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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

#### Retaining flexibility is key for appropriate response

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

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

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

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

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

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

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

#### No large-scale Russian cyberattacks

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

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

#### No nuclear retaliation

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

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

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

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

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

#### No Russian war

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

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

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

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

#### Deterrence and norms solve cyberattacks

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

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

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

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

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

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

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

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

#### Russia war won’t escalate

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

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

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