**NEG --- OCO’s**

**Solvency**

**1NC --- No Integration**

**Allies will resist---a litany of constraints ensure disagreement.**

**Häussler 10** – Assistant Legal Advisor of Operational Law at the Allied Command Transformation (NATO ACT, Norfolk/Va., USA)

Ulf Häussler, “Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty,” International Cyber Security, Legal & Policy Proceedings, Chapter 6, 2010, https://ccdcoe.org/uploads/2010/01/LP\_Proceedings\_2010-2.pdf

Political Policy and Institutional Arrangements

The fact that a given cyber threat or incident crosses the threshold of political concern is without prejudice to its political and legal characterisation for the purpose of developing an appropriate response. Much will depend on political policy perceptions – are cyber threats and incidents predominantly perceived as human rights (i.e. data privacy) issues, matters of law enforcement and/or homeland security300, or matter of national security and defence – and the different roles played by the government agencies involved on the examination and assessment of cyber threats and incidents, and competent to adopt or contribute to actual responses. Accordingly, it may be for multiple reasons that **NATO faces challenges** in **developing consensus** regarding the **full integration** of **cyber** security and **defence** in its **respective mechanisms**, as well as the necessary institutional arrangements.

First, in an environment where any security and defence discourse is to a **great extent predetermined** by the **level of political concern**, there may simply have been a **limited number of opportunities** to actually put cyber security and defence **prominently on NATO's agenda**. Second, quite similar to threats arising from international terrorism, threats arising in and out of the cyber space may give rise to both **internal**, or homeland, and **external security concerns**, and thus trigger the oftentimes **complex delineations** of competence between the defence, law enforcement, and intelligence sectors which many NATO Nations have developed into strong checks and balances amounting to a **separation of powers en miniature** within their executive branches of government. Whilst obviously such **domestic arrangements lack** the **capacity** to **affect** the **interpretation** and **application** of the **North Atlantic Treaty**301, they may nevertheless **de facto challenge** NATO Nations' Defence Ministries' as well as Armed Forces' ability to put cyber security and defence on NATO's policy, concept, and **doctrine agendas**. To date, **no well-entrenched method**, structure or process for **overcoming** this de facto challenge – e.g. through involvement of foreign intelligence, homeland security and/or law enforcement stakeholders – **exists** within NATO. Third, there is a **near complete lack** of **NATO-wide**, **standardised doctrine** for cyber warfare. The resulting absence, amongst NATO Nations, of a **militarily agreed** and **legally cleared** (Article 36 of GP I) understanding concerning the means and methods of cyber warfare may also **contribute** to the **lack of political policy consensus**. The appetite for engaging in hostilities which might be perceived as potentially involving legally doubtful means and methods of warfare may be **limited**. Ultimately, the **absence of consensus** regarding **jus in bello** may thus have **repercussions** on the **likelihood that consensus can be reached** concerning jus ad bellum as well as **collective** security and **defence**.

**2NC --- No Integration**

**NATO consensus is impossible---a number of issues ensure political disagreements are insurmountable.**

**Joubert 12** – Associate Research Fellow at the Centre for Geopolitical Studies of the Raoul Dandurand Chair of Strategic and Diplomatic Studies, UQAM

Vincent Joubert, “Five years after Estonia’s cyber attacks: lessons learned for NATO?,” NATO Defense College Rome, Research Division, Research Paper, No. 76, May 2012, https://www.jstor.org/stable/pdf/resrep10366.pdf

In addition, the potential for NATO to play a **bigger role** in defending the information infrastructure by **implementing** a **credible cyber deterrence strategy** is **limited by political disagreements** on the **conditions** and **circumstances** which would **prompt** any **collective response** to cyber attacks. NATO is currently focusing on implementation of an active cyber defence strategy, with improved security standards and requirements. While improved defence will to a certain extent dissuade potential aggressors, this is of course not enough for it to be considered as a real deterrent in its own right. For actual cyber deterrence (by punishment), there is the prerequisite that Article 5 of the North Atlantic Treaty be considered applicable to cyber attacks. In this respect the NATO Policy on Cyber Defence reiterates that any collective defence response is **subject to political decisions** of the **North Atlantic Council**, and that NATO will **remain flexible** on how it will respond to cyber attacks. This flexibility can be interpreted in two ways: as a deliberate position calculated to keep potential aggressors in a state of uncertainty regarding the consequences they might face, or as a **sign** that the Alliance has **difficulty** in **achieving consensus** on a **firm response option**. In the first case the aggressor might indeed be dissuaded from attacking NATO’s information networks by fear of an unforeseeable retaliation. Unfortunately, however, leaving response options unspecified creates a degree of **ambiguity** which might be perceived as **reflecting political disagreements** among the Allies on when and how NATO should intervene. If this were indeed the case, it might actually give an adversary good reason to favour cyber attacks over other forms of action against the Alliance’s – or the individual Allies’– critical infrastructure. In other words, the rationale for a cyber attack would be that **political** and **conceptual divergences** within NATO might **delay** the **consensus required** to **trigger** a **collective response**. Here, an interesting historical parallel is often drawn with the ambiguity regarding NATO’s nuclear deterrence in Europe during the Cold War: the point made by some analysts is that the experience of nuclear deterrence as practised by NATO and other actors can be usefully applied to the cyber domain, insofar as nuclear deterrence doctrine prevented nuclear conflicts. Unfortunately, nuclear and cyber deterrence differ significantly in both technical and strategic terms. Attackers might thus interpret the perpetuation of ambiguity in NATO’s nuclear and cyber retaliation posture as additional proof not only of political disagreements, but even of strategic misunderstanding.

Such an interpretation must unfortunately be taken seriously. Cyber attacks can take various forms, depending on their objectives and techniques – ranging from espionage, organized crime and disruption to outright destruction. Determining which category a specific type of attack falls into will **largely depend** on **legal** and **political considerations** at the **national level**. **Interpretations** might thus **vary** from one country to another, to the extent that a given action might be considered an act of war by one member state but not by another. This **severely jeopardizes** the **political consensus required** to **initiate collective defence measures**. The **resulting difficulty** in **defining** a **threshold** for **collective response** and an appropriate form of retaliation might in turn lead to a **considerable weakening** of NATO’s **strategic credibility** in cyber defence.

**Adv --- OCO’s**

**1NC --- Squo Solves**

**NATO is ready for hybrid war---they’ve rapidly modernized political and military responses.**

**Oguz 16** – Ph.D, Security Expert at the International Strategic and Security Research Center

Safak, 2016, “The New NATO: Prepared for Russian Hybrid Warfare?” Insight, https://www.jstor.org/stable/pdf/26300458.pdf?refreqid=excelsior%3A54f0cb5a96b9cf9c79b2b9b43d8623b9

**NATO was caught off guard** when the crisis started in Ukraine. **At the beginning**, Russia’s **hybrid warfare** strategy of deception, ambiguity, and denial **complicated** attribution and response, and rendered **the decision-making process** more difficult for NATO. The Alliance did not manage to assess the environment correctly.27 As Major General Gordon Davis, the United States general in charge of operations and intelligence at NATO’s military headquarters in Belgium during the Ukrainian crisis, admitted, it took some time for the Alliance to determine the “size and the scale” of the troop reinforcement, which was continuously denied by the Russians.28

Russian President Putin masterfully played off the regional divisions within NATO during his slow-rolling invasion of Eastern Ukraine.29 The crisis shed some light on the fact that the sense of insecurity is not the same in all NATO countries. Despite significant pressure from the United States and NATO’s worried Eastern European members, countries enjoying good relations with Russia, notably France, Germany and Italy, refrained from challenging Russia, and tried to mitigate the crisis via diplomacy. German Chancellor Angela Merkel stated she was “convinced that there is no military solution to this conflict, adding on the other hand that no one could be sure they would manage to achieve a truce through talks,” such as those between Merkel, Hollande, and Putin.30

And so the Russian methodology outflanked NATO’s reaction policies, with the Alliance and its 28 members remaining bystanders, though there was clear potential for the conflict to spread far beyond Ukraine. The course of the conflict also proved paradoxical: Germany, for instance, delivered military equipment to the Iraqi Kurds in the Middle East but not to desperate Ukraine.31 France’s focus on operations in Mali and the Central African Republic during the Ukrainian crisis also highlighted the superiority of national interests over the collective in the Alliance.

**However, subsequent** Russian **activities bolstered solidarity** among the Alliance **and all members agreed upon** political and military **measures** that broke the tangled relations between NATO and Russia. The **Wales Summit** became a **cornerstone of solidarity and cohesion** for the Alliance, as the allies agreed upon measures to counter the Russian threat. The RAP sought to ensure a rapid and firm response to new security challenges. The RAP includes assurance measures, designed to reassure the Alliance’s worried members (especially in Eastern Europe) of NATO’s solidarity and commitment against Russian aggression. These include **continuous** air, land, and maritime **presence and activities** in Eastern Europe, specifically in the Baltic countries and Poland, on a rotational basis. As a result, the Alliance increased its air-policing activities over the Baltic States, enhanced naval patrols in the Baltic Sea, the Black Sea, and the Mediterranean, commenced AWACS (Airborne Warning and Control System) surveillance flights over eastern Allies, deployed ground troops to the eastern members for training and exercises, and conducted three hundred NATO and national exercises in 2015 alone.

The **RAP** also **has adaptation measures that envisage major structural** and functional **changes in NATO’s military system**. Specifically expected to enhance the Alliance’s capabilities is the reorganized NATO Response Force (NRF), set up after the Prague summit in 2002 and including the new Very High Readiness Joint Task Force (VJTF) of around 5,000 troops, some of are deployable within 48 hours. The size of the enhanced NRF has since tripled to around 30,000 troops, composed of land, air, naval and special operations forces. The **RAP insists on responsiveness** and, above all, on the mutation of the NRF into a new, revitalized model.

During the Warsaw Summit in 2016, the Allies also decided to **establish a forward presence** of multinational troops in the eastern regions of the territory, in order to reassure worried member countries, just as during the Cold War the Alliance’s strategy included demonstrating solidarity, cooperation, and cohesion. As the Warsaw Summit declaration has it, Alliance members “have decided to establish an enhanced forward presence in Estonia, Latvia, Lithuania and Poland **to unambiguously demonstrate**, as part of overall posture, the Allies’ solidarity, **determination**, and ability **to act** by triggering an immediate Allied response to any aggression.

In addition to RAP, the leaders also approved the **New Strategy on Hybrid Warfare** during the Foreign Ministers’ Meeting in December 2015. NATO Secretary General Stoltenberg described the new strategy: to prepare, to deter, and to defend. He stressed the Alliance requires many different kinds of capabilities in order to defend its population, since hybrid threats are themselves so diverse in nature, and he **outlined the key elements**: increased responsiveness and readiness of NATO forces, of intelligence, and of surveillance; improved situational awareness; the use of special operations and of cyber capabilities; and **close cooperation** with the European Union.

The framework of the New Strategy on Hybrid Warfare enhanced the Alliance’s counter-hybrid-threat capabilities. **Improved situational awareness** through enhanced intelligence and reconnaissance, and better **information sharing** between allies as well as other international organizations, constitutes one of the main developments. The Alliance aimed to **quickly identify** low-level attacks or indications of impen**ding hybrid warfare**, in order to **reduce** ambiguity and **surprise**, as well as to **enable more precise**, timely, and correct **decision-making**

**2NC --- Squo Solves**

**They’re coordinating with civilian institutions, accelerating political response times, and boosting overall resilience to hybrid threats.**

**Oguz 16** – Ph.D, Security Expert at the International Strategic and Security Research Center

Safak, 2016, “The New NATO: Prepared for Russian Hybrid Warfare?” Insight, https://www.jstor.org/stable/pdf/26300458.pdf?refreqid=excelsior%3A54f0cb5a96b9cf9c79b2b9b43d8623b9

The **Special Operations Forces** are expected to **provide strategic** and operational **support** for the Alliance’s efforts, most especially in effectively countering irregular warfare elements, as they are more effective in this realm than regular forces. For this reason, the **integration** of special forces into the NRF and VJTF **constitute another key measure** adopted in the New Strategy. The first demonstration of this integration took place during the Noble Jump exercise of June 2015, when NATO deployed VJTF based on scenario that Poland was under threat of irregular warfare. The deployment made clear in terms of potential aggression against Alliance members, Russian irregular warfare is seen as far more likely than conventional warfare.

Arguing that Russia resorted to massive and effective cyber assaults against both Ukraine and NATO countries, the **Alliance enhanced** its **cyber warfare capabilities** as well. A February 2016 technical agreement launched a joint program with the European Union, which initiated the exchange of information and incident data, in order to boost situational awareness of cyber threats.35 The Alliance also began to study the legal background of the relation between cyber assault and common defense. The statement by NATO Secretary General Stoltenberg that “a major cyber attack against the Alliance could trigger a collective response”36 has made clear that cyberspace is likely to be an important operational domain in future.

Additionally, **NATO opted to counter hybrid threats by** pursuing **a comprehensive approach across all** military, diplomatic, economic, information, and social **levers available to the** international **community**. Cooperation and coordination with other partner countries and international organizations, especially with the European Union and Organization for Security and Cooperation in Europe (OSCE), is recognized as key to countering hybrid threats; in particular in this regard, the **critical civilian assets** and civil issue capabilities **of the European Union.**

Both during and after the Cold War, Russia enjoyed an advantage over NATO in speedy decision-making and deployment of forces, as well as in the use of special forces. Ever since the establishment of the NATO Alliance, authority to deploy troops, and the use of these troops, has constituted a critical issue between member nations and NATO officials. During the June Defense Ministerial meeting in 2015, **leaders** decided to **grant authority to SACEUR to prepare** troops **immediately** when the Allies deem it necessary, thereby **accelerating the** military **reaction process**. As a result, when SACEUR sees an unfolding crisis he is authorized to mobilize NATO’s new VJTF and send troops to the nearest flight line, to await final orders for takeoff. Authority from the Alliance’s highest decision-making body—the North Atlantic Council—must be granted before actually deploying the troops.37 In this way, member countries retained final authority for use of the troops.

**The new measures** were adopted to **deter**, **dissuade**, and **challenge Russian hybrid warfare** in addition to a Russian conventional assault against the Alliance—the latter scenario described by Putin himself as only a madman’s fantasy.38 **The Alliance is militarily stronger**, **swifter**, and **more capable of responding to any Russian hybrid threat**, particularly **against a member country**. Nevertheless, political determination will remain a key factor in challenging Russia.

**NATO is effectively deterring Russian hybrid threats---upgraded defenses and enhanced coordination.**

**Rynning 20,** is Professor of War Studies and Vice Dean for Research at the faculty of business and social sciences, the University of Southern Denmark (SDU) in Odense, Denmark. Sten Rynning founded the Center for War Studies at SDU in 2011 and headed it until 2019. (Sten, “Deterrence in the 21st Century—Insights from Theory and Practice,” *NL ARMS Netherlands Annual Review of Military Studies,* 2020, https://library.oapen.org/bitstream/handle/20.500.12657/43303/2021\_Book\_NLARMSNetherlandsAnnualReviewO.pdf)

Deterrence by denial (i.e., an ability to deny Russian objectives by defensive measures) is only possible for NATO at the lower rungs of this ladder, and NATO has not been idle here either. In fact, most of the early measures taken by NATO in response to the annexation of Crimea fall into the deterrence of denial category and centre on rapid reaction capacities, especially in the shape of a NATO Response Force (NRF) upgraded for deterrence purposes. The NRF now has a **reinforced**, quicker spearhead—a Very High Readiness Joint Task Force potentially up to 13,000 troops strong, and then two complementing brigades with support (each 13,000 strong) forming a layered, sizeable reaction force explicitly linked to **collective defence** purposes and regularly exercised in Eastern Europe and the Baltic states.35 In 2016, in response to the foreseeable difficulties of projecting mainly Western forces into zones of conflicts close to Russia, NATO decided to established an “enhanced forward presence”—four multinational battalion-sized battle groups —in the Baltic states and Poland, and a “tailored forward presence”—mainly naval forces—in the Black Sea region. Whether these forces can credibly “deny” Russian objectives in the case of limited war is a bone of contention. Most observers and sometimes NATO itself employ the descriptor “tripwire” to these forces, thus indicating that they are triggers that promise to unleash NATO’s big guns and therefore part and parcel of deterrence by punishment. However, US diplomats (interviewed on background) feel more confident that the US battalion embedded (in Poland) in the collective forward presence posture would actually be able to fight and survive, and thus **deny Russian objectives**. That may be so, in which case the conclusion is that NATO has a moderate-to-low—and geographically focused—capacity for deterrence by denial and then a more general and impressive capacity for deterrence by punishment. NATO’s unquestionable capacity for deterrence by denial is rather found at the **level of grey zone**, non-kinetic conflict. In this regard, NATO has **upgraded** not only its **cyber defences** and enhanced intelligence coordination, as mentioned, but has **enhanced coordination** with the European Union on hybrid threats, with a 2016 joint declaration leading to a common work program and a collaborative Centre of Excellence for Countering Hybrid Threats, located in Helsinki, the 2016 adoption of societal resilience benchmarks that, while mostly falling outside NATO’s political-military remit, nations must meet, and finally the decision in 2018 to organize counter-hybrid support teams that can tailor assistance to individual allies and circumstances.36 NATO’s full range of actions in response to Russia’s 2014 annexation of Crimea —a range to which this brief overview can do only limited justice—thus combines deterrence by denial (grey zone conflict, societal resilience, reaction and forward deployed forces to counter limited land grabs) and deterrence by punishment (the full chain of reaction and deployable forces, from conventional to nuclear). NATO’s strong suit is the military piece of this posture, but it has considerably adapted to grey zone conflict scenarios in an effort to achieve a **comprehensive deterrence** posture vis-à-vis Russia’s unified (kinetic and non-kinetic) and uninterrupted (all domains, in war and peace) doctrine of “new generation warfare”.

**1NC --- Alt causes**

**Alt cause – lack of staff wrecks cyber operations**

**Collier, 20** (Jamie Collier, Writer for war on the rocks, “CYBER RESERVES ARE NOT A SILVER BULLET”, war on the rocks, may 22, 2020, <https://warontherocks.com/2020/05/cyber-reserves-are-not-a-silver-bullet/>)//babcii

The most significant long-term challenge facing American and British cyber agencies is not China or Russia — it’s a shortage of cyber talent. This workforce deficit isn’t only affecting intelligence agencies. One [recent study](https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx) looked at 11 countries’ cyber skill shortages and extrapolated that the global deficit of qualified personnel sits at over four million unfilled positions and argues that the workforce needs to grow by a staggering 145 percent. Government agencies struggling to match the lucrative private sector salaries on offer naturally find themselves on the back foot. Cyber reserves, conscription models, and [the use of volunteers](https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/) are often touted as a panacea for boosting government recruits. Yet, [calls for a cyber reserve](https://www.rand.org/pubs/research_reports/RR1490.html) are not enough. Cyber reserve models are often impractical and fail to materially address nascent policy challenges. While cyber reserves can certainly play a limited role in improving security, states such as Britain and the United States should instead continue to focus on policy initiatives that are better aligned with their political cultures and operational requirements. Working with the private sector provides more scalable reinforcements and enables a coordinated approach to protecting what is often predominantly privately-owned infrastructure. Both approaches can certainly co-exist, yet robust public-private collaboration will often trump the whims of volunteers. Practical Limitations of Cyber Reserves Calls for [expanded cyber reserves](https://warontherocks.com/2019/09/the-presidents-own-as-a-model-for-the-marine-corps-cyber-auxiliary/) underestimate the logistical challenges of implementation. This has led to [many policy proposals](https://www.thetimes.co.uk/article/young-people-should-do-national-cyberservice-jshrhkf9l) failing to address the nature of cyber operations or the lengthy timelines often involved. As much as anything, both offensive operations and securing networks are a collection of practices that require full-time staff and an organized approach. Most large government departments defend their networks 24 hours a day. Security operations centers run around-the-clock monitoring for potential threats. Likewise, vulnerability management programs, used to patch high-severity flaws, require constant vigilance and active coordination in order to stay ahead of the threat. Within these contexts, full-time staff who have experience working together develop continuity and established workflow patterns to ensure threats aren’t missed. Cyber espionage campaigns are no different. It is assumed that operations conducted by prominent state espionage groups, often [referred to as advanced persistent threats](https://collierjam.com/apt-simplistic-as-123/), rely on technical wizardry alone. Yet, rather than their ability to exploit flashy zero-day vulnerabilities or deploy highly bespoke malware, it is often their operational capabilities that make the difference. This was captured by National Security Agency and former cyber security White House advisor Rob Joyce, who [stressed that targeting large corporate networks requires plenty of patience and focus](https://www.youtube.com/watch?v=bDJb8WOJYdA&t=39s). This is largely due to the [variety of stages](https://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1142093) involved in cyber operations. This can include extensive open source research on employees ahead of sending phishing emails, putting in the hours to fully understand a target’s infrastructure, or waiting for the right moment to move laterally within a network. Crucially, successful operations often come down to gritty abrasion. Full-time staff, shift patterns, and established routines are at the foundation of a successful campaign. Supplementary staff waltzing in with the occasional weekend or evening to spare might be able to contribute, yet these operational realities limit their ability to substantially move the needle.

**1NC --- Turn --- OCOs Bad**

**OCO’s cause escalation with Russia over Ukraine**

**Healey, 22** (Jason Healey, Healey is a senior research scholar at Columbia University’s School for International and Public Affairs, 3-9-2022, accessed on 6-19-2022, War on the Rocks, "Preventing Cyber Escalation in Ukraine and After - War on the Rocks", <https://warontherocks.com/2022/03/preventing-cyber-escalation-in-ukraine-and-after/)//Babcii>

Second, Western offensive cyber operations might **spark war.** U.S. cyber espionage and operations against Putin, his cronies, or Russia’s military forces will appear far more ominous to Putin if he believes they are aimed at regime change. Could Putin turn the other cheek if the United States were to electronically raid the cryptocurrency wallets of Russia’s sanctions-avoiding kleptocrats? He might feel the need to escalate his own cyber operations as part of his own version of defending forward. **Escalation could happen on the battlefield as well**. [According to the New York Times](https://www.nytimes.com/2022/03/06/us/politics/us-ukraine-weapons.html), teams from U.S. Cyber Command are “in place to interfere with Russia’s digital attacks and communications.” Other teams are almost certainly collecting digital intelligence on the location and intent of Russian combat forces. The United States is sharing such intelligence with the Ukrainians but [apparently not yet providing any real-time targeting](https://www.nbcnews.com/news/investigations/biden-administration-walks-fine-line-intelligence-sharing-ukraine-rcna18542). That may change soon, as the United States seeks to alleviate intensifying attacks on civilians. And with his KGB-bred paranoia, Putin might already see the presence of U.S. defensive and intelligence teams operating on or against Russian military networks as evidence of direct U.S. involvement in the war. Confirming his apparent belief that Ukraine is just a NATO puppet, this might force a response, either inside or outside of cyberspace. Further, if Western governments have infiltrated Russia’s operational military networks, they may feel pressure to disrupt those networks to prevent civilian massacres. Because cyber capabilities are billed as non-lethal, reversible, and non-escalatory, tub-thumping newspapers may push decision-makers to take shots they might not otherwise: “We can’t create a no-fly zone but [can use cyber capabilities to prevent civilian harm](https://mobile.twitter.com/Jason_Healey/status/1498416936891387912).” Some [well-meaning national leaders](https://twitter.com/JacquiHeinrich/status/1500961829509636099) may succumb to this pressure, **potentially causing a larger conflict.** Future Risks Even if Russia and the West avoid direct conflict this time, they might not be so lucky the next. As relations worsen, future disruption of critical Western infrastructure by Russian intelligence, such as the [NotPetya](https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html) and [Olympic Destroyer](https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html) attacks, are less likely to be viewed as mere crimes. Repeated crises bordering on war may further erode the tacit agreements and relative restraint of quieter times. After repeated iterations of intensifying cyber operations, both Russia and the West may feel their backs to the wall with few options left other than military force when the next crisis — physical or cyber — emerges. Under extreme conditions, some of the same characteristics that lead cyber capabilities to be a pressure release might have the opposite effect, a mechanism that Bob Jervis and I have described as the [Escalation Inversion](https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/). If Putin believes a direct conflict with NATO is likely and expects its adversaries to [take measures to reduce vulnerabilities](https://www.cnas.org/publications/reports/a-new-era-in-u-s-russian-strategic-stability), he could conclude that the best possibility for success is to launch a massive preemptive cyber attack. Since the U.S. military may seem otherwise unbeatable, this [may lead](https://www.brookings.edu/book/surprise-attack/) Russia to “compensate with audacity in order to redress the balance.” The more the United States **brags about its overwhelming offensive cyber advantage**, but frets over weak defenses, the more any adversary might feel the need to [target the United States as early and as hard as possible](https://www.lawfareblog.com/getting-drop-cyberspace).

**OCOs backfire and fail.**

**Slayton ’17** (Rebecca; 2/2017; PhD in chemical biology from Harvard University, Masters in chemistry and chemical biology from Harvard University, Bachelor’s in chemistry from Westmont College, author of Arguments that Count: Physics, Computing, and Missile Defense, winner of the Computer History Museum Prize, author of Shadowing Cybersecurity, winner of a 5-year National Science Foundation CAREER award, project lead on research funded by the Department of Homeland Security Center of Excellence’s Critical Infrastructure Resilience Institute; “Why Cyber Operations Do Not Always Favor the Offense,” <https://www.belfercenter.org/sites/default/files/files/publication/Cyber%20Ops%20Offense%20-%20final.pdf>; Date Accessed: 7/10/2017; DS)

Creating Unnecessary Vulnerabilities Prioritizing offensive operations can **increase adversaries’ fears**, suspicions, and **readiness to take offensive action**. Cyber offenses include cyber exploitation (intelligence gathering) and cyberattack (disrupting, destroying, or subverting an adversary’s computer systems). An adversary can easily mistake defensive cyber exploitation for offensive operations because the distinction is a matter of intent, not technical operation. The difficulty of distinguishing between offensive and defensive tactics makes mistrustful adversaries **more reactive**, and repeatedly conducting offensive cyber operations only **increases distrust**. A focus on offensive operations can also **increase vulnerabilities**; for example, secretly stockpiling information about vulnerabilities in computers for later exploitation, rather than publicizing and helping civil society to mitigate those vulnerabilities, leaves critical infrastructure vulnerable to attack. The skills and organizational capabilities for offense and defense are very similar. Defense requires understanding how to compromise computer systems; one of the best ways to protect computer systems is to engage in penetration testing (i.e., controlled offensive operations on one’s own systems). The similarity between offensive and defensive skills makes it **unnecessary to conduct offensive operations** against adversaries to maintain offensive capability. Thus, rather than stockpiling technologies in the hope of gaining offensive advantage, states should develop the skills and organizational capabilities required to innovate and maintain information and communications technologies. Managing Complexity The complexity of information systems gives the offense certain advantages for purely probabilistic reasons. Imagine a race: offense and defense go hunting for randomly distributed vulnerabilities, with the offense attempting to exploit those vulnerabilities and the defense aiming to patch them. The number of vulnerabilities grows with the **size and complexity** of the computer system, as do the technological advantages of offense—at least in principle. With a vast number of vulnerabilities, it is **unlikely** that the defense will be able to find and patch every vulnerability before the offense finds and exploits it. Technology is, however, embedded in social organizations, and organizations can help the defense better manage complexity. Those that develop software can check for common errors before making hardware-software systems available for use. The defender has complete access to its computer system, whereas the attacker has a more limited set of attack vectors. Organizations can help skilled defenders by establishing good cybersecurity processes, such as continually scanning for vulnerabilities and updating software. Assessing Kinetic Effects To date, failures of cyber defense have largely been failures of management, and the successes of offense are a result of its relatively simpler goals. Offense, like defense, becomes more difficult as its goals become more complex. In particular, the advantages that complexity offers the offense in cyberspace diminish in the physical world. Computers controlling physical machinery can be hacked, but achieving particular physical effects, such as covertly sabotaging nuclear enrichment facilities, requires knowledge of the physical processes that the computers control, not merely knowledge of the computers. Much of the detailed knowledge needed to run an industrial control system is tacit, passed from one engineer to another but never written down, let alone stored on a computer. Gathering such information requires traditional espionage by humans on the ground, which is both expensive and risky. A cost-benefit analysis of Stuxnet for both the offense and the defense demonstrates why damaging physical infrastructure is **more costly** than simply infiltrating information networks. The costs of Stuxnet were likely far greater for the offense (the United States and Israel) than for the defense (Iran), and Stuxnet was relatively ineffective, setting back Iran’s nuclear program by fewer than three months. The great expense of Stuxnet was intelligence; though digital espionage can be used to obtain some kinds of information, the knowledge needed to disrupt a physical control system, such as the detailed methods and settings used to control pressure in Iran’s nuclear centrifuges, is not generally held in computers. The costs for both sides are dominated not by technology but by skilled labor—for example, hackers who identify and exploit zero-day vulnerabilities, systems administrators who manage and defend computer systems, and the nuclear engineers who understand enrichment processes and the means of disrupting them. In addition, assessing costs alone is misguided: the perceived benefits of attacking with and defending from Stuxnet (i.e., the value of Iran’s nuclear weapons program) greatly exceeded the costs for both the offense and the defense. This is one reason not to be complacent about the need to secure industrial control systems and critical infrastructure: though cyberattacks on such systems will be costly, a determined adversary may be **willing to pay the cost** to achieve its aims. Conclusion The common assumption that the offense dominates cyberspace is dangerous and deeply misguided. The offense-defense balance can be assessed only for specific operations, not for all of cyberspace, as it is shaped by the capabilities of adversaries and the complexity of their goals in any conflict. When it comes to exerting precise physical effects, cyberspace **does not offer overwhelming advantages** to the offense. Because the capabilities of offense and defense are similar, improving defensive operations allows preparation for cyber offense without **risking geopolitical instability** or increasing vulnerability to attack.

**An offensive cyber posture fails and causes escalation.**

**Valeriano & Jensen 19** – Senior Fellow at the Cato Institute, Bren Chair of Military Innovation at the Marine Corps University, serves as Senior Advisor for the Cyber Solarium Commission; Associate professor at the Marine Corps University and a scholar‐​in‐​residence at American University’s School of International Service

Brandon Valeriano, Benjamin Jensen, “The Myth of the Cyber Offense: The Case for Restraint,” The CATO Institute, Policy Analysis No. 862, January 2019, https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint

The Myth of the Offense

Contrary to observed patterns of limited disruption and espionage, Cyber Command sees cyberspace as a domain fraught with increasing risk, where great powers such as China and Russia will undermine American power. The only solution, from this perspective, is to go on the offense. Yet, the benefits of an offensive posture, especially in cyberspace, are mostly **illusory** to date. Instead, the cyber domain tends to be optimized for defense and deception, not decisive offensive blows. Not only is offense likely the weaker form of competition in cyberspace, it also **risks inadvertent escalation**. The fear, suspicion, and misperception that characterize interstate rivalries **exacerbate** the **risk** of offensive action in cyberspace.

Cyber Command’s 2018 persistent-action strategy aims to “expose adversaries’ weaknesses, learn their intentions and capabilities, and counter attacks close to their origins.”44 Put in simple terms, the best defense is a good offense: get on adversary networks and stop cyber operations targeting the United States before they occur. Under this strategy, offensive cyber operations will also be **preemptive** in that they are designed to “contest dangerous adversary activity before it impairs [U.S.] national power.”45 To use another sports metaphor, come out swinging. Go on the offense first and establish escalation dominance (that is, demonstrating such superior capabilities over the target state that it can’t afford to escalate in response).46

According to Cyber Command, preemptive strikes will “impose . . . strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks.”47 Whether through punishment, risk, or denial strategies, offensive actions theoretically alter the target’s behavior by increasing the expected costs of targeting U.S. interests.48 Offensive action, according to this thinking, deters future aggression by signaling resolve and establishing escalation dominance. Yet, there are well-established reasons to doubt that offensive options produce the intended results in cyberspace.

Defense and Deception

The rationale behind persistent action—that the best defense is a good offense—is **deeply flawed**. In fact, most military and strategic theory holds that the defense is the **superior posture**.49 For example, Sun Tzu describes controlling an adversary to make their actions more predictable, and hence easy to undermine, by baiting them to attack strong points.50 The stronger form of war is a deception-driven defense: confusing an attacker so that they waste resources attacking strong points that appear weak. This parallels cybersecurity scholars Erik Gartzke and Jon Lindsay’s claim that cyberspace is **not offense dominant**, but **deception dominant**.51 Rather than persistent action and preemptive strikes on adversary networks, the United States needs **persistent deception** and **defensive counterstrikes** optimized to **undermine adversary planning** and **capabilities**.

Fear and the Security Dilemma

New policy options proposed by Cyber Command and the Trump administration **risk exacerbating fear** in other countries and creating a **self-reinforcing spiral** of **tit-for-tat escalations** that ri**sk war** even though each actor feels he is acting defensively—or, as it is called in the scholarly literature, a security dilemma.52 As shown above, most cyber operations to date have not resulted in escalation. The cyber domain has been a world of spies collecting valuable information and engaging in limited disruptions that substitute for, as well as complement, more conventional options. Shifting to a policy of **preemptive offensive cyber warfare** risks **provoking fear** and **overreaction** in other states and possibly **producing conflict spirals**. Even limited-objective cyber offensive action defined as “defending forward” can be misinterpreted and lead to inadvertent escalation.53 As the historian Cathal Nolan puts it, “intrusions into a state’s strategically important networks pose serious risks and are therefore inherently threatening.”54

More worryingly, with a more offensive posture, it will be **increasingly difficult** for states to differentiate between cyber espionage and more damaging degradation operations.55 What the United States calls defending forward, China and Russia will call preemptive strikes. Worse still, this posture will likely lead great powers to assume all network intrusions, including espionage, are preparing the environment for follow-on offensive strikes. According to cybersecurity scholar Ben Buchanan, “in the [aggressor] state’s own view, such moves are clearly defensive, merely ensuring that its military will have the strength and flexibility to meet whatever comes its way. Yet potential adversaries are unlikely to share this perspective.”56 The new strategy risks producing a “**forever cyber war**” prone to **inadvertent escalation** because it implies all cyber operations should be interpreted as escalatory by adversaries.57

The Myth of Decisive Cyber Victory

There is a tendency in the military profession, at least in the United States and Europe, to uphold the concept of decisive battle as central to the Western way of war.58 Often, disruptive technologies—from strategic bombers in the mid-20th century to cyber operations in the 21st century—are seen as providing decisive offensive advantages in crises. In the interwar period between the world wars, airpower enthusiasts argued that bombers would reliably reach their targets, forcing political leaders to end hostilities or face the prospect of destroyed cities and economic collapse.59

Yet the search for decisive battle is often an **elusive**, if not **dangerous**, temptation for military planners and policymakers. In a comparative historical treatment of major 19th- and 20th-century battles, Nolan argues that “often, war results in something clouded, neither triumph nor defeat. It is an arena of **grey outcomes**, partial and ambiguous resolution of disputes and causes that led to the choice of force as an instrument of policy in the first place.”60 Decisive victories in any one battle are rare. Adversaries can refuse to fight.61 They can even signal resolve through demonstrating their ability to endure pain.

**Offensive operations are escalatory and fail.**

**Valeriano & Jensen 19** – Senior Fellow at the Cato Institute, Bren Chair of Military Innovation at the Marine Corps University, serves as Senior Advisor for the Cyber Solarium Commission; Associate professor at the Marine Corps University and a scholar‐​in‐​residence at American University’s School of International Service

Brandon Valeriano, Benjamin Jensen, “The Myth of the Cyber Offense: The Case for Restraint,” The CATO Institute, Policy Analysis No. 862, January 2019, https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint

New policy options proposed by Cyber Command and the Trump administration **risk exacerbating fear** in other countries and creating a **self-reinforcing spiral** of **tit-for-tat escalations** that **risk war** even though each actor feels he is acting defensively—or, as it is called in the scholarly literature, a security dilemma.52 As shown above, most cyber operations to date have not resulted in escalation. The cyber domain has been a world of spies collecting valuable information and engaging in limited disruptions that substitute for, as well as complement, more conventional options. Shifting to a policy of **preemptive offensive cyber warfare** risks **provoking fear** and **overreaction** in other states and possibly **producing conflict spirals**. Even limited-objective cyber offensive action defined as “defending forward” can be misinterpreted and lead to inadvertent escalation.53 As the historian Cathal Nolan puts it, “intrusions into a state’s strategically important networks pose serious risks and are therefore inherently threatening.”54

More worryingly, with a more offensive posture, it will be **increasingly difficult** for states to differentiate between cyber espionage and more damaging degradation operations.55 What the United States calls defending forward, China and Russia will call preemptive strikes. Worse still, this posture will likely lead great powers to assume all network intrusions, including espionage, are preparing the environment for follow-on offensive strikes. According to cybersecurity scholar Ben Buchanan, “in the [aggressor] state’s own view, such moves are clearly defensive, merely ensuring that its military will have the strength and flexibility to meet whatever comes its way. Yet potential adversaries are unlikely to share this perspective.”56 The new strategy risks producing a “**forever cyber war**” prone to **inadvertent escalation** because it implies all cyber operations should be interpreted as escalatory by adversaries.57

The Myth of Decisive Cyber Victory

There is a tendency in the military profession, at least in the United States and Europe, to uphold the concept of decisive battle as central to the Western way of war.58 Often, disruptive technologies—from strategic bombers in the mid-20th century to cyber operations in the 21st century—are seen as providing decisive offensive advantages in crises. In the interwar period between the world wars, airpower enthusiasts argued that bombers would reliably reach their targets, forcing political leaders to end hostilities or face the prospect of destroyed cities and economic collapse.59

Yet the search for decisive battle is often an **elusive**, if not **dangerous**, temptation for military planners and policymakers. In a comparative historical treatment of major 19th- and 20th-century battles, Nolan argues that “often, war results in something clouded, neither triumph nor defeat. It is an arena of **grey outcomes**, partial and ambiguous resolution of disputes and causes that led to the choice of force as an instrument of policy in the first place.”60 Decisive victories in any one battle are rare. Adversaries can refuse to fight.61 They can even signal resolve through demonstrating their ability to endure pain.

Planning and Assessment Pathologies

The new policy framework for offensive cyber operations **risks compounding common pathologies** associated with strategic assessments and planning. 62 **Removing interagency checks** increases the risks that an operation will **backfire** on the attacker or **compromise ongoing operations**.

**Misperception** is **pervasive** in insulated decisionmaking processes for several reasons.63 First, small groups unchecked by bureaucracy tend to **produce narrow plans** prone to escalation during crises.64 Second, leaders often give guidance to planners during crises that reflects their political bias or personality traits rather than a rational assessment of threats and options.65 Third, offensive bias in planning may have little to do with the actual threat and more to do with a **cult of the offensive** and the desire of officers to ensure their autonomy and resources.66 Removing interagency checks therefore risks compounding fundamental attribution errors and other implicit biases. Cyber operations are too important to be left to the generals at Cyber Command alone.

**1NC --- Cyber War Answers**

**Neither side will “escalate to de-escalate” OR climb the ladder.**

**Oliver & Baklitskiy 18** – \*Directs the Russia and Eurasia Program at the Center for Strategic and International Studies. \*\*Arms control and nonproliferation consultant at PIR Center, Moscow. Olga & Andry, 2-20-18, "The Nuclear Posture Review and Russian ‘De-Escalation:’ A Dangerous Solution to a Nonexistent Problem," War on the Rocks, https://warontherocks.com/2018/02/nuclear-posture-review-russian-de-escalation-dangerous-solution-nonexistent-problem/

There is a [growing certainty](https://www.wsj.com/articles/the-case-for-tactical-u-s-nukes-1516836395) in the West that [Russia has adopted](https://cisac.fsi.stanford.edu/news/william-perry-warns-nuclear-dangers-drell-lecture) an “escalate to de-escalate” nuclear strategy, which [lowers the bar](https://warontherocks.com/2016/03/three-minutes-to-midnight-closer-to-nuclear-conflict-than-we-think/) for nuclear weapons use to a terrifyingly low level. Importantly, it’s referenced as fact in the Trump administration’s new [Nuclear Posture Review ,](https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF) which argues that the United States itself therefore needs new low-yield nuclear weapons to deter Russia at lower levels of conflict. But the **evidence of a dropped threshold** for Russian nuclear employment **is weak**. Moreover, even if this was Russia’s doctrine, a shift to more American reliance on lower-yield nuclear weapons would be the wrong solution to the problem. Understanding Russian Doctrine What do people mean when they say “escalate to de-escalate?” The words themselves are not particularly helpful. Any action that is neither a perfectly symmetrical nor smaller response to adversary action is escalation. Any threat (nuclear or otherwise) to raise the costs of conflict is a threat of escalation. And countries both escalate and threaten to do so fairly regularly as they seek to convince adversaries to rethink plans. The fact is that most escalation is intended to, well, de-escalate. Western analysts have developed a range of descriptions of Russian nuclear strategy that all fall, with varying degrees of consistency and contradiction, under the “escalate to de-escalate” umbrella. The [new NPR](https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF) and political scientist [Matthew Kroenig](https://www.wsj.com/articles/the-case-for-tactical-u-s-nukes-1516836395) hold that Russia intends to use nuclear weapons early in a conflict to attain an advantageous battlefield outcome. So does current Pentagon official [Elbridge Colby.](https://www.cnas.org/publications/commentary/countering-russian-nuclear-strategy-in-central-europe) [Juri Luik and Tomas Jermalavicius believe](http://www.tandfonline.com/eprint/umSnuTKFrMZggbaRv3SR/full) Russia would turn to nuclear weapons in the face of imminent battlefield defeat: e.g., to make up for conventional inferiority in a conflict with the NATO alliance. [Evelyn Farkas holds](http://foreignpolicy.com/2017/02/15/trump-needs-a-russia-policy-or-putin-will-force-one-on-him/) that Russia simply likes escalation, nuclear and otherwise. The notion that Russia might use nuclear weapons on the battlefield may originate in arguments in a 1999 paper published in the Russian military journal Voennaia Mysl. The authors, military officers and analysts V. I. Levshin, A. V. Nedelin, and M. E. Sosnovskii, [posited](http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/1999-zvo/8995-o-primenenii-jadernogo-oruzhija-dlja-dejeskalacii) that the use of nuclear weapons in a heretofore conventional conflict could demonstrate credibility and convince the adversary to stand down for fear of further escalation. The argument for more nuclear steps on the escalation ladder has been made more recently as [well](http://nvo.ng.ru/concepts/2015-11-27/1_stairway.html). It was even promised by a senior Russian official prior to the release of a new military doctrine almost a decade [ago](https://www.rbc.ru/politics/14/10/2009/5703d6e19a7947733180bb63). However, neither that [doctrine](http://carnegieendowment.org/files/2010russia_military_doctrine.pdf) nor the one that followed it in [2014](https://rusemb.org.uk/press/2029) (the most recent) in fact lowers the nuclear use threshold. As one of us has argued [previously](https://www.csis.org/analysis/russia%E2%80%99s-nuclear-doctrine), the official statements, followed by a doctrine that did not deliver on them, suggest that **proponents** of a lowered threshold ultimately **lost a bureaucratic fight**. To this day, Russian “escalation” advocates occasionally publish an article, still hoping to change the policy — but continue to fail. Nor does Russian doctrine call for the use of nuclear weapons if Moscow is losing a conventional conflict. To the contrary, military doctrine clearly states that nuclear weapons will be used only in response to an adversary using nuclear or other weapons of mass destruction and/or “when the very existence of the state is [in](https://rusemb.org.uk/press/2029) [jeopardy.](http://www.mid.ru/ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3054726)” One can argue what does and does not qualify as existential jeopardy, but the scenarios in which Western analysts envision Russian nuclear escalation — most of which involve ending a conventional conflict — seem to fall short by most definitions. In the past, Russia’s bar for nuclear use has been both higher and lower. In 1993, [Moscow dropped the no-first-use pledge](http://www.nytimes.com/1993/11/04/world/russia-drops-pledge-of-no-first-use-of-atom-arms.html) it inherited from the Soviet Union. In 2000, however, following the NATO air campaign in Yugoslavia, Russia’s new military doctrine allowed for first use in case of large-scale conventional aggression against Russia or its [allies](https://www.armscontrol.org/act/2000_05/dc3ma00). It is plausible that at this time, plans indeed looked something like “escalate to de-escalate.” But soon after that, proponents of reliance on nuclear weapons found their views eclipsed by Russian government decisions to instead invest in conventional [forces](https://dspace.mit.edu/handle/1721.1/107537). At the time, this was mainly because Russia believed [most of its battles would be smaller-scale](http://milrf.ru/conference/cf_030604/5ru_esin.htm). Today, however, Russia is [increasingly confident](https://sputniknews.com/russia/201701121049508492-precision-weapons-russia/) that its conventional capabilities can play at least some of the strategic deterrence roles historically played by nuclear weapons. A Secret Plan to Escalate? Those who believe in a lowered Russian threshold for nuclear use thus believe that Russia’s formal doctrine is intentionally disingenuous. Indeed, speculation about a secret annex to the doctrine that clandestinely lowers the nuclear threshold [abounds](https://www.usni.org/magazines/proceedings/2017-02/escalate-de-escalate). But as [Kristin ven Bruusgaard has pointed out](https://warontherocks.com/2017/09/the-myth-of-russias-lowered-nuclear-threshold/) in in War on the Rocks, if Russia’s goal is deterrence, **a stated strategy** of restraint **at odds with a real strategy** of escalation **seems counterproductive**. Deterrence works best when the adversary understands which actions will trigger an undesirable response. Three categories of evidence are offered to support the argument that Russia’s true nuclear threshold today is lower than its doctrine indicates: exercises, capability, and rhetoric. Like other nuclear states, Russia runs exercises that involve [nuclear weapons](https://www.foi.se/reportsummary?reportNo=FOI-R--4326--SE). The vast majority of these test strategic readiness, command and control, and interoperability. In a handful of recent cases, various sources [have](https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_01/20160128_SG_AnnualReport_2015_en.pdf) [reported](http://www.businessinsider.com/nato-report-russia-sweden-nuclear-2016-2) [that](https://jamestown.org/program/reflections-on-vostok-2010-selling-an-image/) [nuclear](https://jamestown.org/program/belarus-and-russia-prepare-zapad-2013-military-exercise/) use was simulated in otherwise conventional Russian exercises, supposedly boosting the evidence for “escalate to de-escalate.” It does not, however, appear that scenarios for these exercises fit the model of a small-scale nuclear strike early in a conflict—as one of us has argued in the [past](https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160504_Oliker_RussiasNuclearDoctrine_Web.pdf). If one believes the strikes happened, conditions of a battlefield defeat posing an existential threat to the state are more plausible. However, as Bruno Tertrais explains, the evidence for simulated nuclear use in large conventional exercises is itself not fully [convincing](https://www.iiss.org/en/politics%20and%20strategy/blogsections/2018-4cda/february-e91d/does-russia-really-include-limited-nuclear-strikes-bf12). Importantly, Russia’s most recent large-scale military exercise focused on its Western flank, Zapad 2017, did not have any evident nuclear [strike](https://www.chathamhouse.org/expert/comment/five-things-know-about-zapad-2017-military-exercise) [component](https://news.err.ee/650543/michael-kofman-what-actually-happened-during-zapad-2017), despite positing a conflict with the NATO alliance. Then there’s Russian capability, specifically smaller-scale, shorter-range nuclear capabilities suitable for the battlefield. Russia maintains a substantial legacy [arsenal](https://fas.org/sgp/crs/nuke/RL32572.pdf) of nonstrategic weapons, which some may believe suggests a willingness to use them. Moreover, in recent years, Moscow has emphasized the development of new warfighting systems that can be deployed with either nuclear or conventional firepower, the oft-touted Iskander being one [example](https://www.csis.org/analysis/russia%E2%80%99s-nuclear-doctrine). Russia is also working on hypersonic [systems](https://www.csis.org/analysis/russia%E2%80%99s-nuclear-doctrine). Finally, the “accidental” leak of plans (in the form of a presentation slide) for a nuclear [torpedo](http://www.bbc.com/news/world-europe-34797252) in 2015 fueled speculation that Russia is thinking creatively about nuclear warfighting (although the destructive power of the purported weapon would surely have strategic, not merely “de-escalatory,” effects). Some may argue that capability is evidence enough of possible “escalate to de-escalate” plans, and the West should therefore respond in kind. This is wrong, for two reasons: First, weapons can be used for all sorts of things, and one cannot plan for all possible contingencies — only those that seem plausible. Russia could also, in principle, plan to set off all of its nuclear weapons at once, or fire some of them into space. If a possible strategy is not supported by the evidence, it should not drive planning. Second, the argument that capabilities prove intent works both ways. The United States also has low-yield nuclear capabilities (and will have more if proponents have their way). Should Russia therefore expect the United States to use nuclear weapons first if American conventional forces were losing, say in a fight against Russia over Ukraine? Indeed, such an approach would be consistent with the American doctrine outlined in the new Nuclear Posture Review. But while the review may make this scenario less ludicrous than it was in the past, Russia would still be dangerously paranoid to base its planning on the possibility. **There is no evidence of U.S. plans** to start an offensive war against a major nuclear power like Russia or China, much less **to use a preemptive nuclear strike to “de-escalate” a conventional conflict** once it went wrong. So what is Russia’s very large nonstrategic arsenal for, and why is it emphasizing dual-use systems? First, as regards the nonstrategic arsenal as a whole, Russia is quite simply loath to give up something it has a lot of without getting something else in return. Second, Moscow knows that its nuclear capabilities make Brussels and Washington nervous. Russians did not discuss a nuclear role for the Iskander—and, indeed, rejected the possibility—until the Western press started describing the system as [dual-capable.](https://www.csis.org/analysis/russia%E2%80%99s-nuclear-doctrine) To be blunt, if not reassuring, Moscow has noticed that an emphasis on dual-capable systems keeps the West off-balance, and sees that as a clear benefit. This brings us to the last category of evidence for a clandestine lowered threshold: Russian rhetoric. While some Russian pundits recklessly talk of turning countries to [ash](https://www.reuters.com/article/ukraine-crisis-russia-kiselyov/russia-can-turn-us-to-radioactive-ash-kremlin-backed-journalist-idUSL6N0MD0P920140316), senior officials, including President Vladimir Putin, have been far more careful with their threats. Putin may [mention](https://www.cnn.com/2015/03/16/europe/russia-putin-crimea-nuclear/index.html) that the Crimea crisis could, in some contingencies, have led him to place nuclear weapons on alert. However, this never happened, and it is something of a stretch to interpret that as meaning he would have used a tactical nuclear weapon to end a conventional conflict. Moreover, in the face of recent nuclear [rhetoric](https://twitter.com/realDonaldTrump/status/948355557022420992?ref_src=twsrc%5Etfw&ref_url=https%3A%2F%2Fwww.cnn.com%2F2018%2F01%2F03%2Fpolitics%2Ftrump-nuclear-authority%2Findex.html) from America’s own president, the comments Putin has made seem almost circumspect. Putin’s rhetoric is meant not to signal plans to use nuclear weapons recklessly, but rather to remind any who may have forgotten that Russia is a nuclear weapons state. While this is prospectively destabilizing, it does not indicate a deep occult doctrine, much less a doctrine that has been consistently and publicly rejected. Russian rhetoric reflects the fact that Russia, much like the Soviet Union before it, sees NATO posing a threat that needs to be deterred. Moscow continues to believe, and Russian generals in private conversations emphasize, that any conventional conflict with NATO risks rapid escalation without “de-escalation” — into all-destroying nuclear war. It must therefore be **avoided at all costs**. This logic is consistent with that put forward by American scholars who have [argue](https://www.jstor.org/stable/1962764)d [that](http://www.newsweek.com/how-nuclear-weapons-can-keep-you-safe-78907) nuclear weapons kept the peace during the Cold War. The success of the nuclear peace, in this view, lay in the threat of extreme escalation, not the bespoke step-by-step deterrence the Nuclear Posture Review seems to advocate and that the postulated Russian “de-escalation” doctrine would implicitly endorse.

**2NC --- Cyber War Ansers**

**No false alarms, accidents, or nuclear pressures.**

**Tertrais 17** –Deputy Director at the Paris-based Fondation pour la Recherche Stratégique (Foundation for Strategic Research).

Bruno, 2017, “On The Brink”—Really? Revisiting Nuclear Close Calls Since 1945,” The Washington Quarterly, https://www.frstrategie.org/web/documents/publications/autres/2017/2017-tertrais-twq-on-the-brink.pdf

**The short answer?** If we are to discard Pope John Paul II’s explanation (“Divine Providence”),5 it is that **the system worked** and that, with rare exceptions, those in charge of nuclear weapons have been responsible, prudent, and careful. “**Close calls**” have ranged in fact from “**not-so-close” to “very distant**.”

A number of technical incidents have taken place since 1945, all of which led to one degree or another to nuclear precautionary measures, generally involving the elevation of alert levels. Most of these incidents are well documented, but one of them does not seem to have taken place at all. It was revealed in 2015 that in the midst of the Cuban Missile Crisis, a Mace missile squadron based in Okinawa received a launch order.6 The ambassador of a Latin American country to the United Nations claimed that this incident “could have altered the course of civilization forever.” 7 One should note that according to the account—based on a single testimony—the safeguards worked: given that the procedure was not respected (the order came at DEFCON-2, whereas it was supposed to happen only at DEFCON-1), the unit commander suspended the launch.8 In any case, an in-depth inquiry by Stars & Stripes magazine at the end of 2015 did not find any confirmation of the incident; U.S. Air Force historians did not find any trace of it.

At least a dozen real incidents took place in the United States in the 1960s, 1970s, and 1980s. (Even though there is little or no evidence that as many happened in other countries, one should assume that some also occurred in the Soviet Union or elsewhere.)10 In these cases, alert levels were elevated due to a false alarm, generally caused by the malfunction of a technical system. For instance, in 1960 a U.S. early warning radar in Greenland confused the moonrise with a missile launch.11 In 1961, a dysfunctional transmitter made the Strategic Air Command (SAC) believe that its lines of communication had been cut off.12 In 1962, a cascade of minor incidents and misinterpretation led to bombers being put on alert.13 The same year, a rare conjunction of events led a U.S. radar station to believe that a Soviet missile attack was underway.14 Something similar occurred in 1967, when a solar storm jammed three early warning radars.15 In 1980, two incidents caused by faulty computer chips led U.S. authorities to mistakenly believe that a Soviet attack could be underway.

In the Soviet Union, a well-known 1983 incident of the same sort was recently publicized through a documentary entitled The Man Who Saved The World (2014), according to which “millions of lives were hanging by a thread,” and no less than “the end of our civilization” was at stake.17 A more sobering account of the incident casts serious doubts on whether this was actually the case. When the alarm sounded in the Soviet nuclear command center because of a U.S. missile launch, the officer in charge suspected that it was a mistake and requested visual confirmation. Such confirmation never came, and the command thus stood down.

Some incidents involve direct human errors. This was the case for the infamous magnetic tape mistake of 1979, which went up the chain of command to the U.S. presidency. Woken up by a phone call announcing that 200 missiles were coming in the direction of U.S. territory, National Security Advisor Zbigniew Brzezinski requested a confirmation.19 He was informed a couple of minutes later that ten times that number of missiles had now been detected. The cause was the insertion of a tape used for training and exercises in SAC computers. Nobody knows what President Jimmy Carter would have done had Brzezinski told him that he only had a few minutes to decide, but can one seriously believe that he would have launched a massive counter-strike in the absence of any confirmation that an attack was underway?

In a few of these incidents, a real launch caused confusion. In 1980, for instance, the Soviet Union launched four submarine-launched ballistic missiles (SLBMs) as part of an exercise, and a U.S. early warning radar wrongly judged that one of them was going in the direction of the United States. This evaluation was quickly corrected.

The Norwegian rocket launch of 1995 belongs in the same category and has become another poster child for nuclear dangers. However, the episode should rather be taken as a testimony to Russian cool-headedness. Norwegian and American scientists launched a new type of rocket, the Black Brant XII, in order to study weather data; they had sent word of the launch to Moscow, but the information had not reached the appropriate authorities. Since Black Brant XII was new, large, and with a high-altitude trajectory, its launch was interpreted as a possible missile strike. Some in the general staff raised the hypothesis of a highaltitude electro-magnetic pulse (EMP) detonation. Yeltsin considered an interception, but it soon became clear that Russia was not a target. “After the rocket emerged onto a ballistic curve, the direction of the flight became clear, and we could see that it would in no way touch on Russian territory, but land in the Spitsbergen region—we calmed down and took no serious measures … ”21 Generals Vladimir Dvorkin, a well-known Russian expert, and Eugene Habiger, former head of STRATCOM, denied that the incident had any character of gravity.

The System Worked

Based on the above examples, one must wonder: **is luck a necessary hypothesis** to explain why none of these events led to nuclear war? Is it not at least equally possible that since 1945, people in charge of nuclear weapons “have taken greater care [of them] than is taken in any other situation involving human agents and complex mechanical systems”?

Nuclear-armed countries have **set up mechanisms** designed **to ensure** that nuclear **weapons will not be used by mistake**. This includes fail-safe procedures (where non-use remains the default condition up until the last possible moment) as well as dual phenomenology (the need to confirm the attack by two independent means relying on different physical principles). When The Man Who Saved The World was shown in New York City, the Russian mission to the United Nations issued a communiqué that stated: “Under no circumstances a decision to use nuclear weapons could be made or even considered in the Soviet Union (Russia) or in the United States on the basis of data from a single source or a system. For this to happen, a confirmation is necessary from **several systems**: ground-based radars, early-warning satellites, intelligence reports, etc.” 24 In all the incidents mentioned above, **safety mechanisms worked**, even in the early 1960s **when they were still rudimentary**.

Furthermore, is it credible to imagine that the head of a State or government would order a nuclear strike without being certain that a major military attack was underway? U.S. nuclear expert Jeffrey G. Lewis rightly argues that he cannot imagine that an American president would embark in nuclear reprisals if there was the slightest doubt on the reality of the attack.25 Retired Russian General Vladimir Dvorkin thinks similarly, claiming that “**No president**, no matter what president it is, **will ever make a decision** about launch-on warning b**ased on information about one rocket** or missile or even … two or three missiles.”

From the point of view of logic and complex systems analysis, it remains possible that a combination of incidents can lead to the failure of all safety mechanisms designed to prevent accidental nuclear war. Such a thesis is embodied by the classic work of Scott D. Sagan, The Limits of Safety. It would thus only be “a matter of time” due to cumulative probabilities.27 In a recent documentary about nuclear risks, author Eric Schlosser reiterates the point: “it’s also due to luck, pure luck, and the problem with luck is that eventually it runs out … Every machine ever invented eventually goes wrong.”

But the probability of failure increases markedly with time only if conditions do not change—and conditions do change. Safety mechanisms have been perfected (without necessarily becoming more complex) and lessons of past incidents are being learned. Sagan claimed in 1993 that the Yom Kippur war (see below), as well as the 1979 and 1980 incidents (see above), are proof that organizations fail to learn from experience. But if that was the case, why would the number of known incidents have significantly declined since 1983? We only know of one significant incident in nearly 35 years: the Black Brant XII episode. Charles **Perrow**, the father of “normal accidents” theory (those resulting from the complexity and interconnection of systems), wrote: “with regard to firing [nuclear weapons] after a false warning we reach a surprising conclusion, one I was not prepared for: because of the safety systems involved in a launchon-warning scenario, it is **virtually impossible** for wellintended actions **to bring about an accidental attack.**

**Nuclear Crises**

A second type of crisis involves episodes during which there was an alleged risk of deliberate nuclear use. One has to differentiate between types of crises: to say that the use of nuclear weapons was “discussed” for instance, is different from “considered” or from “planned.” A closer look at them suggests that in most cases, there was an elevation of alert levels and/or various forms of nuclear signaling, and in some cases contingency planning, but **no evidence of intention** of, or temptation **to**, actually **employ nuclear weapons in almost all cases**. As is the case for false alarms, many of the known cases involve U.S. nuclear forces. But there is no evidence in the public domain that the Soviet Union ever considered the use of nuclear weapons outside the East–West confrontation, for instance.

False Nuclear Events

One should start with the nuclear crises that were not. Many episodes sometimes labeled as such did not have any nuclear dimension. There was no “nuclear ultimatum” during the Azerbaijan crisis of 1946, for instance, despite what President Truman himself claimed.30 Nor was there any significant nuclear dimension to the Falklands war of 1982, despite reports to the contrary.

On some of the most-often mentioned episodes, there are important question marks. The famous Kissinger “DEFCON 3” initiative of October 1973, aimed at deterring Moscow from intervening in the Middle East during the Yom Kippur war, involved all U.S. forces, not merely nuclear ones. There was never any explicit nuclear signal or threat during the crisis, and it is far from certain that nuclear weapons per se played any role then.

Likewise for the Kashmir crisis of 1990, a moment of high tension between Pakistan and India. Despite initial reports to the contrary, which were thinly sourced, it seems that there was never any significant nuclear dimension in it— if at all. A roundtable organized in 1994 involving participants in the crisis concluded that the two countries were never on the nuclear brink during that spring.33 Another in-depth study of the crisis one year later led to the same conclusion.34 There may have been confusion between regular, unrelated Pakistani nuclear activities and deliberate crisis-time decisions.35 The former head of Pakistani weapons designs has stated that his country did not have a weaponized device at the time.3

One crisis deserves a separate treatment. By the fall of 1983, a particularly tense moment of the Cold War, NATO was conducting the final phase (Able Archer) of its annual Autumn Forge exercise, which was more elaborate than in previous years.37 Moscow increased the alert of a significant number of forces including nuclear units. NATO simulated nuclear strikes on the 9th and 11th of November. How dangerous was the crisis? A 2008 British documentary claimed that the world had come very close to catastrophe,38 but more information is available today. “We knew that NATO were [sic] doing an exercise,” said General Ivan Yesin, then head of Soviet strategic forces.39 His opinion is reflected by those of other former Soviet and Warsaw Pact officials.40 Note that by November 11, even as the NATO exercise reached its climax, the Soviet alert had been withdrawn and normal flights had resumed. Most indepth analyses of the 1983 crisis all concur that Moscow did not really fear an attack and that the alert was just a precautionary one.41 One should also note that the Pershing 2 missiles, which were in Moscow’s view a possible instrument for a surprise attack, had not yet been deployed to Germany: the first ones arrived on November 23.

Nuclear Signaling

Instances of deliberate nuclear signaling through verbal threats or ad hoc deployments were frequent during the Cold War, and most of them have been well documented: the Berlin blockade of 1948–1949, the Suez crisis of 1956, the status of Berlin crisis of 1958, the U.S. intervention in Lebanon that same year, the October 1962 retaliatory threat by President Kennedy, the Sino–Soviet Ussuri skirmishes of 1969, the India–Pakistan war of 1971, and the Vietnam War all belong to that category. But there is no evidence in the public domain that such episodes included either nuclear contingency planning or serious consideration of nuclear use.

What about India–Pakistan crises post-1998 (the year both countries tested nuclear devices)? In 1999, there were threats on both sides, and some evidence of an increase in alert levels of Indian missiles.42 There is no clear evidence of the same steps being taken on the Pakistani side: during the crisis, the head of Pakistani nuclear forces was in Switzerland.43 This is also true for the 2001– 2002 “Twin Peaks” crisis, during which there is no evidence, despite some heated rhetoric, that either of the two sides was ready to embark in nuclear brinkmanship. A former Pakistani nuclear official reports that Islamabad did not change the alert level of its forces during the crisis.

The Ukrainian crisis that began in 2014 has seen many small nuclear signals, including an increase in flights of Russian nuclear-capable bombers around the European continent. But the only known instance of a clear nuclear-related threat by Russian authorities referred to a hypothetical past situation. In 2015, answering a question about raising alert levels at the height of the Crimean crisis a few months before, Vladimir Putin said, “We were ready to do it,” but seemed to refer to a situation where Western forces would have tried to repel Russia in Crimea, since he added, “Historically, this territory is ours. Russians live there. They were in danger.” 45 Hardly a case of nuclear coercion.

Contingency Planning

Then we have crises where contingency planning was indeed made—an indication that nuclear use was possible. However, there is no evidence that any political leader had his or her “finger on the button” in any of these episodes. In some cases, the use of nuclear weapons was suggested by subordinates and not pursued further. Twice in 1950, General MacArthur suggested such use in Korea, but his requests were rejected.46 In 1967, some in the Israeli government seem to have considered a nuclear demonstration in the Sinai if Egypt threatened the country’s urban centers.47 In 1968, U.S. commanders in Vietnam recommended the use of theater nuclear weapons to defend Khe Sanh, but senior military authorities disagreed.48 In 1973, it seems that part of Israel’s nuclear arsenal was put on alert49—but even at the darkest hour, as is now known through the testimony of a direct witness, Prime Minister Golda Meir categorically refused the nuclear demonstration suggested by General Moshe Dayan.50 Finally, in 1980, a Pentagon study reportedly considered the same option in case of a Soviet invasion of Iran;51 but the contingency never came up.

The more interesting cases are those where the approach was “top-down,” i.e. where nuclear contingency planning was ordered by the highest political authorities. In 1954, Washington considered striking the Vietminh’s positions around Dien Bien Phu to support the beleaguered French forces.52 President Eisenhower was reluctant: he wanted to do it only in the case of an international intervention; he also doubted the added value of nuclear (as opposed to conventional) weapons. In any case, “Eisenhower never came close to approving any action to save Dien Bien Phu,” as former National Security Advisor McGeorge Bundy describes.

During the 1961 Berlin crisis, nuclear options were discussed in depth—a discussion that contributed to the emergence of the flexible response doctrine—but only in case of a war over Berlin, which never materialized.

In 1969, Henry Kissinger ordered the Pentagon to elaborate bombing plan Duck Hook, designed to force Hanoi to negotiate. It is possible (though still not certain to this day) that it included small-scale nuclear options. The plan was shortlived.55 Despite his bravado, President Nixon was aware of the political costs of using nuclear weapons in Southeast Asia.56 In fact, Kissinger said later that during his time in government, “there was no situation in which we were involved, in which we ever made a plan for using nuclear weapons [apart from the Single Integrated Operational Plan (SIOP, the massive war plan to respond to a Soviet attack)].” 57 The famous journalist Seymour Hersh himself, a staunch critic of the administration, admits that he never found any evidence of an imminent use of nuclear weapons at that time.

Finally, one should mention the 1990 request by Defense Secretary Dick Cheney to evaluate the results of a use of theater nuclear weapons on Iraqi forces. Mr. Cheney would later say that he was acting out of “curiosity” and for the sake of “comprehensiveness.” The study was immediately destroyed.5

Serious Consideration of Nuclear Use

We are left then with three cases where the use of nuclear weapons seems to have been very seriously considered: the Korean War, the two Formosa Strait crises in the 1950s, and of course the Cuban Missile Crisis.

Korea and Formosa

As soon as the Korean War began, President Truman ordered the preparation of attack plans in case the Soviet Union was to enter the fray.60 He sent B29 nuclear bombers twice in the region, in 1950 and 1951—the second time with several assembled weapons. However, in June 1951, a Joint Staff study threw cold water on these plans by concluding an absence of “good” targets for nuclear use.

The use of nuclear weapons was also seriously discussed several times at the beginning of the Eisenhower administration, between February and May 1953.62 One contingency plan involved the large-scale tactical and strategic (on Chinese territory) use of nuclear weapons.63 On May 20, the U.S. president secretly approved this option in the form of a memorandum entitled “NSC Action 794” to be executed if circumstances warranted a resumption of offensive action—which never came, since the Armistice was signed in July.64 As described by Columbia University professor Richard Betts, “NSC Action 794 was not a commitment, but it was as close to a final decision as a president can come, short of the moment of execution.” 65 Nobody knows what Eisenhower would have decided had fighting erupted again.

In any event, several reasons prevented the use of nuclear weapons during the Korean War.66 As documented, inter alia, by Nina Tannenwald and T.V. Paul, both presidents appeared seriously concerned with the international reputation of the United States.67 And in almost all scenarios, the use of nuclear weapons did not offer any prospect to make a serious difference on the ground.

During the Formosa Strait (also known as the Taiwan Strait) crises of 1954– 1955 as well as 1958, nuclear use was seriously considered in case of an invasion of Taiwan.69 But that was to come only as a last resort, for fear of allied reactions or Soviet escalation. Eisenhower was prepared but not “anxious” to use nuclear weapons.70 Despite his public positions on the subject, a U.S. Air Force report made clear that “the President simply did not accept the contention that nuclear weapons were as conventional as high explosives.”

The Cuban Missile Crisis seems to remain the only moment since 1945 when the world came really close to nuclear use. This refers less to the retaliatory threat that President Kennedy publicly made in case a missile was launched against the Americas,72 instead referring more to three specific episodes about which the details only became public in the 1990s.

First, on October 24, 1962, the U.S. Navy attempted to force a B29 Soviet submarine to surface. The U.S. crew was unable to reach the general staff.73 An “exhausted” and “furious” Soviet captain Vassili Savitsky considered putting the ship’s 15-kiloton nuclear torpedo in operational condition. He told his crew: “We’re going to blast them now! We will die, but we will sink them all—we will not disgrace our Navy.” 74 The traditional account holds that only the fortuitous presence in the submarine of the fleet commander, Vassili Arkhipov, prevented the shot, since he voted against it. But this version is questionable. According to the Soviet Navy rules, the circumstances for allowing the torpedo strike were not met: written rules of engagement stated that it was possible only on Moscow’s orders.75 Also, it is by no means certain that any real vote took place. The commander “consulted” Arkhipov and deputy political officer Ivan Maslennikov—and they were both opposed. Viktor Mikhailov, an officer on board, testified that “**Savitski never lost it**.”

In the second episode, on October 27 at the height of the crisis, U.S. radars in Alaska detected two Soviet MiG-19s attempting to intercept a U.S. U2 reconnaissance plane, which was flying towards the Kola Peninsula due to a navigation error. Two U.S. F-102s took off to accompany the plane, armed with Falcon nuclear air to-air missiles. However, Khrushchev declared in his memoirs that the Soviet Union would not have intercepted the plane under such circumstances (even less with nuclear missiles) before ascertaining that it was not a navigation error.

In the third episode, Soviet forces in Cuba were endowed with theater nuclear weapons, and rules of engagement initially allowed them to be used in case of an invasion if no contact with Moscow was possible. However, Khrushchev took the initiative on October 26 to alter those rules as to ensure that a Kremlin order would be a prerequisite.

The Tradition of Non-Use Is Strong

The Cuban crisis reveals that Soviet and U.S. officials were able to refrain from foolish judgments even in conditions of extreme stress. Adversaries have never put at stake the “vital interests” of their opponents—either because they were unable to, or because they never intended to, or simply because they feared retaliation. The barriers to the use of nuclear weapons were solid, and the “tradition of non-use” emerged very quickly.

One last element of the anti-nuclear narrative deserves discussion. There is no certainty at all that any use of a nuclear weapon would turn into a major nuclear war. Yes, Cuba was a time of great danger. But why would the use of a nuclear torpedo, for instance, necessarily have led to a global thermonuclear exchange? **Is it** not at least **equally likely** that **the two countries would** have done their best to **limit escalation**? It is possible, as Herman Kahn famously argued, that “**the nuclear threshold is not so weak** that **a single use** of nuclear weapons **would make anyone careless** about crossing it a second time.”

Escalation in the nuclear age would not necessarily be a descent into the abyss. It might very well be the equivalent of walking up a staircase where the last stairs are considerably higher than the first ones. Resistance to actual use or launch could increase as one moves up the escalation ladder—not unlike two magnets repelling each other.

**The narrative** claiming that **the world has stood** many times “**on the brink of apocalypse**,” or that we were within a “hair’s breadth” of a nuclear catastrophe, thus deserves deconstruction. It **discards** the strength of the **technical, operational, or mental safety valves** that prevent nuclear use. Stanislas Petrov, the “man who saved the world,” was not a superhero who single-handedly stopped a runaway train: he was an average Soviet official who applied procedures.

Some legitimate questions remain. What would happen if a false alarm erupted during wartime? If a full-blown conflict involving nuclear-armed countries erupted—something that has never happened, probably thanks to deterrence—can we assume that caution would still prevail? This is an important question and a legitimate preoccupation. The absence of any such conflict since 1945 suggests that nuclear deterrence is a robust construct—but no human construct is infallible. Whether it is for safety mechanisms or for deterrence, even “virtually impossible” does not mean zero. Some would argue that any probability of a nuclear war is too much. But surely this does not close the discussion: a very small probability of a deadly car accident has to be balanced against the benefits of driving to work, for instance. Is the nuclear system “tolerably safe”? 80 The conversation between proponents of deterrence and anti-nuclear activists should revolve around the costs and benefits equation. It is also far from certain that such safety mechanisms and human resistance will always be present in the decision-making complexes of all nuclear-armed states (think North Korea or Pakistan, for instance).

Nevertheless, a history of **nearly 40 crises** with some nuclear dimension has **taught** an important lesion: **solid command-and-control** arrangements, **sound procedures**, **constant vigilance**, **efficient training**, and **cool-headedness of leadership** have ensured—and can **continue to ensure**—that nuclear weapons will continue to play only a deterrence role. “**Luck” has very little to do with it**.

**1NC --- Grid Collapse Answers**

**Grid shut down is physically impossible for 3 reasons and their impact is media fable-telling**

**Pollet 14** - JONATHAN POLLET, founder of Red Tiger Security, and a 17 year veteran of the US ciritcal infrastructure Nov. 23, 2014 "Here's What Chinese Hackers Can Actually Do To The US Power Grid Read more: http://www.businessinsider.com/what-hackers-can-do-to-our-power-grid-2014-11#ixzz3hTq8klee" www.businessinsider.com/what-hackers-can-do-to-our-power-grid-2014-11

There’s been a lot of discussion lately about the risks posed by hackers to America’s critical infrastructure systems, with terms like “cyber-Pearl Harbor” and “cyber-9/11” being bandied about by government officials and other prominent figures.¶ Invariably, one of the worst scenarios often depicted by these cyberwar predictions is an attack on the US power grid that would cause a widespread blackout.¶ In his testimony before the House Intelligence Committee on November 20th, NSA Director Adm. Michael Rogers went into some detail on those risks:¶ House Intelligence Committee Chairman Mike Rogers: “It was determined that malware was on those (critical infrastructure) systems. Can you be a little more definitive about what does that mean? If I’m on that system and I want to do some harm, what does that do … ? Do the lights go out? Do we stop pumping water? What does that really mean? And the fact that it was there, **does that mean they already have the capability to ‘flip the switch’ if they wanted to?”¶** Admiral Michael Rogers: “Well let me address the last part first. There shouldn’t be any doubt in our minds that there are nation-states and groups out there that have the capability to do that. To enter our systems, to enter those industrial control systems, and to shut down, forestall our ability to operate, our basic infrastructure. Whether it’s generating power across this nation, whether it’s moving water and fuel … Once you’re into the system and you’re able to do that, it enables you to do things like, if I want to tell power turbines to go offline and stop generating power, you can do that. If I wanted to segment the transmission system so that you couldn’t distribute the power that was coming out of the power stations, this would enable you to do that. It enables you to shut down very segmented, very tailored parts of our infrastructure.”¶ A number of media outlets interpreted these comments as a claim by the NSA that a country like China could take down our nation’s power grid. But is that what the NSA director really said? And is a widespread, national blackout caused by hackers a realistic scenario?¶ While it’s easy to draw that conclusion from the generalized nature of Adm. Rogers’ responses, it’s important to re-read the last line in that exchange: “It enables you to shut down very segmented, very tailored parts of our infrastructure.” (Emphasis added.)¶ This line is important because it clarifies the types of risks we’re actually talking about when it comes to the electric grid. **No**, hackers can’t take down the entire, or even a widespread portion of the US electric grid. From a logistical standpoint, this would be **far too difficult** to realistically pull off - and it’s not what we should be devoting our attention to. What is more realistic is for a cyber attack to ~~cripple~~ [devastate] an individual utility, causing a blackout or disruption of service at the local level.¶ The power grid is vulnerable to attack — there’s no question about that. In my own work, testing the security readiness of US and global energy companies and utilities, I regularly find serious vulnerabilities on these networks and I am often called in to deal with compromises that have already taken place — including cyber-espionage activities by state-sponsored groups.¶ Adm. Rogers testimony is extremely important as it provides a strong authoritative voice to what is an urgent problem facing this country right now: America’s critical infrastructure is vulnerable to attack, it’s a complicated problem to fix it and an attack is eminent. But the notion that a hacker could basically turn off the country’s power with the ‘flip of a switch,’ as Rep. Rogers called it, is more science fiction than reality.¶ Here’s why:¶ The US energy grid is owned and operated by hundreds of various regional utilities that all use different hardware and software. That means hackers would have to tunnel into hundreds of diverse networks, which would take several years, and then write custom exploits which are unique for each specific environment they’re targeting. For those who would argue that China or Russia have the money, time and capability to do that, try to understand that developing a functional exploit, getting it placed on the exact part of the network that it needs to be on in order to have the desired effect (i.e., specific programmable logic controllers that run the utility’s machinery), then keeping it hidden on that network over a period of months or years while security teams try to hunt it down, and doing all of this at the same time on hundreds of networks is extremely difficult. To put it in perspective, **it would be like trying to rob a hundred different banks at the exact same time.**¶ However, even if a hacker group was able to pull this off, there is a catch-all that would create yet another hurdle. **There are high-voltage DC interconnects at various points that were specifically designed to prevent widespread outages.¶** By clarifying what we mean when we warn about attacks on the electric grid and other critical infrastructure, I’m not trying to downplay this risk at all. US critical infrastructure networks, which include the electric grid, utilities, oil/gas refineries and pipelines, water treatment plants, transportation networks, etc., are all highly vulnerable to cyber attacks, and this threat should be prioritized at the highest level by the federal government.¶ In the meantime, the individual asset owners who are the ones technically responsible for securing their networks and facilities need to start taking more aggressive steps immediately to guard against highly sophisticated cyber actors. But the real risk when it comes to the electric grid specifically is of localized disruptions in service — not a widespread outage. It would be extremely difficult for hackers, without an almost superhuman effort, to cause a power outage that stretched across the country.

**2NC --- Grid Collapse Answers**

**Total shut-down would be next to impossible and the impact is overblown – literally squirrels statistically pose more of a threat**

**Chow 14** - Eugene K. Chow, journalist for the Week January 28, 2014 "Forget hackers: Squirrels are a bigger threat to America's power grid" theweek.com/articles/452311/forget-hackers-squirrels-are-bigger-threat-americas-power-grid

While American lawmakers and security officials repeatedly warn of a catastrophic cyberattack that will ~~cripple~~ [devastate] the nation's power grids, in reality, squirrels and tree branches are proving more troublesome than hackers when it comes to actual power outages.¶ According to numerous reports and headlines: America's power grid is "too vulnerable to cyberattack;" thousands will die if terrorists attack the grid; cyber attacks could keep America in the dark for nine to 18 months; and electric companies face "daily" cyber attacks, which over a month can build to 10,000.¶ With cyber security so abysmal, incentive so high, and attacks constant, why hasn't there been a massive hacker-triggered power failure yet? Simply put, because **it's not that easy.**¶ To be clear, attacks on the power grid would be disastrous and there are significant gaps that must be addressed — procedures improved, vulnerabilities patched, software updated — but even with these glaring weaknesses, an ordinary hacker wouldn't be able to take down the electrical grid. Turning America's lights off remotely is a complex operation that requires not only hacking expertise but an array of intelligence and analysis — something only the most sophisticated terrorist organizations or nation states can muster.¶ Take one of the grid's greatest cyber vulnerabilities, SCADA (supervisory control and data acquisition) software. It allows utility companies to remotely monitor and control facilities, which has the unfortunate consequence of also giving hackers the ability to sabotage the grid from afar.¶ While terrifying in theory, cyber security expert Bruce Schneier explains that SCADA vulnerabilities are "overblown" and the reports are "hype." Actually hacking into SCADA software and causing physical damage to a system is exceptionally difficult. In fact, the only known SCADA attack to cause damage was the Stuxnet virus, which was created after years of intensive research and espionage by Israel and America's most advanced spies and engineers to damage a secret Iranian nuclear facility.¶ Veteran intelligence officer Michael Tanji points out in Wired just how complex such an attack would be. For starters SCADA systems are "rarely connected directly to the public internet," which makes "gaining access to grid-controlling networks a challenge for all but the most dedicated, motivated and skilled — nation-states, in other words."¶ If hackers were somehow able to enter the system, to actually cause physical damage Tanji explains, they would still need to have **advanced intelligence gathering** abilities to learn which SCADA software utilities are running, how they are connected, what the generator blueprints look like, which weaknesses exist in equipment, how to exploit those weaknesses, which machines are linked, how to override safety mechanisms and keep engineers or automatic safeguards from stepping in, and much more.¶ In other words, "a purely online approach is simply not going to provide you with the type and volume of information you are going to need to accomplish your mission," Tanji said. "You're going to have to deploy national-level resources."¶ Meanwhile, as lawmakers worry over these highly sophisticated hypothetical attacks, the nation's aging power grid is falling apart all by itself.¶ In its annual report on US infrastructure, the American Society of Civil Engineers gave the electric grid, some of which dates back to the 1880s, a "D-plus" as the number of power failures continues to rise.¶ According to a study by the Institute of Electrical and Electronics Engineers, between 1965 and 1988, there were three major power failures. From 2000 to 2005, there were 11 and from 2006 to 2009, there were 33. **The primary cause** of these failures **was weather.**¶ More troubling is the fact that the second largest blackout in history, the 2003 Northeast blackout that left more than 50 million without power for two days, **was caused by power lines brushing against tree branches in Ohio.**¶ Even **squirrels** are proving to be, well, a squirrelly problem. No one really knows how much damage the rodents do, but **it's certainly more than hackers manage**. A cursory analysis in The New York Times found that over a four month span last year, squirrels caused at least **50** power outages across the country — and those were just the ones that made the news. And while no one knows how many people are affected by squirrel-related outages each year, in just two days last June, four squirrel-related incidents left more than 18,000 homes in four different states in the dark. How do squirrels manage such mayhem? They simply chew through wires or scamper over fragile electrical equipment.¶ If squirrels weren't troublesome enough, on the more malicious end, there has been a sharp increase in the number of physical attacks on America's energy infrastructure and authorities are struggling to find who's responsible.¶ Last year, Arkansas suffered three separate attacks on the electrical grid that left thousands without power including a substation being lit on fire, the chopping down of two key utility poles with a stolen tractor, and an attempt to use a train to pull down a 100-foot transmission tower.¶ Meanwhile in California, an individual entered a substation and cut several cables, knocking out 911 calls, landlines, and cell service in the area before firing a high-powered rifle at transformers, which ultimately shut down the transformer bank.¶ Military-grade hackers could certainly trigger a blackout for the ages, but with saboteurs waltzing into power stations and causing mayhem with impunity, tree branches leaving millions in the dark, and squirrels wrecking havoc, there are more clear and present dangers to worry about.

**It is impossible for hackers to perform a large scale attack on the US power grid.**

**Perera 14** [David Perera, cybersecurity reporter for POLITICO Pro, “U.S. grid safe from large-scale attack, experts say,” September 10, 2014, http://www.politico.com/story/2014/09/power-grid-safety-110815.html#ixzz3fEZeVZrQ]//JIH

The specter of a large-scale, destructive attack on the U.S. power grid is at the center of much strategic thinking about cybersecurity. For years, Americans have been warned by a bevy of would-be Cassandras in Congress, the administration and the press that hackers are poised to shut it down. But in fact, the half-dozen security experts interviewed for this article agreed it’s virtually impossible for an online-only attack to cause a widespread or prolonged outage of the North American power grid. Even laying the groundwork for such a cyber operation could qualify as an act of war against the U.S. — a line that few nation-state-backed hacker crews would wish to cross. None denied that determined hackers could penetrate the networks of bulk power providers. But there’s a huge gap between that and causing a civilization-ending sustained outage of the grid. Electrical-grid hacking scenarios mostly overlook the engineering expertise necessary to intentionally cause harm to the grid, say experts knowledgeable about the power generators and high voltage transmission entities that constitute the backbone of the grid — what’s called the bulk power system. There’s also the enormity of the grid and diversity of its equipment to consider. “The grid is designed to lose utilities all the time,” said Patrick Miller, founder and director of the Energy Sector Security Consortium. “I’m not trying to trivialize the situation, but you’re not really able to cause this nationwide cascading failure for any extended duration of time,” he added. “**It’s just not possible**.”

**1NC --- Meltdowns Answers**

**Extremely small risk even if there’s an extended blackout**

**Bradley** **16** (Arthur, PhD in Electrical Engineering, former NASA engineer, “Would A Long-Duration Blackout Cause Nuclear Armageddon?” February 3, http://www.thesurvivalistblog.net/would-a-long-duration-blackout-cause-nuclear-armageddon/)

The risks of nuclear power are many, but two stand above the rest. The first is that the fuel assemblies in the reactor might overheat. That would only occur if the fission process became uncontrolled or if the cooling system failed. Should overheating occur, the fuel rods’ zirconium cladding and nuclear materials could both melt, resulting in a nuclear sludge akin to molten lava. That slag would be so hot that it might melt through the bottom of the reinforced reactor. Eventually, it would cool enough to harden, but not before it had spewed nuclear contaminants into the air. Melting zirconium also releases hydrogen, which could lead to an explosion that might actually expel the nuclear material into the surrounding area—think Fukushima. The good news is that nuclear fission can be stopped in **under one second** through the insertion of control rods. Those control rods are **automatically inserted** near the fuel rods either by a hydraulic system or through the use of an electromagnetic deadman switch that activates when power is removed. That means that when the electrical grid goes down or an emergency shutdown is initiated, **fission would automatically stop one second later**. That’s a good thing, but it doesn’t make the reactor inherently safe. Even without fission, the fuel rod assemblies remain incredibly hot, perhaps a thousand degrees C. If they were not actively cooled, pressure and temperatures would build in the reactor until something breaks—not good. After three days of active cooling, however, the reactor would be thermally **cool enough to open**, should it be deemed necessary to remove the fuel rod assemblies. The second major risk has to do with cooling of the spent fuel rod assemblies. Nuclear fuel rod assemblies have a usable life on the order of 54-72 months (depending on reactor type). Every 18-24 months, the reactor is brought down and serviced. While it is down, the fuel rod assemblies are removed, and 1/3 of them are replaced with fresh assemblies. Think of this like rotating cans of food in your emergency pantry. In the U.S., fuel rods are not refurbished like in other countries. Instead, they are carefully stored in giant pools of water laced with boric acid—imagine a swimming pool at your local YMCA that is 75-feet deep. Those spent fuel rod assemblies are still incredibly radioactive, and they continue to generate heat. Water in the pool must therefore be circulated to keep them cool. How long must the fuel rods be cooled? According to Mr. Hopson, the answer is 5-7 years. After that, the rods are cool enough to be removed and stored in reinforced concrete casks. Even then, the rods continue to be radioactive, but their heat output can be passively managed. Nuclear plants obviously require electricity to operate their cooling pumps, not to mention their control systems. That power is normally tapped off of the electricity that the reactor generates. If the plant is offline, the power is provided by the electrical grid. But what happens when the grid itself goes down? The short answer is that large on-site diesel generators **automatically activate** to provide electricity. And if those should fail, portable diesel generators, which are **also on-site**, can be connected. Recent **standardization** has also ensured that generators can be swapped between plants without the need to retrofit connectors. There are also a couple of additional emergency systems that can be used specifically to cool the reactor. These include the turbine-driven-auxiliary-feedwater pump, which uses steam generated by the reactor to power a cooling turbine. The pump requires an operator, but it runs **completely without electricity**. This system, however, is meant only for emergency cooling of the reactor during those critical first few days when the fuel rod assemblies are being brought down in temperature, not for long-term cooling. And finally, **in the worst case**, most plants have a method of bringing in river or ocean water to **flood the reactor**. This typically damages the cooling system, but again, it helps to cool and cover the reactor core should all else fail. Unlike in other countries, permission from the federal government is not required to flood the reactor. With **backup systems to the backup systems**, it would seem that there’s nothing to worry about, right? Under all but the direst of circumstances, I think that assessment is correct. However, one could imagine a scenario in which the grid was lost and the diesel generators ran out of fuel. Speaking of fuel, how much is actually stored onsite? It depends on the plant, but at the Watts Bar Nuclear Plant, for example, there is enough fuel to run the emergency diesel generators for **at least 42 days.** I say at least because it would depend on exactly what was being powered. Once the reactor was cooled down, a much smaller system, known as the Residual Heat Removal System, would be all that was required to keep the fuel assemblies cool, both in the reactor and the spent fuel rods pool. The generators and onsite fuel supply could power that smaller cooling system for **significantly longer** than if they were powering the larger reactor cooling system. **Even if we assumed a worst case** of forty-two days, it’s hard to imagine a scenario in which that would not be enough time to bring in additional fuel either by land, water, or air. Nonetheless, let’s push the question a little further. What would happen in the unlikely event that the diesel fuel was exhausted? Even with the reactor having been successfully cooled, the biggest risk would continue to be overheating of the fuel rod assemblies, both in the reactor and the spent fuel rods pool. Without circulation, the heat from the fuel rod assemblies could boil the surrounding water, resulting in steam. In turn, the water levels would drop, ultimately exposing the fuel rods to air. Once exposed to air, their temperatures would rise but not to the levels that would melt the zirconium cladding. Thankfully, that means that meltdown **would not occur**. The steam might well carry radioactive contaminants into the air, but there would be no release of hydrogen and, thus, **no subsequent explosions**. The situation would certainly be dangerous to surrounding communities, but it **wouldn’t be the nuclear Armageddon that many people worry about.**

**2NC --- Meltdowns Answers**

**No meltdown impact**

**Adams, 12** (Rod, Former Submarine Engineering Officer also Founder of Adams Atomic Engines Inc., "Has Apocalyptic Portrayal of Climate Change Risk Backfired?", 5-2-12, <http://atomicinsights.com/2012/05/has-apocalyptic-portrayal-of-climate-change-risk-backfired.html?utm_source=feedburner%26utm_medium=feed%26utm_campaign=Feed%3A+AtomicInsights+%28Atomic+Insights%29-http://atomicinsights.com/2012/05/has-apocalyptic-portrayal-of-climate-change-risk-backfired.html?utm_source=feedburner%26utm_medium=feed%26utm_campaign=Feed%3A+AtomicInsights+%28Atomic+Insights%29>, accessed 10-9-12)

Not only was the discussion enlightening about the reasons why different people end up with different opinions about climate change responses when presented with essentially the same body of information, but it also got me thinking about a possible way to fight back against the Gundersens, Caldicotts, Riccios, Grossmans and Wassermans of the world. That group of five tend to use apocalyptic rhetoric to describe what will happen to the world if we do not immediately start turning our collective backs on all of the benefits that abundant atomic energy can provide. They spin tall tales of deformed children, massive numbers of cancers as a result of minor radioactive material releases, swaths of land made “uninhabitable” for thousands of years, countries “cut in half”, and clouds of “hot particles” raining death and destruction ten thousand miles from the release point. Every one of those clowns have been repeating similar stories for at least two solid decades, and continue to repeat their stories even after supposedly catastrophic failures at Fukushima have not resulted in a single radiation related injury or death. According to eminent scientists – like Dr. Robert Gale – Fukushima is unlikely to EVER result in any measurable increase in radiation related illness. One important element that we have to consider to assess cancer risks associated with an accident like Fukushima is our baseline risk for developing cancer. All of us, unfortunately, have a substantial risk of developing cancer in our lifetime. For example, a 50-year-old male has a 42% risk of developing cancer during his remaining life; it’s almost the same for a 10-year-old. This risk only decreases when we get much older and only because we are dying of other causes. It’s true that excess radiation exposure can increase our cancer risk above baseline levels; it’s clear from studies of the survivors of the 1945 atomic bombings of Hiroshima and Nagasaki, of people exposed to radiation in medical and occupational settings, and of people exposed to radon decay products in mines and home basements. When it comes to exposures like that of Fukushima, the question is: What is the relative magnitude of the increased risk from Fukushima compared to our baseline cancer risk? Despite our fears, it is quite small. If the nuclear industry – as small and unfocused as it is – really wanted to take action to isolate the apocalyptic antinuclear activists, it could take a page from the effective campaign of the fossil fuel lobby. It could start an integrated campaign to help the rest of us to remember that, despite the dire predictions, the sky never fell, the predicted unnatural deaths never occurred, the deformations were figments of imagination, and the land is not really irreversibly uninhabitable for generations. The industry would effectively share the story of Ukraine’s recent decision to begin repopulating the vast majority of the “dead zone” that was forcibly evacuated after the Chernobyl accident. It would put some context into the discussion about radiation health effects; even if leaders shy away from directly challenging the Linear No Threshold (LNT) dose assumption, they can still show that even that pessimistic model says that a tiny dose leads to a tiny risk. Aside: My personal opinion is that the LNT is scientifically unsupportable and should be replaced with a much better model. We deserve far less onerous regulations; there is evidence that existing regulations actually cause harm. I hear a rumor that there is a group of mostly retired, but solidly credentialed professionals who are organizing a special session at the annual ANS meeting to talk about effective ways to influence policy changes. End Aside. Most of us recognize that there is no such thing as a zero risk; repeated assertions of “there is no safe level” should be addressed by accepting “close enough” to zero so that even the most fearful person can stop worrying. The sky has not fallen, even though we have experienced complete core meltdowns and secondary explosions that did some visible damage. Nuclear plants are not perfect, there will be accidents and there will be radioactive material releases. History is telling me that the risks are acceptable, especially in the context of the real world where there is always some potential for harm. The benefits of accepting a little nuclear risk are immense and must not be marginalized by the people who market fear and trembling.

**1NC --- Terror Answers**

**They’re nowhere near an *existential threat***

Daniel **Benjamin 14**, Nonresident Senior Fellow @ the Brookings Institute, current Director of the John Sloan Dickey Center for International Understanding @ Dartmouth, “Hawks Exaggerate Islamic State Threat to the United States,” 8/17, Brookings, http://www.brookings.edu/research/opinions/2014/08/17-hawks-exaggerate-islamic-state-threat-benjamin

To judge by the **doom-laden prophecies** cascading in from Washington, the United States faces a towering and imminent threat in the form of the militant group calling itself the Islamic State, or ISIS. “They are coming here,” Republican Senator Lindsey Graham of South Carolina intoned on Fox News Sunday. “I think of an American city in flames because of the terrorists’ ability to operate in Syria and Iraq.” Senator Graham’s friend Sena tor John McCain is no less alarmist. Calling for immediate air strikes in Iraq and Syria, he declared, “They are getting stronger all the time . . . And their goal . . . is destruction of the United States of America.”Stoking the panic has been a very excitable press. On CNN last week, I was asked if Islamic State fighters represented an “existential threat” to the United States. Set aside that absurdity; **no terrorist group threatens our existence**. (America has faced one existential threat in modern times — the Soviet nuclear arsenal — and that is it.) But is the **I**slamic **S**tate a huge and menacing terrorist threat? **Certainly not to the United States today.** The danger to Iraq and its neighbors is real. The Islamic State has shown itself to be a formidable insurgency. Its focus is on ripping apart Iraq and Syria, sowing sectarian conflict, and creating in its midst a new jihadist state or caliphate. (That very word seems to incite fearmongers: “Every day that goes by, ISIS builds up its caliphate, and it becomes a direct threat to the United States,” said New York Representative Peter King, conjuring an image of a new Golden Horde with nuclear-tipped scimitars.) If the insurgency grows, and the threat to Jordan or Lebanon increases, we may have to act. But, for now, it’s important to understand that even if marauding operatives in Land Cruisers may be humiliating Iraq’s hollowed-out military, **that doesn’t mean they have genuine terrorist skills.** Consider the details: The Islamic State has never carried out a significant attack outside of its neighborhood. In 2005, when its operatives were still part of Al Qaeda in Iraq, operatives carried out hotel bombings in Jordan and tried and failed to attack an American warship in the Red Sea. More recently, four people were killed in an apparent lone-wolf attack at the Jewish museum in Brussels by a young man trained in Syria. In other words, we’ve seen no demonstrated ability to carry out the kind of complex international strike that kills dozens or hundreds, let alone engulfs a US city in flames.

**2NC --- Terror Answers**

**No US nuclear retaliation**

**Neely 13**—Meggaen Neely, The George Washington University Master of Arts (M.A.), Security Policy Studies 2012—2014 (expected) Baylor University Master of Arts (M.A.), Public Policy and Administration 2010—2012, Richard D. Huff Distinguished Masters Student in Political Science (2012) Baylor University Bachelor of Arts (B.A.), Political Science and Government, Research Assistant, Elliott School at George Washington University, Research Intern, Project on Nuclear Issues (PONI) at Center for Strategic and International Studies (CSIS) Communications Intern at Federation of American Scientists Graduate Assistant at Department of Political Science, Baylor University [March 21, 2013, “Doubting Deterrence of Nuclear Terrorism,” http://csis.org/blog/doubting-deterrence-nuclear-terrorism]

Because of the difficulty of deterring transnational actors, many deterrence advocates shift the focus to deterring state sponsors of nuclear terrorism. The argument applies whether or not the state intended to assist nuclear terrorists. If terrorists obtain a nuclear weapon or fissile materials from a state, the theory goes, then the United States will track the weapon’s country of origin using nuclear forensics, and retaliate against that country. If this is U.S. policy, advocates predict that states will be deterred from assisting terrorists with their nuclear ambitions. Yet, let’s think about the series of events that would play out if a terrorist organization detonated a weapon in the United States. Let’s assume forensics confirmed the weapon’s origin, and let’s assume, for argument’s sake, that country was Pakistan. Would the United States then retaliate with a nuclear strike? If a nuclear attack occurs within the next four years (a reasonable length of time for such predictions concerning current international and domestic politics), **it seems unlikely. Why?** First, there’s the problem of time. Though nuclear forensics is useful, it takes time to analyze the data and determine the country of origin. Any justified response upon a state sponsor would not be swift. Second, **even if** the United States proved the country of origin, it would then be difficult to determine that Pakistan willingly and intentionally sponsored nuclear terrorism. If Pakistan did, then nuclear retaliation might be justified. However, if Pakistan did not, nuclear retaliation over unsecured nuclear materials would be a disproportionate response and potentially further detrimental. Should the United States launch a nuclear strike at Pakistan, Islamabad could see this as an initial hostility by the United States, and respond adversely. An obvious choice, given current tensions in South Asia, is for Pakistan to retaliate against a U.S. nuclear launch on its territory by initiating conflict with India, which could turn nuclear and increase the exchanges of nuclear weapons. Hence, it seems more likely that, after the international outrage at a terrorist group’s nuclear detonation, the United States would attempt to stop the bleeding **without a nuclear strike**. Instead, some choices might include deploying forces to track down those that supported the suicide terrorists that detonated the weapon, pressuring Pakistan to exert its sovereignty over fringe regions such as the Federally Administered Tribal Areas, and increasing the number of drone strikes in Waziristan. Given the initial attack, such measures might understandably seem more of a concession than the retaliation called for by deterrence models, even more so by the American public. This is not an argument against those technologies associated with nuclear forensics. The United States and International Atomic Energy Agency (IAEA) should continue their development and distribution. Instead, I question the presumed American response that is promulgated by deterrence advocates. By looking at possibilities for a U.S. response to nuclear terrorism, a situation in which we assume that deterrence has failed, we **cast doubt on the likelihood of a U.S. retaliatory nuclear strike** and hence cast doubt on the credibility of a U.S. retaliatory nuclear strike as a deterrent. Would the United States launch a nuclear weapon now unless it was sure of another state’s intentional sponsorship of nuclear terrorism? **Any reasonable doubt** of sponsorship might stay the United States’ nuclear hand. Given the opaqueness of countries’ intentions, reasonable doubt over sponsorship **is inevitable** to some degree. Other countries are probably **aware of U.S. hesitance** in response to terrorists’ use of nuclear weapons. If this thought experiment is true, then the communication required for credible retaliatory strikes under deterrence of nuclear terrorism is missing.

**No nuke terror** – people like Allison are hacks

**Mueller** and Stewart **10/29**/18 [John Mueller is Woody Hayes Senior Research Scientist, Mershon Center for International Security Studies, and adjunct professor of Political Science, at Ohio State University. He is also a Senior Fellow at the Cato Institute in Washington. Mark G. Stewart is Professor of Civil Engineering and Director of the Centre for Infrastructure Performance and Reliability at The University of Newcastle in Australia. Terrorism and Bathtubs: Comparing and Assessing the Risks. October 29, 2018. https://www.tandfonline.com/doi/abs/10.1080/09546553.2018.1530662?journalCode=ftpv20]

However, there is of course no guarantee that things will remain that way, and the 9/11 attacks inspired the **remarkable extrapolation** that, because the **terrorists were successful with box cutters**, they might soon be able to **turn out** **w**eapons of **m**ass **d**estruction— particularly **nuclear ones**—and then detonate them in an American city. For example, in his influential 2004 book, Nuclear Terrorism, Harvard’s Graham **Allison** relayed his “considered judgment” that “on the current path, a nuclear terrorist attack on America in the decade ahead is more likely than not.”11 Allison has had a great deal of company in his alarming pronouncements. In 2007, the distinguished physicist Richard Garwin put the likelihood of a nuclear explosion on an American or European city by terrorist or other means at 20 percent per year, which would work out to 91 percent over the eleven-year period to 2018.12 **Allison’s time is up**, and so is Garwin’s. These **off-repeated warnings** have **proven** to be **empty**. And it is important to point out that **not only** have terrorists **failed to go nuclear**, but as William Langewiesche, who has assessed the process in detail, put it in 2007, “The best information is that **no one has gotten anywhere near this**. I mean, if you look carefully and practically at this process, you see that it is an **enormous undertaking** **full of risks for** the would-be **terrorists**.”13 That process requires **trusting corrupted** foreign **collaborators** and **other criminals**, **obtaining** and **transporting** **highly guarded material**, setting up a **machine shop** staffed with **top scientists and technicians**, and rolling the **heavy**, **cumbersome**, and **untested** finished **product** into position to be **detonated** by a **skilled crew**, all the while **attracting no attention** from outsiders. Nor have terrorist groups been able to steal existing nuclear weapons—characteristically burdened with **multiple safety devices** and often **stored in pieces** at **separate secure locales**—from existing arsenals as was once much feared. And they certainly **have not been able** to **cajole leaders** in nuclear states to palm one off to them—though a war inflicting more death than Hiroshima and Nagasaki combined was launched against Iraq in 2003 in major part under the spell of fantasies about such a handover.14 More generally, the actual terrorist “adversaries” in the West scarcely deserve accolades for either dedication or prowess. It is true, of course, that sometimes even incompetents can get lucky, but such instances, however tragic, are rare. For the most part, terrorists in the United States are a **confused**, **inadequate**, **incompetent**, **blundering**, and **gullible bunch**, only **occasionally able to get their act together**. Most seem to be far **better** at frenetic and often **self-deluded scheming** than at actual **execution**. A summary assessment by RAND’s Brian Jenkins is apt: “their numbers remain small, their determination limp, and their competence poor.”15 And much the same holds for Europe and the rest of the developed world.16 Also working against terrorist success in the West is the fact that almost all are amateurs: they have never before tried to do something like this. Unlike criminals they have not been able to develop street smarts. Except perhaps for the use of vehicles to deliver mayhem (though this idea is by no means new in the history of terrorism), there has been remarkably **little innovation** in **terrorist weaponry** or methodology since 9/11.17 Like their predecessors, they have continued to rely on **bombs** (many of which **fail to detonate** or do much damage) and bullets.18

**1NC --- Iran Answers**

**No US-Iran war – mutual disincentives and empirics – rhetoric doesn’t matter.**

**Tabatabai ‘17** (Adnan Tabatabai is co-founder and CEO of the Center for Applied Research in Partnership with the Orient, “Why Iran-US war of words won't turn physical”, Al-Monitor, February 9, 2017, <http://www.al-monitor.com/pulse/originals/2017/02/iran-us-war-words-trump-escalating-rhetoric.html>, accessed 6/29/2017,)

As much as the United States' new tone toward Iran is worrisome, and as much as the Islamic Republic's Jan. 29 ballistic missile test is disconcerting, **Tehran and Washington are unlikely to collide** directly. In both capitals, decision-makers see an urgent need for harsh rhetoric — albeit for different reasons. The Iranians see a need to show resilience vis-a-vis an explicitly hostile US administration. Meanwhile, the latter wants to make clear to both its domestic and international audience that the Obama era is over. This involves signaling that the easing of tensions with Iran has ended. It also involves reassuring regional allies such as Saudi Arabia and Israel that Washington would not engage in a rapprochement with Tehran at their expense. Indeed, it should not come as a surprise that US national security adviser Michael Flynn's warning that Iran "is officially on notice" came shortly after lengthy phone calls between the White House and both Israeli Prime Minister Benjamin Netanyahu and Saudi Arabia's King Salman bin Abdul-Aziz Al Saud. **But escalating rhetoric aside, the reality is that US policy toward Iran has largely remained intact.** In the 13 months since the implementation of the Joint Comprehensive Plan of Action (JCPOA), Iran has repeatedly conducted ballistic missile tests. And it is entitled to do so. In UN Security Council Resolution (UNSCR) 2231, which endorses the nuclear deal, Iran is "called upon" not to carry out tests of missiles "designed" to carry nuclear weapons. There is no legally binding prohibition of such launches, unlike in UNSCR 1929 — the last and most harsh UN resolution against Iran over its nuclear program — which is superseded by UNSCR 2231. To be clear, the nuclear deal does not address Iran's missile program. Moreover, the world powers with which Iran negotiated UNSCR 2231 — apart from the United States — did not display any appetite to insert legally binding text on Iran's missile tests. Thus, as provocative as the missile tests may be, it is hard to see them providing a legal basis for the United States to spearhead new multilateral sanctions, leaving Washington with the option of adopting unilateral sanctions, which it did on Feb. 3. While it took the Trump administration less than two weeks to slap sanctions on Iran, the idea that there was a sanctions freeze in Obama's final year in office is inaccurate. In fact, the latest sanctions were prepared by the previous administration. In January 2016, not long after the implementation of the nuclear deal, changes were made to the Visa Waiver Program, which excluded Iranian dual nationals and anyone who had visited Iran in the preceding five years. Moreover, last December, Obama refrained from moving to veto the congressional vote on a 10-year extension of the Iran Sanctions Act. While these sanctions are unrelated to Iran's nuclear program, they undoubtedly undermine the impact of the lifting of nuclear-related sanctions. Iran has reacted to the escalating rhetoric and sanctions by stressing that its missile program is defensive in nature, promising retaliatory sanctions, and by carrying out new military drills. **Yet, there is little incentive for Iran to greatly alter the status quo**. Iranian leaders see the JCPOA as much more than just about the United States. It is an international arrangement with world powers — including the European Union, which Iran holds in high regard as a multinational institution. They see this arrangement as beneficial to Iran's economic and security calculations. Foreign investment, albeit limited due to remaining US sanctions, is trickling in. The EU oil embargo has been lifted and major contracts in the area of petrochemicals, civic aviation and transport are increasingly sealed. Additionally, the JCPOA provides a sense of security to Iran. It is highly unlikely for any party to the agreement to green-light military action by another party against Iran. Hence, Iran has little incentive not to abide by the nuclear deal. **As such, while the cycle of escalating rhetoric is discomforting at a time of deep uncertainty and conflict in the Middle East, it is important to see that it has its limits. Short of outright regime change, the United States has in fact rather limited options to weaken and contain Iran.** Given its experiences in places like Iraq and Afghanistan, it is unlikely that the United States will launch full-scale unilateral military action against Iran. It could move to arm a third country to hit Iranian infrastructure. This was tried with Iraq under Saddam Hussein. Today, Saudi Arabia could be such a third country. But given the lack of appetite in Riyadh for direct confrontation with Tehran, and considering the downward spiral in the Saudi military intervention against Yemen — the poorest country in the region — it is unthinkable that Saudi Arabia would take such a step. Israel has repeatedly threatened to attack Iranian nuclear sites. But considering the low chances of success and the potentially dire consequences, including retaliatory attacks by Lebanon's Hezbollah movement, it can be argued that such threats primarily serve a political purpose. Less costly measures aimed at weakening and containing Iran, such as sanctions, have been tried and tested. The Obama administration managed to put in place an unprecedented multilateral sanctions regime targeting Tehran. Yet, it was under those very sanctions that Iran’s nuclear program evolved into what the international community came to perceive as a major threat to global security. Consequently, the Obama administration tried diplomacy. And it worked. The JCPOA reduced the capacity and increased the transparency of Iran's nuclear program in exchange for the lifting of nuclear-related sanctions. And as the International Atomic Energy Agency has repeatedly certified, the deal is working. Bearing in mind the nuclear deal is fulfilling its objectives, the limited military options to contain Iran, and perhaps most of all the likely US inability to forge an international consensus against Iran in case of its unilateral breach of the accord, the security establishments of both Israel and Saudi Arabia have publicly urged Washington not to dismantle the JCPOA. While reveling in the newfound reassurances from Washington, it can thus be argued that Riyadh and Tel Aviv understand the limits of the cycle of escalation and mostly take solace in Trump's unwillingness to realize their nightmares under Obama. In this vein, the Trump administration can be expected to do whatever it can to minimize the economic benefits Iran will reap under the JCPOA. It will likely seek to discredit Iran's regional policies to prevent the normalization of the Islamic Republic's ties with the world, while also diminishing the political capital the deal affords Iran. But it will do this short of breaching the accord. **Thus, while likely to squabble about respective obligations and further drift away from rapprochement, neither Iran nor the United States has the incentive or ability to take the new cycle of tension to a military confrontation.**

**2NC --- Iran Answers**

**Multiple factors constrain Iranian aggression or adventurism**

**Kaye 10** (Dalia, , RAND senior political scientist, “Dangerous But Not Omnipotent”, <http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG781.pdf>, ldg)

To accurately gauge the strategic challenges from Iran over a ten- to fifteen-year horizon, this study sought to assess the motivations of the Islamic Republic, not just its capabilities. **This approach**, although difficult given the complexities of the Iranian system, **is critical in identifying potential sources of caution and pragmatism in Iran’s policy formulation**. Our exploration of Iranian strategic thinking revealed that **ideology and bravado frequently mask a preference for opportunism and realpolitik**—the qualities that define “normal” state behavior. Similarly, when we canvassed Iran’s power projection options, we identified not only the extent of the threats posed by each but also their limitations and liabilities. In each case, we found significant barriers and buffers to Iran’s strategic reach rooted in both the regional geopolitics it is trying to influence and in its limited conventional military capacity, diplomatic isolation, and past strategic missteps. Similarly, tensions between the regime and Iranian society—segments of which have grown disenchanted with the Republic’s revolutionary ideals—can also act as a constraint on Iranian external behavior. ¶ This leads to our conclusion that analogies to the Cold War are mistaken: The Islamic Republic does not seek territorial aggrandizement or even, despite its rhetoric, the forcible imposition of its revolutionary ideology onto neighboring states. Instead, it feeds off existing grievances with the status quo, particularly in the Arab world. Traditional containment options may actually create further opportunities for Tehran to exploit, thereby amplifying the very influence the United States is trying to mitigate. A more useful strategy, therefore, is one that exploits existing checks on Iran’s power and influence. These include the gap between its aspiration for asymmetric warfare capabilities and the reality of its rather **limited conventional forces**, disagreements between Iran and its militant “proxies,” and the potential for sharp criticism from Arab public opinion, which it has long sought to exploit. In addition, we recommend a new U.S. approach to Iran that integrates elements of engagement and containment while de-escalating unilateral U.S. pressure on Tehran and applying increased multilateral pressure against its nuclear ambitions. The analyses that informed these conclusions also yielded the following insights for U.S. planners and strategists concerning Iran’s strategic culture, conventional military, ties to Islamist groups, and ability to influence Arab public opinion.

**Adv --- Cohesion**

**1NC --- NATO Fails**

**NATO cohesion does not provide any practical benefits.**

**Carpenter 22** — Ted Galen Carpenter, Senior Fellow for defense and foreign policy studies at the Cato Institute, PhD in U.S. diplomatic history from the University of Texas, 2022 (“NATO Security Dependents Are Not Useful Allies,” *CATO,* January 8th, Available Online at <https://www.cato.org/commentary/nato-security-dependents-are-not-useful-allies>)

SINCE THE end of World War II, U.S. officials have had an **unduly expansive** concept of what constitutes worthwhile strategic allies for the United States. In too many cases, the “allies” that Washington touts are **small**, **weak**, often **militarily useless** dependents. Worse, some of them are on bad terms with more **powerful neighboring states**. Under those circumstances, the so‐​called allies are **major liabilities** rather than assets to the United States. Indeed, they are potential snares, ones that can **entangle America** in unnecessary military confrontations.

Washington would do well to become far more selective about which nations it includes in its roster of allies, and U.S. leaders should stop elevating security dependents to the status of allies. When U.S. officials described the regimes that Washington installed through military force in Afghanistan and Iraq as allies, it became clear that they had lost even minimal understanding of the concept. That point became abundantly evident when their Afghan client collapsed almost overnight in the face of the Taliban military offensive. It’s time for U.S. policymakers to do better.

TROUBLING PROMISCUITY about acquiring weak U.S. security partners was evident even during the Cold War, and the tendency has become **even more pronounced** in the post‐​Cold War era. As the fiasco in Afghanistan (and its ugly predecessor in South Vietnam) confirmed, that problem with U.S. foreign policy has existed in multiple regions. However, the defect has become most acute with respect to Washington’s campaign to expand NATO into Eastern Europe. Since the mid‐​1990s, U.S. administrations have worked to add a menagerie of new NATO members, and it has done so with even less selectivity and good judgment than some people use to acquire Facebook friends.

Many of those new members have **very little to offer** to the United States as security partners. Indeed, some are mini‐​states, bordering on being micro‐​states. Such lightly armed Lilliputians would add little or nothing to Washington’s own capabilities—especially in a showdown with another major power.

As economic assets, their importance is **decidedly limited**, and militarily, they are **even less valuable**. It’s **hard to see** how new NATO allies such as Albania, Slovenia, Montenegro, and North Macedonia enhance America’s **power** and **security**. That point should be apparent based on size of population alone. Albania’s 2.87 million, North Macedonia’s 2.1 million, and Slovenia’s 2.07 million people put those countries squarely in the mini‐​state category, while Montenegro’s 628,000 barely deserves even that label. It doesn’t get much better with respect to either annual gross domestic product or size of military forces. Even Slovenia’s $52.8 billion GDP puts that country only eighty‐​sixth in the global rankings. Albania’s $15.2 billion (125th), North Macedonia’s $12.26 billion (135th) and Montenegro’s $4.78 billion (159th) are even less impressive.

The military forces that our new NATO allies can field are **not likely** to strike fear into Russia or any other would‐​be aggressor. Albania’s armed forces consist of 8,500 active‐​duty personnel, Slovenia’s consist of 8,500, and North Macedonia has 9,000 available. Montenegro’s active‐​duty force totals 2,400. In comparison, the Austin, Texas, police department has 2,422 people in its ranks.

Granted, the Cold War edition of NATO also had some mini‐​states as members, most notably Luxembourg and Iceland. However, those members were located within a stable, democratic Western Europe. Their defense also was geographically inseparable from Washington’s mission of protecting important military and economic players, such as West Germany, France, Italy, Spain, and Great Britain, from what appeared to be a totalitarian superpower with expansionist ambitions. That situation was qualitatively different from Washington’s gratuitous post‐​Cold War decision to manage the security of quarrelsome mini‐​states in the chronically volatile Balkans. Since the mid‐​1990s, the United States has entangled itself in the region’s parochial spats, but giving some of the countries NATO membership intensified America’s exposure to needless risks and burdens.

THE RISK-BENEFIT calculation is **even worse** with respect to some of the other small nations that have joined NATO in the post‐​Cold War era. Those partners are not merely irrelevant from the standpoint of U.S. security; they are potentially dangerous tripwires that could trigger a conflict between the United States and a nuclear‐​armed Russia.

That point underscores one very important difference between individuals casually amassing Facebook friends and the United States promiscuously adding new security mendicants. Facebook friends do not have the ability to entangle anyone in armed conflicts; irresponsible security dependents definitely can do so. Indeed, there are multiple examples throughout history of such clients snaring their patrons into devastating, unnecessary wars. One notable example was how Tsarist Russia’s fateful decision to give strong backing to Serbia in the latter’s escalating quarrel with Austria‐​Hungary following the assassination of Archduke Franz Ferdinand helped ignite World War I—and caused the utter ruin of the Russian empire.

The United States is flirting with a similar danger today regarding its small clients in Eastern Europe. President George W. Bush’s decision to support the NATO membership bids of the three Baltic republics was—and remains—highly provocative to Russia. One crucial way to reduce the danger of armed clashes between great powers is to show mutual respect for respective spheres of influence. Washington has repeatedly violated that principle by pushing NATO to expand right up to Russia’s border.

**2NC --- NATO Fails**

**Ukraine crisis proves.**

**Ranhotra 22** — Sanbeer Ranhotra, Political Researcher at TFIGlobal, 2022 (“The irrelevance of NATO is now out in the open,” *TFIGlobal,* February 25th, Available Online at https://tfiglobalnews.com/2022/02/25/the-irrelevance-of-nato-is-now-out-in-the-open/)

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

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

**NATO obsolete**

Christian **Whiton**, State Department senior adviser George W. Bush administration and Senior Fellow Center for National Interest, “NATO Is Obsolete” July 6, 20**18**, https://nationalinterest.org/print/feature/nato-obsolete-25167

Before President Donald Trump attempts real diplomacy with Russian President Vladimir Putin at a summit in Helsinki on July 16, he'll first be subjected to another summit. That first summit is a gathering of leaders of the North Atlantic Treaty Organization (NATO). These leaders continually assure the United States they are America's best allies, even as most contribute little to America's defense and rack up huge trade surpluses with the United States. Trump will insist on a better deal but should go farther and wind down U.S. membership in NATO. After the alliance was established in 1949, its first secretary general, Lord Hastings Ismay, summed up its purpose concisely: “to keep the Russians out, the Americans in, and the Germans down.” The unofficial mission matched the time well: Western Europe’s postwar future was clouded by the prospect of a Soviet invasion, American insularity, or German militarism— all possible given the preceding decades of history. Nearly seventy years later, none of these concerns still exist. Furthermore, NATO's opposing alliance during the Cold War, the Warsaw Pact, quit the Soviet Bloc in 1989, and the Soviet Union itself passed into history in 1991 —twenty-seven years ago. Despite endless searches for a new mission to justify its massive burden on U.S. taxpayers, **NATO has failed** to be of much use since then. As its boosters like to remind us, after 9/11, the alliance invoked its Article 5 mutual-defense provision on our behalf. But action from America’s allies did not follow the grandiose gesture—the NATO mission in Afghanistan relied mostly on U.S. forces and effectively failed. Today, the alliance’s bureaucrats and some member states spotlight a threat from Russia as a reason for keeping the organization alive, along with a laundry list of “train and equip” missions. Yet NATO members' defense budgets don't reflect a real sense of danger from Russia or anyone else. Among the twenty-nine members, only the United States is really serious about its Article 3 obligations to defend itself, spending approximately $700 billion or 3.5 percent of its GDP on defense. No other NATO member comes close to this proportion, and the vast majority fail even to meet the modest, self-imposed requirement to devote at least 2 percent of GDP to defense. Britain and Poland are rare members that meet the 2 percent requirement. One of the worst free-riders is Canada, which spends just 1 percent of its GDP on security, amounting to $20 billion. Furthermore, Germany spends a similarly pathetic 1.2 percent. Compare that to non-NATO members facing real threats, some of which spend 5-10 percent of their GDPs on defense. These include Saudi Arabia and the United Arab Emirates, who must contend with Iran and spend nearly a combined $100 billion. Israel, which faces the same enemy, adds $15 billion to the equation. Despite protestations of poverty at a time when their economies have never been larger, NATO members are more than willing to rack up additional liabilities, knowing America has their back. Last year, the alliance welcomed Montenegro. It is now poised to admit the Former Yugoslav Republic of Macedonia, which would mean the United States is pledged to defend a nation that devotes just $120 million per year to its own defense, not quite as much as the Cincinnati Police Department. But the reality is there is no truly capable Russian foe seriously threatening the West. Russia has one million uniformed personnel in its military, the world’s second-largest behind America, but the European Union could easily afford to match that with its combined $17 trillion economy—ten times larger than Russia’s. However, it needn’t bother as Moscow spends just $61 billion on its overwrought military, which doubles as an employment program. Russia’s Vladimir Putin has gotten the most from Russia’s military, occupying parts of Georgia and Ukraine and gaining influence in Syria by backing the Assad regime. Still, his success in all three cases rested heavily on surprises that Moscow seems unlikely to be able to repeat against prepared and adequately funded European militaries. Yer we should expect to hear none of this nuance at the NATO summit, as poohbahs of the dying old European political order gather to tut-tut President Trump in the alliance’s fancy new $1.4 billion headquarters, funded predominantly by American taxpayers. To get out of this abusive relationship, Trump should begin the process of limiting America's role in NATO. A good model is that of Sweden, which cooperates with NATO on some matters and not on others. Such an approach could allow joint training, but end the practice of having overburdened U.S. taxpayers foot the bill for wealthy Europeans' security. As part of this plan, Trump could mothball U.S. bases in Europe and shift most resources spent there and in the Atlantic to the Indo-Pacific region, where China and Iran pose real threats to America—and against which **NATO is irrelevant**. Europe is prosperous and treats America like a patsy. Let it stand on its own.

**1NC --- No Collapse**

**Even if the US pulls out of NATO it will be fine – they will just shift commitments**

**Rynning 18** (Sten Rynning is professor at the Department of Political Science, University of Southern Denmark, where he also heads the Center for War Studies. He researches NATO and modern war; <https://warontherocks.com/2018/09/a-europeanized-nato-the-alliance-contemplates-the-trump-era-and-beyond/>; 9-25-18)

NATO is unraveling and world crisis is upon us, writes Robert Kagan in response to the 2018 NATO summit. Kagan thus starkly depicts the worst-case scenario outlined in this essay. If Trump embodies a fatigue in the U.S. political system with enduring alliances, and if Russia becomes a U.S. partner of choice in tipping the scales of Eurasian land power against China, then NATO as a transatlantic alliance would indeed unravel, and Europe’s peace would be in question. Still, **even in this bleak scenario, it is unlikely that NATO would go away**. Rather, Britain is likely to step in as continental Europe’s offshore power, though, of course, with diminished capabilities compared to those of the United States. A Europeanized NATO would tie Britain to the continent and perhaps become part of the answer to the troubled British-E.U. relationship. The European Union would not be able to stand still in the face of such a security transformation. France and Germany would likely seek to rescue their institutional project by accelerating the construction of a core that would allow France to extend security guarantees to Germany in return for French access to German financial governance, and which would create an E.U. periphery, notably in Eastern Europe, alongside countries such as Ukraine and Belarus. It is probable that **Western Europe could rescue its commitment to collective institutions**, including collective defense, but it is unlikely that it could extend security guarantees far eastwards, as NATO today is able to. A revised bargain with Russia will then become necessary, one in which the sovereignty of Eastern European countries will be questioned.

**2NC --- No Collapse**

**Nothing can break the alliance – common interests outweigh**

Mark **Weisbrot** 8-27-**18**, co-director of the Center for Economic and Policy Research in Washington, DC, and president of Just Foreign Policy, “The Transatlantic Alliance Will Survive Trump” https://www.thenation.com/article/the-transatlantic-alliance-will-survive-trump/

Every week, often more than once a week, there’s another article in the major media or in foreign-policypublications about the demise of the post–World War II Anglo-American world order. These analyses typically single out the transatlantic alliance between the United States and Europe―two of the world’s largest economies―for special concern and anxiety as the underpinning of this world order. Not surprisingly, President Trump’s wildly fluctuating comments on NATO (despite the fact that he is expanding it), his unprecedented **rudeness to Europe**an leaders, and his **friendliness with** Vladimir **Putin** at the Helsinki summit have all added to the angst. The basic story behind this moaning and melancholy is that US leaders put together a “rules-based” system based on “open markets” and democracy (the two are sometimes seen as synonymous) that has fostered prosperity and relative stability. The United States was the only sizable industrial economy to emerge not only unscathed but doubled in size following the war. While others might have taken advantage of this unrivaled power for their own gain, the story goes, America’s beneficent rulers constructed a world order for the good of everyone. Trump is seen as a threat to its continued existence. This assessment of the postwar world order leaves out some 3 million dead Vietnamese and half a million dead in Indonesia, who might question the beneficence of this system if it had not killed them. A million dead Iraqis, if they could be heard, would probably also raise objections about whether US dominance has been in the interests of all. And there are hundreds of millions of people in Latin America, Africa, and other parts of Asia who suffered for decades under US-backed dictatorships, as well as US-sponsored wars. Much of the violent dysfunctionality in these countries today is a direct result of these interventions, as well as continuing US influence. In fact, as I write this now, the US military is directly involved in a war that has deliberately produced what the UN has called the worst humanitarian crisis in the world, in Yemen. That war has pushed more than 8 million peopleto the brink of starvation, created the worst outbreak of cholera in modern history, and killed thousands of civilians in bombing raids. Washington is providing midair refueling to the Saudi and UAE bombers, intelligence, targeting assistance, on-the-ground military personnel, and more―constrained only by growing opposition in Congress. But let us ignore these inconvenient truths for a moment, as almost all of these analyses do, and look at the present situation. In fact, the transatlantic **alliance is much stronger** than most of these analysts recognize. This is mainly because it is not just an alliance of democratic governments with shared values, but also one of the rich countries of the world―their ruling elites, that is―against the poor and middle-income countries of the world. The rules of the **W**orld **T**rade **O**rganization, to which 164 countries are bound, were written by US and European corporations. The WTO’s most significant achievement since its creation in 1995 was to increase US-style patent protection throughout the world, leading to the death of millions of poor people who cannot get access to essential medicines. After years of struggle, some of these rules were rewritten, but much damage remains. The WTO’s rules on agriculture also greatly disadvantage developing countries and seek to prohibit governments from subsidizing domestic production for domestic consumption to feed people who are badly malnourished, for example in India. WTO rules also make it much more difficult for developing countries to employ the industrial policies that high-income countries like the United States used to get where they are today. The **I**nternational **M**onetary **F**und, an organization that has 189 member countries, is run by the United States and Europe. In fact, for most of the world outside of Europe, the US Treasury Department is in charge. The World Bank, which by custom since 1946 has to have an American as its president, is also controlled by Washington and its allies, and cooperates with the IMF in promoting and imposing economic policies that Washington favors. These policies are often not in the interest of developing countries, as one would expect from organizations that are not accountable to low- and middle-income countries, or to any electorate. These are the institutions of global governance that exercise power in the world, other than the **UN** Security Council, where the transatlantic alliance must share **veto power** with **Russia and China**. The IMF, for most of the past half-century, has been the most important avenue of US influence over low- and middle-income countries. It has sat at the top of a creditors’ cartel, where countries that did not agree to IMF conditions would not get loans from other multilateral lenders (e.g., the World Bank) and sometimes not even from the private sector. This cartel lost influence in most middle-income countries in the first decade of the 21st century, but it has been coming back (e.g., inArgentina), and it still maintains its creditors’ cartel in poor countries. European leaders are quite angry about the Trump administration’s unilateral abrogation of the Joint Comprehensive Plan of Action, the negotiated agreement with Iran that had put an end to the threat that it would develop nuclear weapons in the foreseeable future. Europe clearly has much more of a security risk stemming from Middle East turmoil, which is worsened by Trump’s threatened war with Iran; not to mention all the political problems that have been created by the refugee inflow that was primarily a result of US intervention there. **But what did they do** about it, after their anxious pleading with Trump failed to move him? **Nothing**, because these leaders―quite apart from the people of Europe, who have been screwed royally since the Great Recession―need their beloved partner in crime. The United States is the gendarme of the rich countries’ global economic and political order. This is partly because Washington did not suffer the destruction that Europe did in the world wars, and partly because Europeans have developed welfare states that do not allow for the fantastically wasteful military spending that maintains 800 US military bases around the globe. But Washington’s weapons of mass and ordinary destruction are by no means its whole arsenal. The “exorbitant privilege” of being able to print the world’s most important currency, which makes up 60 percent of global reserves held by central banks, is another. When Lehman Brothers collapsed in 2008 and the world financial crisis hit, the Federal Reserve arranged currency swaps for its European partners to make sure they didn’t suffer any temporary international liquidity problems. On the other side of the divide, if you are outside Washington’s good graces, the **dollarized** world financial **system** allows the United States vast power to enforce **sanctions** against you (e.g., in the cases of Cuba, Venezuela, and Iran), whether or not the UN approves. Europe’s elites are **bound** to the rulers of the **U**nited **S**tates by virtue of their **common interest** in maintaining dominance over the world **economy**. This is true despite the fact that their spoils do not trickle down to the citizenry. This transatlantic dominance won’t last forever. Eurasia, the world’s largest land mass, which bred the colonial powers that conquered the world, continues to increase its economic integration, despite Washington’s efforts to counter this world-historical trend with its attempted TPP and TTIP commercial agreements. China’s economy is already 25 percent larger than that of the United States on a purchasing-power-parity basis (this is the measure most often used by economists for international comparisons, since it takes into account price differences between countries). In a decade, it’s projected to be about twice as big as that of the United States. Over time, European countries, led by their corporations and financial institutions, will look more to the East and less to the West as the world becomes more multipolar and the US share of the world economy shrinks. But for the near future, the **US and Europe**an elite **need each other** as the global hegemon tries to hang on to its unelected position. Trump can be as rude, crude, and ignorant as he pleases with his European allies, but **it won’t make them rebel** against the “leader of the free world.”

**1NC --- Democracy Answers**

**Democracies don’t prevent war — there’s no statistical evidence.**

**Doorenspleet 19** — Renske Doorenspleet, Associate Professor in Comparative Politics at the University of Warwick, Former Research Fellow of the Intrastate Conflict Program/International Security Program at the Belfer Center for International Affairs at the Harvard Kennedy School, holds an MA and Ph.D. in political science from Leiden University, 2019 (“Conclusion: The Power and Limits of the Democratic Peace Idea,” *Rethinking the Value of Democracy: A Comparative Perspective*, Edited by Jean-Paul Gagnon and Mark Chou, Published by Palgrave Macmillan, ISBN 9783319916569, p. 98-99)

My chapter, though, did not look for specifc studies which could support one specifc argument (e.g. ‘democracy is a good thing’ or ‘democracy has instrumental value as it brings peace between states’). The aim of the chapter was to investigate the question whether democracy leads to interstate war or peace, by analysing **dozens** of statistical studies which have been selected in a systematic way. The analyses revealed many caveats.

The first caveat is that **none** of the studies which have directly tested the democratic peace hypothesis demonstrated that democracy is the only and most important factor when explaining interstate war. Some studies provided evidence that other factors are significant as well, and other studies indicated that alternative explanations are much more powerful, sometimes even showing that the impact of democracy is simply spurious. Geographical and economic factors, for example, play a key role as well, and tend to be far more important, so it is certainly not only democracy which matters.

Secondly, these findings are based on quantitative studies, **which show correlation but not necessarily causation**. While there is a lively ongoing debate about the causal mechanisms, it is still unclear how we can understand and interpret the expected absence of interstate war between democracies. The number of studies which criticize these ideas has increased considerably since the mid-1990s, not just theoretically but particularly empirically as there is no strong evidence to back up the ideas that norms and institutional constraints are the key mechanisms (see Hayes 2011). Moreover, the quest to find the underlying mechanisms should not get priority anyway in future research, in my view, as the statistical evidence for the democratic peace hypotheses is weak overall (see frst caveat above).

Thirdly, democracies are not more peaceful than dictatorships. While there might be some evidence for democratic peace among democratic states (or at least a correlation), democracies are not more peaceful in general. The evidence for a monadic link is not clear, not signifcant and certainly not robust. There is no clear support for the monadic peace hypothesis which states that interstate war is less likely in democracies compared to dictatorships in general. And democracies do fight with dictatorships—**quite a lot**.

Finally, ‘democratizing for peace’ seems a dangerous route to take, as democratizing states fight most—more than both democracies and dictatorships. Democracies might not fght with each other, but the countries that are democratizing are quite **war-prone**. Moreover, there is convincing evidence that hybrid systems (or semi-democracies) are more likely to be involved in interstate wars, not only compared to countries with higher levels of democracy but also to countries with lower levels of democracy. Democratization can be a very unpredictable and possibly dangerous process, and the fndings in this chapter show that democratizing for peace is likely to end in a deadly disaster.

Based on those fndings, this chapter comes to the controversial conclusion that eventually we cannot defend the notion that it really matters whether you live in a dictatorship or democracy, at least not with regard to the likelihood that an interstate war will take place in your country. In other words, **democracy is not a panacea for peace in general, and we cannot be sure that people living in democracies have less chance to experience an interstate war** compared to people living in dictatorships. People living in democratizing and hybrid systems seem to be most at risk, which means promoting democratization would not be wise, at least not when achieving peace is the ultimate goal. Hence, war is most likely in democratizing countries. Still, the chance of an interstate war is low in the other political systems—so not only in democracies but in dictatorships as well. In this sense, the idea that democracies make a signifcant difference is not convincing.43 The (instrumental) value of democracy cannot be found in being less war-prone and bringing peace between countries.

**2NC --- Democracy Answers**

**DPT is false — studies empirically haven’t found democracy as most important when explaining war.**

**Doorenspleet 19** — Renske Doorenspleet, Associate Professor in Comparative Politics at the University of Warwick, Former Research Fellow of the Intrastate Conflict Program/International Security Program at the Belfer Center for International Affairs at the Harvard Kennedy School, holds an MA and Ph.D. in political science from Leiden University, 2019 (“Democracy and Interstate War,” *Rethinking the Value of Democracy: A Comparative Perspective*, Edited by Jean-Paul Gagnon and Mark Chou, Published by Palgrave Macmillan, ISBN 9783319916569, p. 76-82)

Caveat 1: It’s Not (Just) Democracy

While analyzing the selected articles, the first remarkable finding is that only a relatively small number of studies have actually tested the democratic peace hypothesis. Most of the studies have focused on the mechanisms (see next section, caveat 2), and hence seem to assume that there is a correlation between democracy and war. In this way, the majority of the studies—often unintentionally—reinforce the idea that democratic peace actually exists without testing this proposition. However, none of the studies that directly test the democratic peace hypothesis found strong evidence that democracy is the most important factor when explaining interstate war. All democratic peace studies have controlled for many possible alternative causes of the peace, such as economic development and growth, geographic distance and contiguity, power status, alliance ties, militarization and political stability. The findings show that **it is not just democracy which explains war, not at all**. Within this group of studies, which explicitly test the democratic peace hypothesis, four different types of fndings can be detected. I will discuss those results more in-depth in the rest of this section.

First Result: There Is Correlation, but Other Explanations Are Signifcant Too

The first subgroup consists of scholars who stress the importance of democratic peace, despite the fact their own analyses have shown that other factors are statistically signifcant as well (Maoz and Russett 1993; Rousseau et al. 1996; Gleditsch and Hegre 1997; Beck et al. 1998; Ray 2013). For example, some studies (e.g. Rousseau et al. 1996) included alternative independent variables in order to test realist arguments. They tested whether the distribution of power determines decisions to use force, and measures each state’s military capabilities relative to its opponent. A state’s military capability is the average of three elements: number of troops, military expenditures and military expenditures per soldier. They found that this realist variable was strong, positive and statistically signifcant at the 0.001 level in their analyses (see, e.g., Rousseau et al. 1996: 522, Table 2). However, not only a state’s military capabilities appeared to be an important explanation for peace. In addition, wealth, growth, alliances and contiguity played a crucial role when explaining interstate war (see, e.g., Maoz and Russett 1993: 632, Table 1).11 Moreover, when other factors are included, the impact of democracy on the likelihood of international crises is even spurious (Maoz and Russett 1993: 632; Henderson 2002: 141, see also p. 3).12 Still, scholars in this group keep defending the democratic peace idea, despite the fact that their own analyses showed the signifcance of alternative explanations.

Second Result: Initially There Is Correlation, but the Impact of Democracy Is Spurious When Other Explanatory Factors Are Included in the Models

The second subgroup of scholars is far more radical. Based on their own analyses, this group concludes that the democratic peace link is a spurious one (Weede 1984, 1996; Barbieri 1996; Mousseau 2013; Gartzke and Weisiger 2014).13 Typically, efforts to demonstrate the spuriousness of the statistical democratic peace pointed to other factors that, when accounted for ‘properly’, eliminated or dramatically reduced the statistical signifcance of shared democracy. Hence, the studies in this second group did not find strong evidence for the democratic peace hypothesis anymore, once other explanatory factors were included in the models.14

One of the most convincing alternative explanations of peace between countries is that there is no democratic peace, but a capitalist peace instead. The settlement in Germany and Japan succeeded because of the establishment of capitalist peace. Because of economic support by the Americans, who encouraged free trade and offered trade opportunities in practice as well, the poorer economies in Europe and Japan would gain economically, resulting in ‘economic growth, prosperity, and, ultimately, free trade among most of the more technologically advanced economies’ (Rasler and Thompson 2005: 232). By establishing and expanding free trade, the incentives for war would quickly decrease among trading states, according to this approach. To prevent new interstate wars after World War II, the capitalist peace was a far more important factor than the American promotion of democracy and its political institutions.

The capitalist peace, or capitalist peace theory, also states that economic development accounts for both democracy and the peace among democratic nations. Economic development is a key factor to explain democracy (Lipset 1959; see also Hegre 2003; Weede 2004).15 Moreover, economic development also plays a role when explaining peace, and the presence of market-oriented economies in countries have a positive impact on both democracy in those countries and peace between them (Mousseau 2000, 2002, 2003, 2005, 2013; see also Hegre 2014). Democratic peace only exists when both democracies have high levels of economic development, when economic development is well above the global median.

In fact, the poorest 21% of the democracies studied, and the poorest 4–5% of current democracies, are signifcantly more likely than other kinds of political systems to fight each other (see, e.g., Mousseau 2005). Moreover, if at least one of the democracies involved has a very low level of economic development, then democracy cannot prevent war.16 Still, there is a pacifying effect of free trade and economic interdependence, which is more important than the effect of democracy, because the former affects peace both directly and indirectly, by producing economic development and ultimately, democracy (see Weede 2004).17

Capitalist peace is not the only alternative explanation. Shared interests in general, and political similarities in specifc, can also be seen as an important second alternative explanation for war and peace between countries (Farber and Gowa 1995, 1997; Gartzke 2007; Gowa 1999; Henderson 2002). Democracies are not peaceful to each other because they are democratic, but rather because they are similar. So the difference of the scores of both countries also contributes to the confict proneness of the dyad. If the difference in levels of democracy is big, then the chance of confict is higher (cf. Oneal and Russett 1997: 281–282).

Many researchers have conflated both the conflict-dampening impact of joined democracy and the confict-exacerbating impact of political distance in the variables focusing on political systems, but as Errol A. Henderson (2002: 32) convincingly argued: ‘Fusing these two contrasting attributes in a single variable makes it diffcult to distinguish between the competing processes’. Therefore, it is better to include an additional variable of ‘political dissimilarity’ in the model. Henderson (2002) was one of the frst scholars who included this variable and measured it by taking the absolute value of the difference between the two states’ scores. His main variables were not only political similarity, but also geographic distance and economic interdependence, and he concluded that democratic peace is a statistical artefact which disappears when those other variables are taken into account. Political similarity clearly has a pacifying effect18 (see Werner 2000; Henderson 2002; Beck et al. 2004), and it is not democracy per se which is the decisive factor.19

Hence, the benefts of trade and trade interdependence are essential explanations, while democracy is spurious or at least subordinate (see also Rosecrance 1986; Weede 1984, 1996; Hegre 2000, 2014; Jervis 2002; Souva 2003; Rasler and Thompson 2005: 235; Mousseau 2000, 2002, 2003, 2005). Based on those studies, it is safe to conclude that democracy, on its own, is an unlikely cause of the democratic peace.

Third Result: There Is Correlation, but Other Explanations Are Much Stronger

This same point that democracy is just one of the explanations for peace (and not even a very important one) is also at the core of studies in the third subgroup. Scholars of this group keep arguing that there is support for the democratic peace hypothesis, and that the link is not spurious. In this sense, they are less radical than the second group of scholars, as they do not completely reject the value of democracy for peace. On the other hand, their own analyses have clearly shown that alternative factors—hence other factors than democracy or type of political system— are not only statistically signifcant but also more important when trying to explain interstate war (Bremer 1992; Gelpi 1997; Oneal and Russet t 1999a, b; Reiter and Stam 2002; Peterson 2013; Caselli et al. 2015).

Theoretical arguments and empirical evidence suggest that democracy is not the most important factor, while war is more likely to occur between states that are geographically proximate, approximately equal in power, major powers, allied, economically advanced and highly militarized than between those that are not. Bivariate analyses of these factors in relation to the onset of interstate war over all pairs of states in the period from 1816 to 1965 have generally supported these associations. However, multivariate analyses revealed some differences. Stuart Bremer (1992), for example, showed that some factors are far more important than others. The existence of a dangerous, war-prone dyad can be best explained by the presence of contiguity, the absence of an alliance and the absence of more advanced economy. The absence of democratic polity and other factors (absence of overwhelming preponderance, and presence of major power) are less powerful. Overall, these fndings suggest that our research priorities may be seriously distorted and that we should not focus too much on the perceived positive impact of democracy, but on other factors (such as alliances and economic factors) instead.

Fourth Result: There Is Correlation, but Only Under Certain Specific Conditions

The final subgroup of scholars argues that we cannot unconditionally accept the idea that democratic peace exists in general, so always and everywhere. Their statistical studies clearly showed that support for this hypothesis heavily depends on other factors. The chance of democratic peace depends not just on the specifc historical period (Cold War or not; Gibler and Sarkees 2004; Siverson and Emmons 1991; Weede 1984), but also the stage of the confict (beginning, duration or severity; see Bremer 1993; Bennett and Stam 1996; Reed 2000), and on the neighbourhood instability (extent of confict in the region; see Gibler and Braithwaite 2013; Gibler and Miller 2013). Despite the differences between the studies, there is one common finding in all studies: when explaining interstate war, we cannot just rely on the impact of democracy, as it is too much dependent on other factors.

Several scholars found strong evidence for the idea that democratic peace exists, but only during some **specific historical periods**. Based on this evidence, they concluded that democratic peace is simply a statistical artefact of the Cold War. For example, Henry Farber and Joanne Gowa (1995) found statistical support for the idea that peace between democracies is an artefact of the Cold War, when the threat from the communist states forced democracies to ally with one another (see also Mearsheimer 1990). Sebastian Rosato (2003) also argued that most of the signifcant evidence for democratic peace has been observed after World War II; and that it has happened within a broad alliance, which can be identifed with NATO and its satellite nations, imposed and maintained by American dominance.

Since the Second World War, war has become a very costly affair. Scholars discovered that only a handful of states are ‘capable of engaging in major power warfare. That process of elimination has not yet extinguished the possibility of major power warfare, but it has lowered its probability immensely’ (Rasler and Thompson 2005: 219). The chance to achieve something in a war is low in general, and even lower in a bipolar world with two big power players risking high nuclear war costs (Jervis 2002). While war became more costly, trade became less costly; as a consequence, the war/trade costs increased during the Cold War (Rosecrance 1986; see also Jervis 2002). In such a world, war and confict have become less attractive, while trade and cooperation have become more appealing (Rasler and Thompson 2005: 219). Hence, more states decided to adopt trading strategies in order to prevent confict and war as much as possible. In the end, democracy was part of the story, but only a very small part with a subordinated role next to the power dynamics during the Cold War, the costs of warfare and the benefts of trade.

Some scholars found evidence that the democratic peace still exists in the post-Cold War period (Park 2013) which weakens this argument. However, most analyses showed that dyadic dispute rates have converged after the Cold War (see, e.g., Gowa 2011). Moreover, jointly democratic dyads are likely to be allied only after 1945 (see Gibler and Sarkees 2004); during the 1816–1944 time period, there is even a negative relationship between democratic dyads and alliance formation.20 These findings cast serious doubts on the idea of a general existence of democratic peace.

Not only the historical period, but also the stage of the confict is crucial. Some scholars in this group provided evidence that democratic peace is not universal, but that it depends on the stage and whether we focus on the beginning, duration or severity of the confict. Although joint democracy has some pacifying effects on the onset of confict, the results suggest that they are unrelated to the escalation of disputes to war (see Reed 2000). Moreover, democratic peace is dependent on the neighbourhood instability. Democracies often have few territorial issues over which to contend, as they tend to be part of a stable region. Democracies only seldom have territorial disputes with their neighbours, and therefore they can more easily choose favourable conficts to escalate. The type of political system does not predict confict selection or victory once controls are added for issue salience (Gibler and Miller 2013; see also Park and James 2015). There is an interaction between joint democracy and regional instability, which confrms the idea that the effects of type of political system on continued confict apply mostly to dyads in peaceful regions (Gibler and Braithwaite 2013; see also Park and James 2015). Very democratic countries might even become more aggressive and faster than other political systems, once the region becomes more hostile (see, e.g., Baliga et al. 2011).

The General Lesson from the Results in a Nutshell (Caveat 1)

In short, regardless of the differences between the statistical studies on democratic peace, all findings have indicated that other explanations are important as well. It is clear that democracy is just one of the explanations, and certainly not the most important one,21 sometimes even spurious and often heavily dependent on other factors. It is not (just) democracy to be preoccupied with, when trying to prevent war between countries (Table 3.1).

**DPT False — economic norms theory fully accounts for it.**

**Mousseau 13** — Michael Mousseau, Professor at the University of Central Florida, teaching International Relations Theory, Political Economy of War and Peace, and Terrorism and Insurgency, former professor at Koç University, holds a Ph.D. in Political Science from Binghamton University and an M.A. in International Studies from the University of Denver, 2013 (“The Democratic Peace Unraveled: It’s the Economy,” *International Studies Quarterly*, Volume 57, Available Online via Academia at https://www.academia.edu/19753792/The\_Democratic\_Peace\_Unraveled\_It\_s\_the\_Economy, Accessed 10-02-2018, pg. 191-193)

Model 2 presents **new knowledge** by adding the control for economic type. To capture the dyadic expectation of peace among contract-intensive nations, the variable Contract-intensive EconomyL (CIEL) indicates the value of impersonal contracts in force per capita of the state with the lower level of CIE in the dyad; a high value of this measure indicates both states have contract-intensive economies. As can be seen, the coefficient for CIEL ()0.80) is **negative** and **highly significant**. This corroborates that impersonal economy is a highly robust force for peace. The coefficient for DemocracyL is now at **zero**. There are **no other differences between Models 1 and 2**, whose samples are identical, and no prior study corroborating the democratic peace has considered contract-intensive economy. Therefore, the standard econometric inference to be drawn from Model 2 is the nontrivial result that **all prior reports** of democracy as a force for peace are probably **spurious**, since this result is predicted and fully accounted for by **economic norms theory**.

CIEL and DemocracyL correlate only in the moderate range of 0.47 (Pearson’s r), so the insignificance of democracy is not likely to be a statistical artifact of multicollinearity. This is corroborated by the variance inflation factor for DemocracyL in Model 2 of 1.85, which is well below the usual rule-of-thumb indicator of multicollinearity of 10 or more. Nor should readers assume most economies: While almost all nations with contract-intensive economies (as indicated with the binary measure for CIE) are democratic (Polity2 > 6) (Singapore is the only long-term exception), more than half—55%—of all democratic nation-years have contract-poor economies. At the dyadic level in this sample, this translates to 80% of democratic dyads (all dyads where DemocracyBinary6 = 1) that have at least one state with a contract-poor economy. In other words, not only does Model 2 show no evidence of causation from democracy to peace (as reported in Mousseau 2009), but it also illustrates that this absence of democratic peace includes the **vast majority**—80%—of democratic dyad-years over the sample period.

Nor is it likely that the causal arrow is reversed—with democracy being the ultimate cause of contract-intensive economy and peace. This is because correlations among independent variables are not calculated in the results of multivariate regressions: Coefficients show only the effect of each variable after the potential effects of the others are kept constant at their mean levels. If it was democracy that caused both impersonal economy and peace, then there would be some variance in DemocracyL remaining, after its partial correlation with CIEL is excluded, that links it directly with peace. The positive direction of the coefficient for DemocracyL informs us that no such direct effect exists (Blalock 1979:473–474).

Model 3 tests for the effect of DemocracyL if a control is added for mixed-polity dyads, as suggested by Russett (2010:201). As discussed above, to avoid problems of mathematical endogeneity, I adopt tohe solution used by Mousseau, Orsun and Ungerer (2013) and measure regime difference as proposed by Werner (2000), drawing on the subcomponents of the Polity2 regime measure. As can be seen, the coefficient for Political Distance (1.00) is positive and significant, corroborating that regime mixed dyads do indeed have more militarized conflict than others. Yet, the inclusion of this term has no effect on the results that concern us here: CIEL ()0.85) is now even more robust, and the coefficient for DemocracyL (0.03) is above zero.7

Model 4 replaces the continuous democracy measure with the standard binary one (Polity2 > 6), as suggested by Russett (2010:201), citing Bayer and Bernhard (2010). As can be observed, the coefficient for CIEL ()0.83) remains **negative and highly significant**, while DemocracyBinary6 (0.63) is in the positive (**wrong**) direction.

As discussed above, analyses of fatal dispute onsets with the far stricter binary measure for democracy (Polity = 10), put forward by Dafoe (2011) in response to Mousseau (2009), yields perfect prediction (as does the prior binary measure Both States CIE), causing quasi-complete separation and inconclusive results. Therefore, Model 5 reports the results with DemocracyBinary10 in analyses of all militarized conflicts, not just fatal ones. As can be seen, the coefficient for DemocracyBinary10 ()0.41), while negative, is not significant. Model 6 reports the results in analyses of fatal disputes with DemocracyL squared (after adding 10), which implies that the likelihood of conflict decreases more quickly toward the high values of DemocracyL. As can be seen, the coefficient for DemocracyL 2 is at zero, further corroborating that even very high levels of democracy do not appear to cause peace in analyses of fatal disputes, once consideration is given to contractintensive economy. Models 3, 4, and 6, which include Political Distance, were repeated (but unreported to save space) with analyses of all militarized interstate disputes, with the democracy coefficients close to zero in every case. Therefore, the conclusions reached by Mousseau (2009) are corroborated even with the most stringent measures of democracy, consideration of institutional distance, and across all specifications: The democratic peace appears **spurious**, with contract-intensive economy being the **more likely explanation** for both democracy and the democratic peace.

**1NC --- Convergence Now**

**Integration, progress, and proper protections are coming in the status quo**

**Smeets, 21** (Max Smeets, Center for Security Studies, ETH Zürich (Switzerland), Aug 2021, accessed on 6-19-2022, Hcss, "NATO Allies' offensive cyber policy: A growing divide?", <https://hcss.nl/wp-content/uploads/2021/08/Essay-3-NATO-allies-offensive-cyber-policy-A-growing-divide-3.pdf)//Babcii>

NATO allies have made slow but steady progress when it comes to crafting policy to deal with cyber security challenges. Yet this progress has not always been made in a collaborative fashion. Especially when it comes to the development and deployment of offensive cyber capabilities, NATO allies are increasingly diverging in policy. This is a worrying development and deserves more attention than it has so far received. Steady progress Member states **agree on the critical need** for a **coherent cyber policy.** Almost all NATO allies have developed both a cyber security strategy and a cyber defense strategy.[[1]](https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/#_ftn1) Some states have published updated versions over the years to reaffirm cyber security as an issue of national security importance, to tweak institutional responsibilities, or to articulate changes in the threat landscape. In addition, since 2018, most NATO allies have established a military cyber organization (either a command or unit) with a mandate to conduct cyber effect operations – that is, cyber operations intended to disrupt, deny, degrade and/or destroy.[[2]](https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/#_ftn2) There is also **shared recognition that international law applies in cyberspace**, although allies have yet to spell out the legal procedures for operating in this new “domain of warfare.” These developments have been both reflected in, and aided by, policy progress made at the inter-governmental level. At the Prague Summit in 2002, NATO for the first time recognized that the Alliance should “Strengthen our **capabilities to defend against cyber attacks**.”[[3]](https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/#_ftn3) In 2008, at the Bucharest Summit, there was another milestone development, when NATO adopted a “Policy on Cyber Defense,” aiming to “protect **key information** systems **in accordance with their respective responsibilities**; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack.”[[4]](https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/#_ftn4) In the same year, the Cooperative Cyber Defence Centre of Excellence – a NATO accredited international research institution – was established in Tallinn, Estonia. In 2016, at the Warsaw Summit, cyberspace was officially recognized as a “domain of operations” and allies made a Cyber Defense Pledge to enhance their cyber defenses.[[5]](https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/#_ftn5) The 2018 Brussels Summit and 2020 London Summit reiterated NATO’s commitment to implement the Cyber Defense Pledge and operationalize the Cyber Operations Center, responsible for situational awareness and the centralized planning of cyber operations and missions.[[6]](https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/#_ftn6) In January 2020, the Allied Joint Doctrine for Cyberspace Operations was published “to plan, execute and assess cyberspace operations (CO) in the context of allied joint operations.”[[7]](https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/#_ftn7)

**1NC --- Alt Causes**

**Alt causes for NATO collapse**

**Boffey 18** (Daniel Boffey; Guardian's Brussels bureau chief; <https://www.theguardian.com/world/2018/jun/19/transatlantic-relationship-at-risk-says-nato-chief>; 6-19-18)

The head of Nato has warned that the deep divisions between the US under Donald Trump and its European allies are not going away and there is no certainty that the transatlantic relationship and its military alliance will survive. Against a backdrop of Trump’s open baiting of the German chancellor, Angela Merkel, over immigration and her domestic difficulties, Jens Stoltenberg has called for all Nato members to work to avoid a disastrous breakdown in western unity. Writing in the Guardian, Nato’s secretary general admits that “political storm clouds” are putting a strain on the ties that bind the Nato allies. But, in an appeal to leaders before the military alliance’s summit in July, the former prime minister of Norway says that “where differences persist, we must limit any negative impact on our security cooperation”. Stoltenberg – who is meeting Theresa May in Downing Street on Thursday as he prepares for the summit in Brussels – writes: “Since the alliance was created almost 70 years ago, the people of Europe and North America have enjoyed an unprecedented period of peace and prosperity. But, at the political level, the ties which bind us are under strain. “**There are real differences between** the United States and other **allies over issues such as trade, climate change and** the **Iran** nuclear agreement. “These disagreements are real and they won’t disappear overnight. In fact, **nowhere is it written in stone that the transatlantic bond will always thrive**. That doesn’t, however, mean that its breakdown is inevitable. We can maintain it, and all the mutual benefits we derive from it.” Stoltenberg’s intervention comes at a point of extreme tension among the leadership of the western powers. In seeking to defend his administration’s policy of separating children from their parents at the country’s border, Trump launched an extraordinary attack on Merkel and the EU on Tuesday, likening Europe to a “migrant camp” while claiming that “the people of Germany are turning against their leadership as migration is rocking the already tenuous Berlin coalition”. Merkel is embroiled in a tense standoff with her interior minister over immigration. She faces a two-week deadline to find a European solution or risk the collapse of her governing coalition. Trump has already caused a fracture in relations with traditional US allies by reneging on his country’s commitments in both the Paris climate change agreement and the nuclear deal with Iran. He is also threatening a transatlantic trade war with the EU, and has criticised Germany and others for not spending enough on defence and freeloading off the US. Of the 29 Nato members, only eight, including the US and the UK, spend more than 2% of their GDP on defence, a threshold that the alliance agreed should be met by all the countries by 2024. Germany spent €37bn (£32.5bn), or 1.2% of GDP, on defence last year. Asked for his position last month on those countries underspending, Trump warned: “They’ll be dealt with.” Greater “burden sharing” is set to be a theme of the Nato summit in Brussels, along with Stoltenberg’s desire to improve the readiness of Nato forces to deploy in quick order, and to build on the alliance’s counter-terrorism efforts, including through the training of the Iraqi military and an extension of financing for Afghan forces until 2024.

**1NC --- Turn --- Trust Turn**

**Cross-alliance intelligence-sharing collapses NATO cohesion and cyber operations**

**APRA, 20** (Association for Political Risk Analysis, “The Looming NATO Offensive Cyber Policy’s Challenges of Harmonizing Deterrence and Decision-making”, APRA, Sep 27, 2020, https://www.aprascpo.org/post/the-looming-nato-offensive-cyber-policy-s-challenges-of-harmonizing-deterrence-and-decision-making)//Babcii

Testing Alliance Consensus and Decision-making The Alliance’s decision-making principle of consensus further complicates the negotiations and agreement of a NATO offensive cyber policy. The above-mentioned nuclear example almost exclusively concerns kinetic and state-level physical destruction of massive proportions. The dire consequences of the extremity of possible nuclear proliferation are enough to establish credibility, deterrence, and is a comparatively simpler way in getting its 30 member states on board, especially in the context of Cold War bipolarity. Cyberspace as a domain of war contains a myriad of vested technical issues including the difficulty of attributing attacks to specific adversaries. Even though this is one the most prominent difficulties according to a variety of research in cybersecurity, more recent analyses published by NATO's Cooperative Cyber Defence Centre of Excellence have suggested that the attribution gap is gradually decreasing in size due to heavy research and development investment into web tracing and identification designs largely spearheaded by the US (Burton 11). A dynamic understanding of deterrence in cyberspace as formerly suggested by taking into consideration social and historical context will also alleviate the traditionally ‘impossible’ problem of attribution. While such technical capabilities play a crucial role in swaying the allies’ considerations and decisions, the political and strategic issues of simply conceptualizing an offensive cyber policy are examined in closer detail here. Trust and Transparency The transparency and capability-sharing quality of NATO may give way for disagreement amongst allies. Although the Alliance’s communication on a strategic and policy level is transparent, it still possesses enough opaque room to maneuver on an operational and tactical level. Furthermore, the problem of American supremacy in cyber capabilities and NATO’s reliance on its critical perspective may displease EU member states like France in their pursuit of strategic autonomy aside from its prevailing aversion to today's American leadership. A new demand for cross-alliance intelligence-sharing on offensive cyber capabilities can also exacerbate internal trust issues with the US. The global surveillance disclosures from 2013 onwards revealed allied surveillance and spying activities which damaged confidence in NATO (Smeets; 2018). Discussion of further integrated intelligence-sharing strategy under an offensive cyber policy can create tension between Five Eyes states (Canada, the US, and the UK) and other NATO allies. Doctrine Diversity Another overarching aspect with the potential to determine allies’ reception and leniency towards an offensive cyber strategy is the diversity of threat perception among NATO allies. The diversity across allied standards in defining the parameters of cyberattacks and the lack of overarching offensive cyber policy could result in strategic ambiguity and discourage retaliation (Arts 2). These differences stem from varied threat perceptions and cyber norms. Nationally, both threat perception and cyber norms are influenced by the state’s experience with malicious cyberattacks and its media and public opinion; and externally, the state’s engagement in bilateral and multilateral engagements are the most effective ways in which threat perception and cyber norms are shaped (Lewis 575). This hints at the political interest of near-Russia states like Estonia and Finland to possess well-rounded cyber norms and threat perception. Conversely, policy engagements on offensive capabilities would also shape NATO allies’ understanding as a whole. Without multilateral definitions, allies like Luxembourg and Iceland who have not experienced similar events do not benefit from harmonized knowledge and may not find justification to prioritize the strengthening of cyber capabilities when allocating funds from the common NATO budget. Not to mention the financial commitment issue affects trust in the Alliance overall as well.

**The plan destroys trust --- NATO hates the idea of OCO’s, and even the discussion creates backlash --- The plans forced disclosure also causes backlash to US surveillance**

**Fidler et al., 13** (David Fidler, Richard Pregent, and Alex Vandurme, Fidler, James Louis Calamaras Professor of Law, Indiana University Maurer Schoolof Law; and Senior Fellow, Indiana University Center on Applied Cybersecurity Research., Pregent, Legal Advisor, NATO Allied Command Counterintelligence, Vandurme, Head, Technical Center Engineering, NATO Computer Incident ResponseCapabilit, Fal 2013, accessed on 6-19-2022, Scholarship.law.stjohns, "NATO , Cyber Defense, and International Law", https://scholarship.law.stjohns.edu/cgi/viewcontent.cgi?article=1024&context=jicl)//Babcii

Concerning the three categories and the potential policy shifting described above, NATO finds itself in a difficult situation that, under current NATO practices, will be hard to escape. In terms of the cyber threat, defense, and technology approaches, NATO reflects behavior that puts the Alliance at a disadvantage. NATO tends to be conservative in terms of legal issues, meaning that the Alliance does not promise to be a fruitful forum for adapting or revising legacy rules to reflect the particular challenges **cyber** poses. Similarly, with NATO operating on the basis of consensus, the Alliance’s decision-making processes might have difficulty handling governance questions created by the cyber defense **approach**, such as how “active” should NATO cyber defense be. Operationally, NATO cyber defense appears more static and reactive than active in orientation—a situation that could lead NATO cyber defense to become a cyber “Maginot line” rather than an effective defensive strategy. It is not clear whether NATO members could reach consensus on what more active cyber defense activities would be permissible under international legal principles on sovereignty and non-intervention. As noted earlier, NATO functions with the capabilities its members make available to it, meaning that NATO’s technological capabilities in cyber might not reach cutting-edge status, leaving NATO cyber defense behind the global technological curve in cyberspace. This problem is exacerbated if policy makers in leading powers, such as the United States and China, are placing more reliance on developing, deploying, and using full-spectrum cyber technological capabilities because of the perceived pitfalls of other approaches and the mounting geopolitical competition now affecting cyberspace. NATO members are also extraordinarily sensitive to the Alliance having any offensive cyber capabilities or even discussing the need to think about the value of cyber capabilities and operations in missions NATO might undertake (as NATO has done with other technological developments affecting its military missions).44 The North Atlantic Council has not discussed, let alone authorized, the development of offensive capabilities, doctrine, or rules of engagement in the cyber realm.45 Whether NATO members could agree on what **offensive cyber operations** international law would permit is also not clear, especially in light of difficulties cyber presents to the international law on armed conflict **revealed by the Tallinn Manual** and other analyses.46 Events outside the specific context of NATO cyber defense might also adversely affect NATO cooperation. For example, in June 2013, negative European reactions to the disclosure of a secret U.S. surveillance program targeting cyber activities of foreign nationals, code-named PRISM, reflected new transAtlantic tensions on **government surveillance in cyberspace**, its implications for privacy and other civil liberties, and the potential for European-American cooperation on cybersecurity. The Washington Post reported that “[t]he **discontent from Europe pointed** to the breadth of fallout from the affair and to the potential for fresh strains between the United States and allies wary of American intrusiveness.”47 Whatever the long-term impact of this political fallout, the short-term consequences will likely not create more willingness among NATO members to become more ambitious with NATO cyber defense.

**Allies say no to OCO’s and countries with OCO’s don’t want to integrate because of free-riding**

**Veenendaal et al 16** (Matthijs Veenendaal has been working for the Netherlands Ministry of Defence since 2006 in various policy positions. He is currently stationed as a researcher at the Strategy Branch of the NATO Cooperative Cyber Defence Centre of Excellence in Estonia. Kadri Kaska is a researcher at the NATO Cooperative Cyber Defence Centre of Excellence. MAJ Pascal Brangetto is a supply officer in the French Army. “Is NATO Ready to Cross the Rubicon on Cyber Defence?” June 2016 https://ccdcoe.org/uploads/2018/10/NATO-CCD-COE-policy-paper.pdf)

Given modern armed forces’ dependency on digital technology, it is legitimate to expect that NATO would adapt to this new reality. Since 2002, NATO has invested significantly in improving the defence of its networks. However, NATO has shown **little inclination** to move away from its current purely defensive posture in cyber defence. At the political level, Allies remain reticent when it comes to discussing the options of using military (offensive) capabilities within a NATO setting. For most of them, cyber operations are generally still uncharted territory in which confusion abounds. Moreover, Allies that have invested heavily in cyber capabilities worry that others might benefit without making a similar investment themselves. Allies therefore remain reluctant to engage in any meaningful discussion on the position and role of cyber capabilities in military operations within the Alliance.

**Case-turn --- Info-sharing Bad: Defense**

**1NC --- Info Sharing Fails**

**Cyber info sharing fails — too unpredictable, technical hurdles, and uncertain effects.**

**Jacobsen 21** — Jeppe T. Jacobsen, Visiting Scholar at New York University, former Cyber Coordinator at the Ministry of Foreign Affairs of Denmark, Ph.D. candidate at the Danish Institute for International Studies and the Center for War Studies at the University of Southern Denmark, M.A. in International Politics from the University of London, M.A. in Political Science from the University of Aarhus, 2021 (“Cyber offense in NATO: challenges and opportunities,” *International Affairs,* May, Available Online at <https://academic.oup.com/ia/article/97/3/703/6205395?login=true>)

Challenges to a smooth integration of cyber effects

The abovementioned incidents have led cyber-conflict scholars to point to **several technical** and **practical difficulties** in the operational integration of cyber effects.29 In the interviews and background conversations that contributed to this study, three of these difficulties were continuously reiterated when discussing successful integration of cyber effects into NATO operational planning: the temporal dimension of developing exploits; the assessment of battle damage; and the problem of confliction.

Developing exploits—a matter of time

One of the characteristics of cyber attacks that receives most attention is the fact that they **hit suddenly** and **without warning**.30 While this is often the case, the central question for operational integration is not the speed at which they hit their target, but the speed with which the tools and techniques that exploit IT vulnerabilities in order to deliver cyber effects can be developed. Like conventional weapons, the cyber tools—the exploits or cyber weapons—take time to develop. However, an exploit is often harder to reuse than a conventional weapon, as it is more dependent on a meticulous analysis and target preparation—in this case, specifically, the target's IT infrastructure. Without knowing the adversary's IT systems and its vulnerabilities better than the adversary itself, meaningful cyber weapons are impossible to develop.

The fact that knowledge about the target is linked not only to the deployment of a weapon but also to its development influences the extent to which it can be used and reused. Stuxnet, for example, required **years of development**, **testing** and **perfecting** before it could deliver the intended effect on the Iranian centrifuges. Despite the techniques used in the Stuxnet malware having been found in other malware,31 Stuxnet lost its ability to destroy the centrifuges when it was discovered and the IT vulnerabilities that enabled it were patched. Importantly, part of the complexity of Stuxnet relates to the US–Israeli intention to keep the effect secret. In a hot conflict, secrecy in terms of the effect is often less important, and thus the development and deployment of cyber effects do not necessarily have to be as complex and time-consuming.

This observation does not necessarily change the fact that the development of exploits often has to **precede** the military confrontation in which they are intended to be used. NATO states that want to deliver cyber effects in NATO operations must try to gain access to Russia's or other potential adversaries' critical military networks to identify and exploit IT vulnerabilities. As several informants emphasized, if states wait for a conflict to escalate before they begin the development of exploits, it is most likely to be **already too late**.32

The alternative to penetrating adversary networks in peacetime is for states to rely on the exploitation of vulnerabilities in as many commercial off-the-shelf products as possible. This can be done, for example, by purchasing exploits from private companies offering this service, in the hope that it will then be possible to quickly create an overview of the enemy's IT infrastructure and adapt the exploits to this environment when a conflict escalates. The latter approach is more likely to succeed against adversaries with low network security, which does not apply in the case of Russia, or in contexts where less sophisticated and less closely targeted cyber effects are required.

Whether member states develop sophisticated exploits for future targeted effects or stockpile well-known exploits to cause more minor effects, they **cannot**—as several informants indicated—**be certain** that they will be able to deliver the cyber effect at the specific time it is requested by CYOC. This is because the IT vulnerabilities upon which exploits depend **might not exist** for ever. Cyberspace is a **dynamic environment**: vulnerabilities are patched, systems are updated or replaced and bad IT security practices are identified and improved. This means that exploits are **temporary in nature** and **cannot be stored** for later use.33 States must constantly ensure that the exploits still work, which requires minor adjustments when updates take place. As a consequence, the larger the military ‘cyber arsenal’, the more **technically skilled** human resources are needed for its maintenance. In the current labour market, where recruitment and retention of a cyber workforce is difficult, extensive investment is required for states to be able to stand ready with cyber effects available when requested.

In short, if a state is to offer a cyber effect in a NATO operation, then the state is likely to have to be able, first, to predict what Russian IT systems it is going to target months or years in advance, and second, to marshal the necessary resources to develop and maintain a large array of exploits that can be used against these systems. Even if this is successfully done, the state still faces difficulty in ensuring that an effect is delivered as promised.

Assessing effects—ensuring proportionality and discrimination

How likely is it that the requested cyber effect will be delivered? The answer to this question is **not clear**, in respect of either its preparation or its execution. This is not only because IT vulnerabilities are constantly discovered and patched; it is also because of the difficulty of assessing the effects and possible side-effects of an exploit when navigating and analysing complex IT infrastructures. In other words, reconnaissance is difficult in cyberspace, and so is the containment of effects. The Russian attempt to use ransomware aimed at disrupting critical Ukrainian infrastructure in 2017, for example, succeeded—but simultaneously encrypted computers globally, causing substantial economic damage to multinational businesses such as Maersk and FedEx.34

**Collateral damage** and **unintended consequences** are **serious issues** for NATO. The alliance takes pride in its adherence to the principles laid out in international law, such as proportionality and discrimination, as former NATO Deputy Assistant Secretary-General Jamie Shea has emphasized.35 Thus, disruptions of servers with huge negative implications for civilians, or the use of generic cyber tools that risk spreading their effects far and wide, are most likely **not going to be considered** for use in NATO operations. Indeed, one of the main challenges to US efforts to disrupt servers in working against ISIS was finding ways to ensure that civilians were not hit by their cyber effects.36

Another aspect of the difficulty of assessing the cyber effect relates to adversaries' cyber defence efforts. For the more sophisticated players in cyberspace, cyber defence has developed into more than simply patching, clearing and updating systems. Cyber defence is also increasingly about following an intruder's activity in one's own network and creating ‘honeypots’ or ‘honeynets’; or about following data traffic back to the intruder's network. In short, cyber defence is also about deception and active defence.37 This approach to cyber defence offers valuable insights into the intruder's techniques and strategies; but the mere knowledge that deception is becoming a predominant defensive strategy also introduces doubts into the intruder's assessment of possible effects.

Consequently, as Russia is considered a peer competitor with considerable cyber-defensive capacities, one informant expressed **scepticism** about the extent to which smaller member states are **confident** in their ability to deliver a cyber effect when it is requested by NATO.38 This is especially the case if operational success depends on a **specific effect**. Even if a state has developed the appropriate exploit, it must also be able to verify that the effect is achieved and ensure that the effect is contained to minimize collateral damage. And even if a state is confident about its current ability to contain and verify an effect, it must also be confident that it can deliver, verify and contain the effect at the specific time in the future when CYOC requests it.

The process of integration is **further complicated** by the fact that NATO must be willing to hand over to contributing states the responsibility for making battle damage assessments and collateral damage estimations. As the following subsection shows, states are generally **unwilling to share** classified information about exploits. Hence, the delegated NATO commander is **unlikely to receive** much useful information about how cyber effects are delivered before a decision about their deployment must be taken. As commanders would prefer to have control over the capabilities used, member-state cyber effects are likely choices of method only if alternative, conventional effects are unavailable.

The challenges associated with assessing cyber effects are naturally most significant in relation to those effects that enable other kinetic effects that are necessary to achieve operational success. For cyber effects that seek to maintain a persistent annoyance of Russian networks, these challenges are less of an issue. If the aim is to create confusion and drain resources by targeting networks and operations that are otherwise difficult and expensive to disrupt using conventional means, then cyber effects can support strategic goals without causing irreversible damage to civilians. As I will conclude at the end of this section, such a change demands an adaptation of the way in which CYOC operates.

**2NC --- Info-Sharing Fails**

**Even if the U.S. successfully shares OCOs, NATO can’t use them.**

**Black and Lynch 20** — James Black, Research Coordinator at RAND, MSc in International Security from Sciences Po, LSE in History from the University of Cambridge, and Alice Lynch, Former Defense and Security Analyst at RAND, M.A. in Applied Security Strategy from the University of Exeter, 2020 (“Cyber Threats to NATO from a Multi-Domain Perspective,” *CCDCOE*, Available Online at https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030\_Horizon-Scanning-and-Analysis.pdf)

C. Capability and Force Development Priorities **Assuming NATO can overcome** conceptual and policy hurdles, **significant effort** will still be required to develop the **necessary forces** and **capabilities** across all domains, but perhaps especially for cyberspace.

Operationalising MDO demands a ‘**calibrated force posture’** with multi-domain formations **strategically positioned**, held at **readiness** and able to deploy over **large distances**, **trained** and **equipped** to operate across multiple contested domains (Grispen-Gelens, 2020). The vision is for different sensors and shooters to share and fuse data, build a common operating picture, inform rapid decision-making and deliver effects at a time and place of the commander’s choosing and to do so agnostic of domains, nation, service or platform (Niewood, Grant & Lewis, 2019). Forces must operate at pace and against an adversary contesting all domains. This tempo necessitates moving beyond NATO’s past focus on synchronisation of pre-planned effects in individual domains towards more agile targeting and more resilience against hostile attempts at ‘disorganisation’ or ‘systems attack’ (Thomas, 2019; Engstrom, 2018).

Linking all this together demands **novel approaches** to C4ISR, as reflected in investments in JADC2 (Harrigian, 2020). This US initiative leverages advances in information and communication technologies such as mesh networks, cloud and edge computing, open architectures, data analytics, AI and machine learning, autonomy and automation, software-defined systems, robotics, satellite communications and sophisticated cyber and EMS capabilities (Hitchens, 2019). Future JADC2 networks must be secure, robust, resilient, agile and more decentralised, with enough bandwidth to share data in a timely and secure manner despite cyber attacks, jamming, spoofing or physical destruction of communication nodes (Goldfein, 2017). Trust is also **essential**, handling data from different sources and at multiple security levels without making controls so arduous that Reliance on connectivity makes cyberspace, space and the EMS the ‘centre of gravity’ for MDO (Hess et al., 2019). JADC2 introduces **obvious challenges** from a cyber threat perspective, both in terms of the attack surface for different threat vectors and the cascading effects from hostile cyber activity—though, of course, existing centralised C2 hubs also have their own vulnerabilities to cyber or physical attack (Hess et al., 2019). Improved cyber capabilities are not only needed to **secure** and **enable** operations in **other domains** (Reilly, 2020). Investments by Russia and China to contest cyberspace and the EMS may also **limit the ability** of NATO commanders to employ **offensive cyber capabilities** at a time and place that will ‘converge’ with effects through other domains. Securing networks against disruption is critical at the operational and strategic levels given requirements for reach-back to headquarters, especially constraining organisations responsible for delivering offensive cyber effects, since these are likely to be physically located in the homeland (Watling & Roper, 2019; Nettis, 2020).

**OCO cooperation can’t solve the aff.**

**Jacobsen 21** — Jeppe T. Jacobsen, Visiting Scholar at New York University, former Cyber Coordinator at the Ministry of Foreign Affairs of Denmark, Ph.D. candidate at the Danish Institute for International Studies and the Center for War Studies at the University of Southern Denmark, M.A. in International Politics from the University of London, M.A. in Political Science from the University of Aarhus, 2021 (“Cyber offense in NATO: challenges and opportunities,” *International Affairs,* May, Available Online at <https://academic.oup.com/ia/article/97/3/703/6205395?login=true>)

While NATO and its member states adapted to the new security environment after the end of the Cold War by scaling down the military investments and presence in eastern Europe and by focusing more on crisis management,53 much of the Cold War deterrence language returned when the Russian–Ukrainian conflict broke out in 2014.54 What needs to be deterred today, much of the literature agrees, is not only a full-scale military invasion but to a larger extent the use and support of pro-Russian militant separatists who are willing to apply insurgency tactics in NATO's post-Soviet member states.55 As a result, the allies' military investments have been increasing again,56 a number of initiatives such as the Enhanced Forward Presence in the Baltic States and Poland have been introduced,57 and the discussions—and disagreements—on the nuclear deterrence (of non-nuclear threats) have re-emerged.58 Such responses are often presented as a renewed attempt by NATO to reassert its deterrence and assurance posture by signalling strength, preparedness and willingness to punish ‘bad’ behaviour.59

At first sight, the introduction of CYOC seems to add to these deterrence efforts. NATO added an offensive cyber option to reinforce its ability to impose costs sufficient to dissuade adversaries from acting aggressively. On closer examination, however, it is not self-evident that requesting member states' delivery of offensive cyber effects in NATO operations constitutes a **necessary** or even a **substantial addition** to credibly signalling the ability and willingness to punish an adversary. NATO's conventional capabilities are clearly already far superior to Russia's—with or without fully integrated cyber effects. Thus, a deterrence failure, resulting for example in a scenario in one of the Baltic states similar to that which occurred in eastern Ukraine, will **not be the result** of NATO's lack of available cyber tools in its military toolbox; rather, if the Russian leadership were to consider it in its interest to pursue such a scenario, it would mean that Russia's decision-makers did not believe in the credibility of NATO's article 5 or in NATO's ability to mobilize its forces. The capacity to integrate cyber effects would do **nothing to change** that.

Furthermore, if the establishment of CYOC is an attempt to signal defensive strength and unity in cyberspace, it remains **difficult to imagine** that such signalling would **dissuade adversaries** from trying to penetrate NATO and allied systems. CYOC does not change the fact that NATO is **not tasked** to govern and secure national IT systems. In an operational setting, states might connect to each other through so-called federated mission networking;60 but there is no tradition of ceding control of the deployed national networks to NATO during military operations. Hence, CYOC can only realistically seek to become a hub for cyber-threat information-sharing and to support states' coordination and synchronization of various national responses to these threats. In other words, CYOC is **unlikely** to become an active defender in cyberspace that causes doubt in the adversary's evaluation of its own cyber capabilities. This also means that even if CYOC's coordination and information-sharing efforts manage to contribute to the denial of intrusions into allied systems, an adversary's military is unlikely to be deterred from trying to hack these systems. In fact, actively articulating that CYOC is supposed to deter (through denial) a perceived adversary such as Russia from hacking NATO and allied operational systems creates an incentive to do just that and thereby show that the alliance is incapable of doing what it says it seeks to do.

**1NC --- Squo Solves**

**Maintaining OCO secrecy sufficiently solves the 1AC.**

**Lewis 15** — James Lewis, Senior Vice President and Director of the Strategic Technologies Program at the Center for Strategic and International Studies, former Senior Advisor to UN Groups of Governmental Experts on Information Security, PhD from the University of Chicago, 2015 (“The Role of Offensive Cyber Operations in NATO’s Collective Defense,” *The Tallinn Papers,* Available Online at <https://ccdcoe.org/uploads/2018/10/TP_08_2015_0.pdf>)

It could be argued, given NATO’s defensive orientation ( pace Russian fears of diabolic plots), that a **purely defensive** and **technical focus** for cyber operations is appropriate. The question, however, is whether NATO can field a credible military force without some public linkage to an offensive cyber capability.

Here again, the **nuclear precedent** offers some suggestions for a way forward. In the NATO phonetic alphabet, “whiskey” (“W”) and “romeo” (“R”) were used by NATO’s command structure in conflict to “warn” capitals that with a deteriorating situation on the ground it would be sending a request to release nuclear weapons for NATO use. Romeo was the actual request for release of nuclear weapons to NATO control. This terminology prepared nuclear capitals to make the decision on release.

Just as nuclear weapons remain under national control but senior NATO commanders can request their release, the US and UK could retain control of offensive cyber capabilities but be prepared to make them available to NATO commanders upon request. In practice, national teams could be assigned to support NATO commanders in theatre or could carry out some operations against targets selected by NATO commanders form their national duty station.

**Case-turn --- Info-sharing Bad: Offense**

**1NC --- Russia Turn**

**OCO sharing OR a NATO posture shift causes Russia to freak-out and undermines strategic stability.**

**Lewis 15** — James Lewis, Senior Vice President and Director of the Strategic Technologies Program at the Center for Strategic and International Studies, former Senior Advisor to UN Groups of Governmental Experts on Information Security, PhD from the University of Chicago, 2015 (“The Role of Offensive Cyber Operations in NATO’s Collective Defense,” *The Tallinn Papers,* Available Online at <https://ccdcoe.org/uploads/2018/10/TP_08_2015_0.pdf>)

Dissimulation is an essential part of hybrid warfare, and Europe and the US face a propaganda barrage that is much more sophisticated than the clumsy Soviet efforts of the Cold War. Despite this clumsiness, a good portion of the Western public has found it persuasive. Similarly, those critical of NATO will find new complaints about aggression and militarisation credible. Russia has **already complained** that NATO’s **defensive cyber doctrine** is **destabilising warmongering** and part of a larger conspiracy to **advance western hegemony**.11 The Snowden revelations have lent a powerful impetus to Russian propaganda.

Behind the rhetoric lies both a desire to conceal their own use of cyber operations and a **real fear** that Russia’s decline leaves it **vulnerable** to new military technologies. The intent is to hamper and complicate any Western response to Russian efforts to regain control in Crimea and the “near abroad”. The Russian position is that NATO’s new cyber doctrine is **destabilising** as it threatens to use conventional or even **nuclear responses** (in the Russian description of the new policy towards low-level cyber attacks).

**Any announcement** by NATO relating to **offensive cyber capabilities** would be greeted with **alarm** and **vitriol** in Moscow. However, the effect on stability would likely be less pronounced. NATO-Russia relations are already in steep decline. It is possible that any NATO announcement would accelerate this, but it is also possible that Russia could recalculate the risk of further adventures if it were faced with a stronger defence. In terms of opponent attitudes, there is probably little effect. Russia, along with NATO’s other potential military opponents, is likely to **overestimate both capabilities** and coordination among NATO member states and **underestimate NATO’s will** to defend. This is an unhappy combination as it makes aggression against NATO seem **less risky**.

NATO’s decision on how cyber attacks could trigger Article 5, while greeted with complaints, had a stabilising effect. It made clear to potential opponents that cyber attacks are not risk-free. Similarly, a clear enunciation of how NATO would use offensive cyber capabilities as part of any defensive operation would also change opponents’ risk calculations in ways that would force them to consider how offensive actions, even if intended to be covert, are not free of risk or cost.

The Cyber Club

Some level of cyber capability is being acquired by all advanced militaries, and perhaps a dozen countries can be identified from public sources as procuring offensive cyber capabilities. These countries include several NATO members. As with nuclear weapons, the capability to undertake offensive cyber operations is a club within a club in NATO, with largely the same membership – the US, the UK and France. Germany’s armed forces may also be developing offensive cyber capabilities.12 The well-developed procedures for release and for integration into NATO planning created for nuclear weapons do not exist for cyber attack, although it is currently far more likely that any NATO military operation will have a cyber component, while the use of nuclear weapons is almost unthinkable.

The US and the UK both possess elite cyber capabilities. They also have a close partnership in cyber espionage. This partnership is centred on a relationship between the US National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ), both of which are intelligence agencies with a long history of supporting military operations. US military cyber operations are the responsibility of U.S. Cyber Command, whose commander is also the head of the NSA. Cyber operations blur the line between intelligence and military activities. The fact, however, that these are intelligence agencies has a created a certain reticence regarding the sharing of information on capabilities and plans, which complicates the integration of offensive cyber into NATO planning and doctrine.

Offensive cyber capabilities are still **too new**, with too many **unknown risks** that hold potentially **profound political consequences**. US policy is that only the President can approve a cyber operation likely to result in “significant consequences” that could produce loss of life or a damaging reaction, although the Secretary of Defense or the head of U.S. Cyber Command can take independent action in an emergency. US policy restricts independent action by tactical and operational commanders for this reason. A local commander may not know all the trade-offs or the risks that using a cyber attack could entail. That said, all of these problems are manageable with some decision-making model based on the precedent of the warning and request system used for nuclear weapons release.13

Until there are better predictive tools and judgments about risk and consequences, offensive cyber operations will require a **politically sensitive decision** as to when the benefit of an attack outweighs the **political risk**. Additional coordination mechanisms would be needed to decide when the benefits of an attack outweigh the risk of a loss of intelligence capabilities, or when a target justifies expending a weapon that might never work again. The inability to predict **collateral damage** and **uncertainty** over political effect encourage caution in the use of offensive cyber operations, but that is not the same as advertising possession of the capability.

**That causes the Ukraine war to draw in the U.S. and NATO --- results in great power cyber war.**

**Healey 22** — Jason Healey, Senior Research Scholar at Columbia University’s School for International and Public Affairs specializing in cyber conflict, Adjunct Professor of International and Public Affairs at Columbia University, 2022 (“Preventing Cyber Escalation in Ukraine and After,” *War on the Rocks,* March 9th, Available Online at <https://warontherocks.com/2022/03/preventing-cyber-escalation-in-ukraine-and-after/>, Accessed on 06-19-2022)

With the world worried about the risk of nuclear escalation between Russia and the West, now might also be a good time to worry about the risk of cyber conflict **escalating to war** as well.

In recent years, a number of scholars and practitioners have argued that cyber conflict should be seen as an intelligence battle or pressure-release valve rather than something that could escalate into actual conflict or war. Indeed, to date, no state has responded to a rival’s cyber attack with a kinetic reprisal. But that does not mean it will not happen now. As **geopolitical circumstances** change, the **escalatory potential** of cyber capabilities is **likely to change** as well.

Moscow, for example, might respond to Western sanctions with **intensified cyber attacks**. Or Western leaders, recognizing that no-fly zones are too risky, might approve cyber interventions to prevent civilian massacres instead. In either case, they could well assume this escalation would not meet with a direct military response. And in either case, they could be wrong.

Minimizing this risk requires both recognizing and respecting the latent but **strong escalatory potential** of cyber attacks. It also involves delving deeper into the psychology of the situation, as escalation will be driven as much by the perceptions and misperceptions of the participants as any technical aspects of cyber warfare.

The Great News

So far, cyber attacks have not proven particularly escalatory or effective on the battlefield. Even the most provocative incidents that came closest to resembling kinetic attacks, such as Stuxnet or the ransomware attack on Colonial Pipeline, have not led to particularly menacing crises, much less war. If anything, over the past decade cyber capabilities have helped de-escalate crises, acting as a “non-kinetic option for leaders who feel pressure to act in a crisis, but who are wary of using force.”

The U.S. conflict with Iran offers a clear example. After Iran attacked several oil tankers and downed a U.S. drone in June 2019, President Donald Trump canceled punitive U.S. airstrikes at the last minute out of concern that the casualties could prompt further escalation. However, he allowed nonlethal cyber disruption of Iranian computer systems, anticipating Iran would not respond violently. Indeed, Iran’s supreme leader “blocked any large, direct retaliation,” limiting the country’s response to the cyber realm.

Scholars have offered different explanations for the non-escalatory nature of these attacks. Cyber effects are “uncertain and often relatively limited” and “offer great powers escalatory offramps [and] signaling mechanisms” to de-escalate. In the “cyber strategic competitive space short of armed conflict,” states have “tacitly agreed on lower and upper bounds” and accordingly “have mutual interests in avoiding escalation to violent conflict.” Cyber conflict also has characteristics of an intelligence, not military, contest.

The Bad News

Cyber conflicts have flourished during a relatively peaceful time when major powers generally did not invade one another. Perhaps cyber capabilities acted as a pressure release simply because in the post-Cold War period states usually wanted to de-escalate and the geopolitical stakes were not that high anyway? What happens now when Moscow feels that the stakes are **much higher**?

Already there have been warnings that if Russian forces face **further setbacks**, Putin may **lash out** in **desperate** and ultimately **self-harming ways**. A major cyber power has never faced such a crisis before, so past performance may be a **limited indicator** of **future potential**. In fact, the very perception that cyber attacks are non-escalatory might itself **increase the risk** of unintended escalation.

There are multiple ways cyber conflict around the Ukrainian invasion might escalate into a **direct conflict** between **Russia and NATO**, possibly as a result of either side’s offensives.

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.

Second, Western offensive cyber operations might **spark war**. U.S. cyber espionage and operations against Putin, his cronies, or Russia’s military forces will appear far more ominous to Putin if he believes they are aimed at regime change. Could Putin turn the other cheek if the United States were to electronically raid the cryptocurrency wallets of Russia’s sanctions-avoiding kleptocrats? He might feel the need to escalate his own cyber operations as part of his own version of defending forward.

Escalation could happen on the battlefield as well. According to the New York Times, teams from U.S. Cyber Command are “in place to interfere with Russia’s digital attacks and communications.” Other teams are almost certainly collecting digital intelligence on the location and intent of Russian combat forces. The United States is sharing such intelligence with the Ukrainians but apparently not yet providing any real-time targeting. That may change soon, as the United States seeks to alleviate intensifying attacks on civilians. And with his KGB-bred paranoia, Putin might already see the presence of U.S. defensive and intelligence teams operating on or against Russian military networks as evidence of direct U.S. involvement in the war. Confirming his apparent belief that Ukraine is just a NATO puppet, this might force a response, either inside or outside of cyberspace.

Further, if Western governments have infiltrated Russia’s operational military networks, they may feel pressure to disrupt those networks to prevent civilian massacres. Because cyber capabilities are billed as non-lethal, reversible, and non-escalatory, tub-thumping newspapers may push decision-makers to take shots they **might not otherwise**: “We can’t create a no-fly zone but can use cyber capabilities to prevent civilian harm.” Some well-meaning national leaders may succumb to this pressure, potentially causing a larger conflict.

**Goes nuclear.**

**Lonergan and Yarhi-Milo 22** — Erica Lonergan, Assistant Professor in the Army Cyber Institute at the United States Military Academy at West Point, Research Scholar in the Saltzman Institute of War and Peace Studies at Columbia University, PhD in Political Science from Columbia University, and Keren Yarhi-Milo, Arnold A. Saltzman Professor of War and Peace Studies in the Political Science Department and the School of International and Public Affairs at Columbia University, former Associate Professor of Politics and International Affairs at Princeton University, PhD and M.A. from the University of Pennsylvania, 2022 (“Cyber Signaling and Nuclear Deterrence: Implications for the Ukraine Crisis,” *War on the Rocks,* Available Online at https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/)

However, conducting cyber operations to signal deterrence would, paradoxically, **increase risks of escalation**. This risk is not just hypothetical, especially in light of Russia’s updated declaratory policy for the **first use of nuclear weapons**, which may include responses to cyber attacks. Russia has **reinforced this message** during the war in Ukraine. In early March, a hacking group affiliated with Anonymous claimed that it had shut down the control center of Russia’s space agency. While denying that the attack took place, Russia nevertheless warned that a cyber attack against its satellites would be a justification for war.

The Biden administration should clearly communicate that cyber operations for nuclear signaling are out of bounds, just as it declared restraint in other aspects of this conflict, like the deployment of American troops to Ukraine.

How Cyberspace Is Creating Nuclear Risks

Policymakers and academics are attuned to the cyber risks to nuclear **command and control**. The practitioner community has largely focused on U.S. vulnerabilities and how to mitigate them. Scholars, in turn, worry about how cyber operations could have **unintended escalatory consequences**. But less attention has been paid to another likely scenario: the use of cyber operations for signaling purposes (operations with visible effects that aim to convey a message to another state) in a nuclear context. The ambiguity of cyber operations can sometimes be useful for signaling — but the same ambiguity can be **dangerous** during a **nuclear crisis**. The problem is that civilian leaders in particular, distinct from the military, are inclined to see cyber attacks as effective signaling tools.

Cyber operations could have **nuclear implications**, especially because modern nuclear command and control systems, like those in Russia and the United States, are becoming **increasingly dependent** on digital infrastructure. Nuclear command, control, and communications systems, which include early warning, information collection, and communications capabilities, alert decision-makers to impending nuclear strikes and also enable leaders to control decisions about nuclear use (or non-use). But their digital dependencies are creating opportunities for exploitation using cyber means. In a 2020 report, the Nuclear Threat Initiative found that “almost 9 out of 10 planned nuclear modernization programs involve at least some new digital components or upgrades.”

Vulnerabilities inherent in the digital infrastructure that undergird modern nuclear systems provide opportunities for actors to engage in cyber espionage — gaining access to a network or system to steal information — or even conduct cyber attacks. Hypothetically, a cyber power like Russia could conduct a cyber attack against a U.S. early warning satellite to degrade its functionality. This has become an urgent concern for practitioners. U.S. Strategic Command, for instance, is currently working to “operationally harden NC3 systems against cyber threats.” Congress has also gotten involved, requiring the Defense Department to evaluate the cybersecurity of major weapon systems. And the Government Accountability Office has published multiple reports decrying the state of cybersecurity and scope of vulnerabilities of weapon systems, including elements of the nuclear triad.

From an academic perspective, scholars have investigated how cyber operations targeting nuclear systems could **exacerbate escalation risks**. Focusing on nuclear forces, early research, such as work by Martin Libicki, was skeptical of the dangers posed by cyber operations. Nuclear forces were seen as being largely immune from digital attacks because they were “air gapped,” meaning that they were separated from information technology systems.

However, as nuclear systems have become increasingly intertwined with the digital environment — not to mention the dual-use nature of many elements of nuclear command, control, and communications systems (like early warning or position, navigation, and timing satellites) — the protection offered by being segregated from the internet is **less robust**. Jacquelyn Schneider, Benjamin Schechter, and Rachael Schaffer, for instance, ran a series of wargames demonstrating that decision-makers in hypothetical crises are likely to use their cyber exploits against an adversary’s nuclear systems. They found that this could have negative effects on states’ respective nuclear strategies, especially decisions to pre-delegate **nuclear launch authority** or **automate nuclear responses**. Erik Gartzke and Jon Lindsay argue that the clandestine nature of cyber operations means that one state could secretly gain access to an adversary’s nuclear command, control, and communications systems, giving the former an information advantage or even creating an incentive for the latter to use its nuclear weapons out of the fear that it may lose them. James Acton notes that the difficulties of distinguishing between cyber espionage and attack could lead a state to misperceive the intent behind a cyber operation, generating a similar “**use it or lose it**” calculus.

**2NC --- Russia Turn**

**Even if the status quo doesn’t escalate, the plan guarantees massive preemptive cyberwar in the future.**

**Healey 22** — Jason Healey, Senior Research Scholar at Columbia University’s School for International and Public Affairs specializing in cyber conflict, Adjunct Professor of International and Public Affairs at Columbia University, 2022 (“Preventing Cyber Escalation in Ukraine and After,” *War on the Rocks,* March 9th, Available Online at <https://warontherocks.com/2022/03/preventing-cyber-escalation-in-ukraine-and-after/>, Accessed on 06-19-2022)

Future Risks

Even if Russia and the West avoid direct conflict this time, they might not be so lucky the next. As relations worsen, future disruption of critical Western infrastructure by Russian intelligence, such as the NotPetya and Olympic Destroyer attacks, are less likely to be viewed as mere crimes. Repeated crises bordering on war may **further erode** the **tacit agreements** and **relative restraint** of quieter times. After repeated iterations of intensifying cyber operations, both Russia and the West may feel their backs to the wall with few options left other than **military force** when the next crisis — physical or cyber — emerges. Under extreme conditions, some of the same characteristics that lead cyber capabilities to be a pressure release might have the opposite effect, a mechanism that Bob Jervis and I have described as the Escalation Inversion.

If Putin believes a direct conflict with NATO is **likely** and expects its adversaries to **take measures to reduce vulnerabilities**, he could conclude that the best possibility for success is to launch a **massive preemptive cyber attack**. Since the U.S. military may seem otherwise unbeatable, this may lead Russia to “compensate with audacity in order to redress the balance.” The more the United States **brags about its overwhelming offensive cyber advantage**, but frets over weak defenses, the more any adversary might **feel the need to target** the United States as early and as hard as possible.

If Russia fears war with the United States may happen on Saturday, it might feel the need to get in its cyber punches on Friday. If the United States thinks the same, it may need to start on Thursday. Cyber capabilities may be to **World War III** as mobilization timelines were to World War I.

Since a cyber sucker punch may also seem less escalatory, adversaries could be **tempted to take risks** they would not otherwise. In this situation, the sense that cyber is a pressure-release valve becomes **positively dangerous**: If the system is seen to be stable, then there is less reason to act with restraint, thereby making it less stable. Fortunately, the good news is leading U.S. policymakers appear attuned to this risk.

**The plan violates intelligence norms — causes adversaries to think they’re being attacked.**

**Jacobsen 21** — Jeppe T. Jacobsen, Visiting Scholar at New York University, former Cyber Coordinator at the Ministry of Foreign Affairs of Denmark, Ph.D. candidate at the Danish Institute for International Studies and the Center for War Studies at the University of Southern Denmark, M.A. in International Politics from the University of London, M.A. in Political Science from the University of Aarhus, 2021 (“Cyber offense in NATO: challenges and opportunities,” *International Affairs,* May, Available Online at <https://academic.oup.com/ia/article/97/3/703/6205395?login=true>)

Escalation and the dominant intelligence norm

The large overlap between intelligence collection and attack in cyberspace makes it difficult to send **clear signals** to adversaries, in terms of either capabilities or intentions. When a foreign entity is moving around in a network, is it then about to start a **military operation?** Is the activity part of a reconnaissance mission? Is it political or economic espionage? Is it active defence? The difficulty of answering these questions has created much nervousness among cyber-conflict experts. Ben Buchanan, for example, has shown how defensive hacking or intelligence-gathering in cyberspace is **easily misinterpreted** as aggressive behaviour.66 Why, then, have we not experienced serious **misinterpretation** and **escalation** in cyberspace?

One way to explain this is through the existence and dominance of a largely unspoken but **widely accepted** norm. For decades, the **predominant actors** in cyberspace have been **intelligence agencies**; and the norms that characterize interactions between intelligence agencies are not primarily concerned with military concepts such as conflict escalation and deterrence.67 In the world of intelligence agencies, success is not about keeping a distance between oneself and the adversary by signalling one's intentions and capabilities. It is about being able to outmanoeuvre adversaries in a space of constant contact.68 There are always risks, and the work usually takes place in legal grey zones where a clear distinction between war and peace is not the guiding principle. This is an arena where the opportunity to annoy, cheat and delay opponents is taken when it arises. In short, espionage and counter-espionage **do not fit well with** the thorough military operational planning that characterizes **NATO operations**. Intelligence operations, on the other hand, fit perfectly with a dynamic cyberspace where anonymity is easy to achieve and uncertainty a constant condition.69 The states that embrace cyberspace as a domain where the intelligence norm dominates are able to use a broader array of tools to pursue or respond to various foreign political objectives than only those that relate to military operations.

In its 2018 ‘vision’, the US Cyber Command **built implicitly** on the dominant **intelligence norm**. Here, the objective is to become more agile and act as close to the adversary as possible (‘defend forward’).70 The United States considers ‘constant contact’ and ‘persistent engagement’ as the necessary guiding principles to achieve superiority in cyberspace and to take full advantage of the broader potential for pursuing its political objectives through cyberspace. During the 2018 US midterm elections, for example, the US Cyber Command worked closely with the NSA to disrupt servers operated by the Russian Internet Research Agency aiming to spread fake news and stir up tension in the United States.71 More recently, the US Cyber Command responded with various cyber effects against Iran after the Iranian Revolutionary Guards apparently placed mines on ships in the Strait of Hormuz.72 These practices illustrate that, for the United States, cyber effects provide political options when one does not want to escalate existing tensions into military confrontation. Defensive coordination between allies through CYOC supports such defensive use of cyber effects, increasing the possibility that US Cyber Command will be allowed to ‘defend forward’ and work persistently through allied networks.73 A more cyber-active NATO, however, risks being counterproductive to the ambition to ‘defend forward’ through allied networks.

Unintended conflict escalation from ongoing cyber activity is mainly a risk if military analysts—in a strategic environment with heightened attention to military confrontation—**ignore the dominant intelligence norm**. If that happens, it becomes more likely that ‘persistent engagement’ and active cyber defence will be misinterpreted as **military preparation**, **armament** or the **initial phase of an attack**. **If NATO,** an organization that has publicly returned to its original raison d'être of deterrence and collective defence, becomes the entity that **coordinates cyber effects** below the threshold of armed conflict, then the likelihood increases that Russia misinterprets these effects as **escalatory** and **acts accordingly**. In other words, a **more active NATO** in the current strategic environment **increases the risk** that the existing intelligence norm will be **undermined** and replaced by a **more militarized norm**.

**Broader cyberwar is likely.**

**Smeets 19** — Max Smeets, Senior Researcher at the Center for Security Studies, 2019 (“Cyber Command’s Strategy Risks Friction With Allies,” *Lawfare,* May 28th, Available Online at https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies)

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

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

**2NC --- Terminal Impact**

**Putin won’t back down — guarantees nuclear escalation.**

**Litwak 22** — Robert Litwak, Senior Vice President and Director of International Security Studies at the Wilson Center, former Adjunct Professor in the Security Studies Program at Georgetown University, PhD in International Relations from the London School of Economics, 2022 (“Russia’s Nuclear Threats Recast Cold War Dangers: The “Delicate Balance of Terror” Revisited,” *Wilson Center,* May 3rd, Available Online https://www.wilsoncenter.org/article/russias-nuclear-threats-recast-cold-war-dangers-delicate-balance-terror-revisited)

Since the Cuban Missile Crisis, assured retaliation—eliminating incentives for a surprise first strike—has been the sine qua non of strategic stability. The risk for crisis stability is that arms race instability could revive those incentives, making the deterrent relationships more “delicate.” With the advent of new technologies, **escalation during a crisis** could occur in a non-traditional domain—cyber or space—and could **misleadingly be viewed** as non-escalatory because it would be non-kinetic. But an inadvertent **escalatory spiral** could be set off by a Russian cyberattack to interfere with U.S. communications with its nuclear systems or an attack on reconnaissance satellites to blind the United States. Hints of that potentiality are already manifest: Russia conducted an anti-satellite missile test last November and, during the Ukraine war, has carried out extensive cyberattacks, often in coordination with its battlefield operations.

In the Ukraine war, as during the Cuban Missile Crisis, inadvertent escalation remains a **major risk.** Putin is a risk-taker (whose agents used a military-grade nerve agent in a 2018 assassination attempt on a Russian military defector in Britain) and he is **prone to miscalculation**. His assumptions going in to Ukraine—that the conflict would be short and decisive, that the Zelensky government would fold quickly, and that the West would be feckless in its disunity—were all miscalculations that ironically led many Western officials and analysts to conclude that he would threaten but not invade.

Given Putin’s propensity for risk-taking and miscalculation, the Biden administration is exploring scenarios in which Russian military “setbacks” and “desperation” (as CIA Director Burns’ warned) lead to the use of **chemical** or **nuclear weapons**. Under what U.S. officials describe as Russia’s “escalate-to-deescalate” strategy, Putin might **double down** in the face of adversity by employing a single weapon for its demonstration effect—to shock the Ukrainian and Western leaderships into acceding to terms favorable to the Kremlin. While the Biden administration has not laid down an explicit deterrent marker specifying the U.S. response, a senior official warned that any Russian use of nuclear weapons would mean “**all bets are off**”—a tacit signal that such a violation of the nuclear taboo could move the United States and NATO to become **directly involved** in the war. The Biden administration could strengthen that deterrent message, as Stanford Professor of Political Science Scott Sagan has recommended, by communicating directly to the Russian military that an order from Putin to use a nuclear weapon in Ukraine would be illegal, a violation of the Geneva Conventions, and should not be obeyed.

The challenges of crisis stability to prevent escalation are **immediate** and **urgent** even as the near-term prospects for a resolution of the Ukraine war appear remote. The U.S. policy focus should be on preventing inadvertent escalation. Key to that imperative is maintaining an open line of communications with Russia’s military leadership. As a disquieting indicator of the virulent relations between Moscow and Washington, Russia has rebuffed calls from Defense Secretary Lloyd Austin and Gen. Mark A. Milley, the chairman of the Joint Chiefs of Staff, to their counterparts.

**1NC --- Deconfliction Turn**

**The plan causes cyber deconfliction — that makes effective OCOs impossible AND ruins NATO cohesion — turns both advantages.**

**Jacobsen 21** — Jeppe T. Jacobsen, Visiting Scholar at New York University, former Cyber Coordinator at the Ministry of Foreign Affairs of Denmark, Ph.D. candidate at the Danish Institute for International Studies and the Center for War Studies at the University of Southern Denmark, M.A. in International Politics from the University of London, M.A. in Political Science from the University of Aarhus, 2021 (“Cyber offense in NATO: challenges and opportunities,” *International Affairs,* May, Available Online at <https://academic.oup.com/ia/article/97/3/703/6205395?login=true>)

Confliction—the issue of secrecy

The third challenge to the integration of cyber effects in NATO operations relates to a well-known military concept, deconfliction. The coordination by allies and military units of their efforts to avoid confliction, between for example an air operation and a special forces operation in the same area, is a central element in every military campaign. Deconfliction is all about openness and communication between allied partners. But in cyberspace, deconfliction comes with **several difficulties**. At the core of these difficulties is the fact that the tools and techniques that produce cyber effects—which are often also used and heavily depended on for intelligence collection—are **developed in secret** and **must stay secret** until the effect is achieved. If the IT vulnerabilities and exploits are known, vendors or adversaries can fix or replace the software and thereby render the effect **impossible to achieve**.39 In an alliance not known for sufficient mutual trust among members to share intelligence,40 there is **little indication** that allies will become more open about the cyber tools and techniques they currently have at their disposal. The request-based model is the result of that lack of trust. And the unwillingness to share cyber intelligence **seriously challenges** NATO's ambition to use CYOC to facilitate **information-sharing** to increase situational awareness and thereby achieve the ‘**cyber readiness’** and ‘**cyber resiliency’** that NATO Deputy Secretary-General Mircea Geoană hopes to attain.41

Furthermore, **lack of coordination** and discussion about the use of military cyber capabilities, both internally in each state and among allies, can have **negative implications** for **intelligence activities** and **general network security**. A conventional military decision to deliver cyber effects is rarely concerned with maintaining access and staying secret after an effect is achieved. Even though it is customary to try to obscure the vulnerabilities that are being exploited, it is difficult to ensure that those operating the targeted system or third-party network analysts do not identify and fix the vulnerabilities in, for example, commercial products used all over the world. Thus, military plans to engage other state entities need to weigh the benefit of delivering cyber effects against the **risk of losing intelligence capacity**, as well as the risk that other actors (allies, corporations, adversaries, criminals, etc.) will use the **same exploits** against oneself. In other words, there is a **conflict of interest** between attack, intelligence collection and internal defence in **each NATO member state**.42 The desire of the US Cyber Command to become more independent from the National Security Agency (NSA) is precisely an attempt to gain a stronger voice when the US government assesses whether a vulnerability should be disclosed to vendors, retained for intelligence purposes or used to deliver ‘loud’ cyber effects.43

The risk of confliction among allies arises from the fact that a similar assessment procedure **does not exist** across NATO. As conversations with several national representatives at the CDC reveal, such a procedure is unlikely to be agreed upon owing to the different perspectives on offence, defence and espionage in cyberspace currently prevailing among member states.44 If the Netherlands, for example, offers to deliver a ‘loud’ cyber effect in a NATO operation, British or American intelligence operations could end up being disturbed because they rely on the same vulnerabilities which—when used in military operations—risk being exposed and subsequently fixed.45 When deploying ‘loud’ cyber effects, malicious actors such as criminals are also given the opportunity to identify and exploit the same vulnerabilities in unpatched systems in allied countries. The ransomware incidents known as WannaCry and NotPetya are examples of the damage that can emerge from government exploits becoming publicly available—even though the specific vulnerabilities were already patched by Microsoft and updates released to supported systems.46

In short, there is a dilemma both **internally**, between intelligence agencies and the military, and **externally, between allies**. While it is difficult to do much about the latter, the internal power dynamics in most states, with the intelligence agencies as the primary cyber actors, are likely to limit the willingness of most states to deliver military cyber effects—whether offensive or defensive—when CYOC makes requests. They also limit the willingness to share cyber threat information across the alliance through CYOC.

This section has pointed to three characteristics about cyberspace that limit the integration of cyber effects in NATO operations. In a complex and constantly changing cyberspace, it continues to be difficult to develop and maintain sophisticated exploits for targeted cyber effects. This is especially the case if the cyber effects are requested for a specific time and place in order to guarantee operational success, and if they simultaneously have to be verifiable and conform to international legal principles. Neither the member states, which face an internal dilemma between attack, intelligence collection and defence in cyberspace, nor the NATO commander, who will prefer to control the capabilities used, are likely to feel sufficiently confident about the targeted or highly integrated cyber effects to choose that option if other capabilities are available.

**2NC --- Deconfliction Turn**

**Info-sharing ruins any potential benefits of OCOs.**

**Black and Lynch 20** — James Black, Research Coordinator at RAND, MSc in International Security from Sciences Po, LSE in History from the University of Cambridge, and Alice Lynch, Former Defense and Security Analyst at RAND, M.A. in Applied Security Strategy from the University of Exeter, 2020 (“Cyber Threats to NATO from a Multi-Domain Perspective,” *CCDCOE*, Available Online at https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030\_Horizon-Scanning-and-Analysis.pdf)

Policy differences exacerbate conceptual ones. Allies differ in their **policy** and **legal constraints**, **strategic cultures**, **threat perception**, **resources**, **planning** and **budgetary cycles** and **forces** (Sondhaus, 2006). While solidarity ultimately remains NATO’s strongest asset, these differences create seams that **adversaries can exploit**. This is especially so with cyberspace, where there is more sensitivity and less commonality to emerging national approaches than in more established domains, and to MDO, which is inherently predicated on integration and interoperability (Sharpy, 2020).

**Information sharing** is **especially problematic** for the **cyber dimension** of MDO, with Allies reticent to share details of their capabilities across NATO given security concerns and political sensitivities. The issue of permissions is also a ‘**significant challenge** in the development of cyber capabilities’, especially where reconnaissance on Allied soil and networks is required to detect hostile cyber activity (Watling & Roper, 2019). Nations also have **differing policy**, **legal** and **ethical stances** on key technologies on which MDO relies. This includes the use of offensive cyber capabilities or basing of hypersonic missiles or longrange penetrating fires in Europe, which some fear could be destabilising and escalatory (Quintin & Vanholme, 2020). NATO similarly lacks a common approach to governance and use of AI, autonomy and automation, all envisaged as essential enablers for JADC2 (Williams, 2020). This affects the levels of autonomy (with the human in, on or out of the loop) used for sensor data fusion and decision-making, or to deliver effects using uncrewed platforms, automated cyber systems and human-machine teaming (Scharre, 2018).

In considering cooperation and burden-sharing, Allies face **several dilemmas** depending on their ambitions and resources for both cyberspace and MDO. The US must overcome domestic inter-service rivalries and decide how to integrate partners, including whether it can accept a multinational vision of MDO that is not imposed on smaller allies—or excludes them entirely, at NATO’s expense—but rather is genuinely collaborative (Watling & Roper, 2019). Larger European nations face the dilemma of whether to buy into a US-led architecture and system-of-systems with implications for freedom of action, data-sharing and procurement choices, or shoulder the costs of sovereign or multinational alternatives.11 They also face choices over how best to contribute to multinational MDO: whether to aspire to full-spectrum capabilities to allow sovereign action and offer redundancy to Allies’ capabilities or to specialise in certain domains (e.g. cyber) to offer niche capability and buy leverage with the US and NATO by making themselves indispensable. Smaller nations must decide how to influence larger Allies and NATO, and what to do if they lack cyber capabilities (or others deemed central to MDO, e.g. long-range fires) or their forces are too small to operate or gain MDO experience at echelons above brigade (Watling & Roper, 2019).

The economic fallout of COVID-19 also raises renewed questions about **affordability** and the extent to which Allies are **willing** and **able** to invest in new cyber capabilities—though some may see these as cost-efficient alternatives to land, air or maritime forces—and how they time investments in ambitious transformation programmes such as MDO (Clark, 2020). Timing presents both threats and opportunities from a cyber perspective. Rapid, hasty transformation risks undermining NATO cohesion and interoperability or creating vulnerabilities in JADC2 systems with immature cyber defences (Donaldson & Sciarini, 2019b). Conversely, overly cautious change risks ceding ground to adversaries such as Russia and China which are investing heavily in asymmetric means, including offensive cyber capabilities, to gain an information advantage over NATO (Kilcullen, 2020).

**NATO will spread info to the private sector — that causes OCOs to fail.**

**Black and Lynch 20** — James Black, Research Coordinator at RAND, MSc in International Security from Sciences Po, LSE in History from the University of Cambridge, and Alice Lynch, Former Defense and Security Analyst at RAND, M.A. in Applied Security Strategy from the University of Exeter, 2020 (“Cyber Threats to NATO from a Multi-Domain Perspective,” *CCDCOE*, Available Online at https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030\_Horizon-Scanning-and-Analysis.pdf)

Problematically, authorities associated with using cyber capabilities are typically held at the strategic and national level; how tactical or operational commanders might call upon cyber means as part of future MDO remains unclear (Nettis, 2020). Responsibilities for cyberspace also often fall at least partly to **civilian agencies**, adding the complexity of **cross-government cooperation**. The private sector’s role developing and applying technologies in the cyber domain (and, increasingly, space) also **necessitates that NATO work more closely with industry**, academia and others than for land, maritime or air operations (Ablon et al., 2019). This presents **operational**, **policy** and **legal difficulties** for C2, and cybersecurity challenges associated with reliance on industry-owned networks, though Allies continue to evolve novel mechanisms for partnering with industry to address cyber threats (Carr, 2016).

There is also the question of **tempo**: how to synchronise operations in cyberspace with the delivery of effects in other domains (Reilly, 2020). Though cyber attacks might initiate in a moment, the underlying tools and exploits may take **years to develop** and the lead times and scale of their eventual effect may be difficult to predict or measure given the difficulties with battle damage assessment in cyberspace or the EMS (Patrikarakos, 2017; US Joint Staff, 2019). Similarly, commanders may **lack awareness** or **understanding** of available cyber instruments and their limitations and effects compared to more familiar weapons in the physical domains, limiting inclusion in joint planning and decision-making (Carbonell, 2017).

**AT --- Ukraine Cyberwar Now**

**Russia cyber efforts are low-level currently, but the plan changes the calculus.**

**Kallberg 22** — Jan Kallberg, Assistant Professor at the United States Military Academy at West Point, Research Scientist at the Army Cyber Institute at West Point, PhD in Public Affairs and M.A. in Political Science from the University of Texas, LLM from Stockholm University, 2022 (“Ukraine: Russia will not waste offensive cyber weapons,” *The Cyberwire,* March 14th, Available Online at <https://thecyberwire.com/stories/75ca5313b59045ccbcbfc7d3b9e5d207/ukraine-russia-will-not-waste-offensive-cyber-weapons>)

When Russia’s strategic calculus would dictate major cyber attacks.

Russia will use advanced strategic cyber at **well-defined** critical junctures. For example, as a conflict in Europe unfolded and dragged in NATO, Russian forces would seek to delay the entry of major US forces through cyber attacks against railways, ports, and electric facilities along the route to the port of embarkation. If US forces can be delayed by one week, that is one week of a prolonged time window in Europe before the main US force arrived, and would enable the submarines of the Northern Fleet to be positioned in the Atlantic. Strategic cyber supports strategic intent and actions.

All cyber-attacks are not the same, and just because an attack originates from Russia doesn't mean it is directed by strategic intent. Naturally, the Russian regime would allow cyber vandalism and cybercrime against the West to run rampant, because these are ways of striking the adversary. But these low-end activities do not represent the Russian military complex’s cyber capabilities, nor do they reflect the Russian leadership’s strategic intent.

The recent cyberattacks in Ukraine have been **unsophisticated** and have had close to no **strategic impact**. The distributed denial-of-service (DDoS) cyber-attacks are **low-end efforts**, a nuisance that most corporations already have systems to mitigate. Such DDoS attacks will not bring down a country or force it to submit to foreign will. Such low-end attacks don’t represent advanced offensive cyber weapons: the DDoS attacks are limited impact cyber vandalism. Advanced offensive cyber weapons destroy, degrade, and disrupt systems, eradicate trust and pollute data integrity. DDoS and website defacements are not even close to this in their effects. By making DDoS attacks, whether it’s the state that carried them out or a group of college students in support of Kremlin policy, Russia has not shown the extent of its offensive cyber capability.

The invasion of Ukraine is not the major peer-to-peer conflict that is the central Russian concern. The Russians have tailored their advanced cyber capabilities to directly impact a more significant geopolitical conflict, one with NATO or China. Creating a national offensive cyber force is a decades-long investment in training, toolmaking, reconnaissance of possible avenues of approach, and detection of vulnerabilities. If Russia showcased its full range of advanced offensive cyber capabilities against Ukraine, the Russian tactics, techniques, and procedures (TTP) would be compromised. NATO and other neighboring nations, including China and Iran, would know the extent of Russian capabilities and have effective insight into Russia’s modus operandi.

From a Russian point of view, if a potential adversary **understood Russian offensive cyber operations’** tactics, techniques, and procedures, strategic surprise **would evaporate**, and the Russian cyber force would **lose the initiative** in a more strategically significant future conflict.

Understanding the Russian point of view is essential, because it is the Russians who conduct their offensive actions. This might sound like stating the obvious, but currently, the prevailing conventional wisdom is a Western think-tank-driven context, which in my opinion, is inaccurate. There is nothing for the Russians to strategically gain by unleashing their full advanced cyber arsenal against Ukraine or NATO at this juncture. In an open conflict between Russia and NATO the Russian calculation would be different and justify use of advanced cyber capabilities.

**Cyberwar is currently a last resort for Russia.**

**Kallberg 22** — Jan Kallberg, Assistant Professor at the United States Military Academy at West Point, Research Scientist at the Army Cyber Institute at West Point, PhD in Public Affairs and M.A. in Political Science from the University of Texas, LLM from Stockholm University, 2022 (“Ukraine: Russia will not waste offensive cyber weapons,” *The Cyberwire,* March 14th, Available Online at <https://thecyberwire.com/stories/75ca5313b59045ccbcbfc7d3b9e5d207/ukraine-russia-will-not-waste-offensive-cyber-weapons>)

Cyberattacks, in this war, are a **last resort**, not an opening gambit.

The lingering threat of offensive cyber operations is Putin’s **last card** – together with nukes. There is no rational reason that Putin’s Russia would play the offensive cyber card without some **reasonable prospect** of **geopolitical gain**.

Russia has achieved an operational stalemate with limited progress in its invasion of Ukraine, but unleashing its advanced cyber capabilities at **this stage** against Western targets will not solve the war. Such attacks will only increase the support for Ukraine without bringing Russia any appreciable battlefield advantage

Western commentaries predicting a Russian cyber onslaught rests upon a general assumption that sees advanced offensive cyber capabilities as being replaceable once used. . In reality, this assumption is **illogical**: there is no hidden cyber armory from which new weapons can be fetched and reloaded for continued cyber bombardment. Exploits, once used, are often parried quickly, and they can’t then be expected to have the same effect they had when first unleashed.

Therefore, Russia is **unlikely to waste** its advanced offensive cyber arsenal on a conflict where there is no value to a cyberattack that couldn’t already be accomplished by kinetic attack: air strikes, Kalibr cruise missiles, and indirect fire. Each advanced and sophisticated offensive cyber weapon represents an investment that, in some cases, is a one-shot ability to exploit a vulnerability. Striking targets in America and within NATO utilizing advanced offensive cyber weapons, without any other goal than to degrade and disrupt, is wasting offensive cyber power.

**The current cyberattacks are categorically distinct from larger cyberwar.**

**Lonergan and Yarhi-Milo 22** — Erica Lonergan, Assistant Professor in the Army Cyber Institute at the United States Military Academy at West Point, Research Scholar in the Saltzman Institute of War and Peace Studies at Columbia University, PhD in Political Science from Columbia University, and Keren Yarhi-Milo, Arnold A. Saltzman Professor of War and Peace Studies in the Political Science Department and the School of International and Public Affairs at Columbia University, former Associate Professor of Politics and International Affairs at Princeton University, PhD and M.A. from the University of Pennsylvania, 2022 (“Cyber Signaling and Nuclear Deterrence: Implications for the Ukraine Crisis,” *War on the Rocks,* Available Online at https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/)

What are the implications of this for the current Ukraine crisis? Thus far, while cyber operations have been used on both sides of the conflict, they have **not played a decisive role** on the battlefield. So far, the United States has been focused on providing cyber defense support to Ukraine and NATO, reportedly to include dispatching Cyber Command’s cyber mission teams to Eastern Europe, as well as seeking to deter potential Russian cyber retaliation in response to U.S. and Western sanctions, especially attacks on U.S. critical infrastructure.

However, if the nuclear dimension of the crisis becomes more acute, policymakers may be tempted to turn to cyber operations to signal resolve to deter Russia in the nuclear domain. Such an approach could be seen as particularly appealing precisely because cyber operations are not kinetic and, therefore, less dangerous than other military moves. But this could have the inverse effect of making **nuclear escalation**, rather than deterrence, **more likely**, for the following reasons.

In 2020, Russia clarified its nuclear declaratory policy to state that Russia reserves the right to use nuclear weapons under a range of contingencies, including an adversary attack against “critical governmental or military sites of the Russian Federation, disruption of which would undermine nuclear forces’ response actions.” Cynthia Roberts has suggested that this particular scenario “likely include[s] cyber attacks against command and control infrastructure and/or attempted leadership decapitation.” Similarly, Dmitry Stefanovich wrote that “[t]here is a wide consensus within the Russian expert community that this also includes possible cyber threats as well as other non-nuclear dangers.” Interestingly, Russia’s declaratory policy contains parallels to the implicit link between cyber attacks and nuclear use contained in the 2018 U.S. Nuclear Posture Review. That document notes that the United States would consider using nuclear weapons under “extreme circumstances,” including “significant non-nuclear strategic attacks … [such as] attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities.”

Therefore, a hypothetical attempt by the United States to conduct a cyber operation against Russian nuclear command, control, and communication systems for signaling purposes, such as to demonstrate resolve or convey a desire to deter the use of nuclear weapons could in practice make their use more likely. Unlike most cyber operations, which rely on secrecy, signals are meant to be seen. And to be sufficiently credible, this kind of cyber operation would have to demonstrate an ability to cause a meaningful effect against Russia’s nuclear systems, rather than a low-cost, unsophisticated cyber operation. Therefore, assuming such an attack were feasible, the chances are greater in this scenario that Russia could interpret U.S. cyber signals as an attack against its critical military systems.

The problem is that, more often than not, cyber operations are ambiguous signals. There is evidence that states can use cyber operations under some (narrow) conditions to signal a desire to de-escalate international crises. But these findings do not extend well to nuclear crises where clarity, rather than uncertainty, is important for stability. The use of cyber operations to defuse crises have involved cyber signaling short of war, not during an ongoing conventional conflict involving nuclear powers. And they have not involved cyber operations targeting a state’s nuclear command and control where states, like Russia, have already staked out declaratory policies. Moreover, states are still at a nascent stage in developing shared indices to inform assessments of intent in cyberspace, especially when it comes to cyber operations in nuclear crises.

Therefore, even if Russia would not take the cataclysmic step of escalating to the first use of nuclear weapons in response to a U.S. cyber operation, it could misinterpret U.S. signaling efforts and take measures to make nuclear use easier (such as making warheads operational, dispersing forces, pre-delegating authority, or increasing automaticity). These readiness measures could increase the chances of **inadvertent** or even **accidental escalation**.