – Senior Research Scholar at Columbia University's School for International and Public Affairs specializing in cyber conflict (Jason, “Preventing Cyber Escalation in Ukraine and After,” War on the Rocks, 3-9-22, <https://warontherocks.com/2022/03/preventing-cyber-escalation-in-ukraine-and-after/>) //nt-sg

First, Russian offensive cyber operations might **spark a wider war**. President Vladimir Putin has declared sanctions “are akin to a declaration of war” and may see aggressive cyber attacks as the perfect response, particularly since they are reversible and non-lethal. Russia has been entangled with Western economies for decades, especially in the realms of energy and finance. But now, as ties are being severed quickly and viciously, Russia no longer has to fear the backlash if its cyber forces were to disrupt Western banks or liquified natural gas terminals. If you are dealt out of the game, why not just flip the table?

Russia’s cyber generals may be just as enthusiastic as their Army counterparts. They may assure Putin their forces are ready for battle and can quickly and bloodlessly get the West to back down. Putin could be convinced disruptive attacks against the West are no big deal, a low-cost signal that the West should de-escalate or just the next natural move in a non-escalatory intelligence contest. After all, U.S. research found that in response to cyber attacks, “Americans are less likely to support retaliation with force” compared to a more traditional strike.

This can lead to escalation in two ways. The United States — along with countries like the United Kingdom, France, and the Netherlands — might well decide to **defend forward against such attacks**. Gen. Paul Nakasone, the commander of U.S. Cyber Command, has **insisted** his forces “must take this fight to the enemy, just as we do in other aspects of conflict.” His then-deputy has also argued that the United States **“cannot cede any territory”** to adversaries as the “Russians will keep pushing until we push back on them.”

Worse, Dmitri Alperovitch recently warned that if Russia launches cyber attacks after “[h]aving already **exhausted the power of economic sanctions**, America and its European allies would have **few choices** other than to respond to these attacks with offensive cyber-strikes of their own.” Such dynamics can feed a **spiraling escalation in cyberspace** that might take on a life outside of the control of policymakers.

#### The US will respond forcefully to Russian cyber attacks

Greig 22 – ZDNet staff writer (Jonathan, “Biden warns of US 'cyber' response after Ukraine says computers wiped during attack,” ZDNet, 1-19-22, https://www.zdnet.com/article/biden-threatens-cyber-response-after-ukraine-says-computers-wiped-during-attack/)//nt-sg

US President Joe Biden **responded forcefully** to reports of a wide-ranging cyberattack on Ukrainian government systems Wednesday afternoon, telling reporters that the US **would respond** with its own cyberattacks if Russia continues to target Ukraine's digital infrastructure.

"The question is if it's something significantly short of an...invasion or major military forces coming across," Biden said in response to a question about how the US would respond to a Russian invasion of Ukraine.

"For example, it's one thing to determine that if they continue to use cyber efforts, well, we can respond **the same way**, with cyber."

The Daily Beast later asked White House Press Secretary Jen Psaki, and she confirmed that if Russia continued to launch cyberattacks, they would be answered with a "**decisive, reciprocal, and united response**."