# OCO Info-Sharing Aff-Neg---GDS 2022

### Notes

#### What does the aff do/How does it work?

#### Currently NATO because of their defensive nature has determined that offensive cyber operations cannot be developed or deployed by NATO itself. Instead, they have adopted a policy where NATO will coordinate cyber effects from the individual members in NATO. I.e. think like how NATO doesn’t have an actual standing army, but uses forces from each individual country and coordinates them underneath the NATO flag. The main problem with this is approach is that while most states are willing to voluntarily lend their cyber capabilities/effects to NATO, the framework does not require states disclose the actual capabilities or other information regarding states offensive cyber operations. The plan would have the United States disclose information regarding their offensive cyber operations and their actual capabilities.

#### What are the aff advantages?

#### First is that disclosing information regarding the United States actual capabilities allows NATO generals to better plan around those capabilities. Under the current policy NATO generals can only request an effect take place without actually knowing whether the individual member states can produce that effect. This leaves NATO generals effectively “flying blindly”, which undermines cyber deterrence.

#### Second is that the current policy risks undermining the cohesion of the alliance. First is that the unwillingness of the United States to disclose what their capabilities are or lend useful information to allies regarding their OCO’s hurts their trust. Second is that because the United States doesn’t need to disclose information regarding their OCO’s, they are/will continue to hack into allies’ networks to disrupt adversaries’ cyber actions. This intrusion into allied networks also undermines trust and willingness to cooperate inside the alliance.

#### What are the neg controversies?

#### First is that there is a large debate ongoing inside the literature as to whether offensive cyber operations are good and whether they produce deterrence or instead provoke other countries into war.

#### Second is there are several authors who disagree about whether information sharing will increase trust. This is because the United States often spies on our allies and forcing information sharing will mean that we must tell our allies about the illegal actions we are currently undertaking. (What NATO allies don’t know can’t hurt them). These authors also believe that information sharing will disrupt the alliance as it means that our data and intel is more likely to be stollen as a result of hack on weaker allies with less cyber capabilities.

# AFF --- OCO’s

## 1AC

### 1AC --- Plan

#### The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization through information sharing regarding its offensive cyber operations and capabilities

### 1AC --- Adv --- OCO’s

#### Advantage one is OCO’s:

#### Currently, NATO requires individual member nations to coordinate offensive cyber operations.

Freedberg, 18 (Sydney Freedberg, Sydney J. Freedberg Jr. is the deputy editor for Breaking Defense. graduated summa cum laude from Harvard and holds masters' degrees from Cambridge and Georgetown., 11-16-2018, accessed on 6-17-2022, Breaking Defense, "NATO To ‘Integrate’ Offensive Cyber By Members - Breaking Defense", <https://breakingdefense.com/2018/11/nato-will-integrate-offensive-cyber-by-member-states/>)//Babcii

Independent Assets, Coordinated Action It’s crucial to understand that NATO doesn’t have its own combat units in any domain. It pulls together assets provided by its 29 **members**. “It’s the nations who actually [provide the forces](https://breakingdefense.com/2017/11/they-will-fight-nato-readies-forces-vs-russia/), through the NATO force structure,” Col. Lewis emphasized. “They bring their ships, their planes, their tanks…. Those sovereign capabilities are exactly that: **sovereign**.” “They’re responsible for defending those things,” including in cyberspace, Lewis continued. “It’s out job to make sure we have situational awareness of how they’re defending those things and how their success may or may not have an impact on the overall operation.” In cyberspace as on land, air, or sea, NATO member nations can act either collectively, through the alliance, or individually, as sovereign states. But acting outside alliance channels doesn’t bar them from coordinating with each other: Contrast the war in [Afghanistan](https://breakingdefense.com/2018/05/the-great-afghan-paradox-were-not-winning-but-that-doesnt-mean-we-should-leave/), which was long run as a [NATO operation](https://www.nato.int/cps/em/natohq/topics_8189.htm), and the war in [Iraq](https://breakingdefense.com/tag/iraq/), waged by a “coalition of the willing” outside the alliance but involving multiple nations that happened to be NATO members. A NATO member can even divorce itself from the alliance’s military structure but still participate in NATO operations, as [France](https://breakingdefense.com/tag/france/) did from [1966 to 2008](https://otan.delegfrance.org/France-and-NATO-presentation-1217). So while NATO, by charter, **renounces offensive operations**, its members can still conduct them — on their own legal authority as sovereign states, but, if they wish, in **coordination** with each other and in **consultation with NATO.** With that in mind, here’s a more formal and precise description, which I drafted but which NATO officials read, revised and agreed is accurate: “In all domains — land, air, maritime, and (as of 2016) cyber — NATO relies on forces contributed by its member nations to conduct military operations. “In all domains, NATO operations are governed by the consensus of all 29 member states, executed by SACEUR and subordinate commanders in accordance with the constraints of the approved operation. “In all domains, if a NATO member state decides to conduct an operation using its own forces and its own legal authorities, it may choose to inform NATO command structures and coordinate with NATO plans and operations. “How this applies in the cyber domain specifically: NATO policy, as set by the consensus of the 29 members, is that the alliance itself, in keeping with its defensive mindset, shall not conduct offensive cyber operations. However, this does not restrict unilateral or **multilateral offensive operations by NATO member states**. NATO policy — again, by member consensus — does provide for the integration of sovereign cyberspace effects provided by Allies with the ability and willingness to provide them. That integration into Allied operations and missions will be orchestrated by the NATO CYOC (Cyber Operations Centre).” As I interpret this, a NATO commander, acting in his or her **alliance capacity**, couldn’t order anyone to conduct an offensive cyber operation. But the same commander could suggest an offensive cyber operation, and one or more of the member states could then voluntarily conduct it. Or a commander with a dual NATO and national role could simply take off his NATO hat and use the authority granted him by his own nation to order his own nation’s forces to conduct a cyber attack. The obvious candidate here is [Gen. Scaparrotti](https://breakingdefense.com/2016/03/gen-scaparrotti-to-move-from-korea-to-europe-low-key-4-star/), who is both NATO’s [Supreme Allied Commander Europe](https://shape.nato.int/saceur-2) (SACEUR) and [Commander](http://www.eucom.mil/commander), US European Command (EUCOM). In either case, the national forces conducting the attack can coordinate with other alliance members, through NATO organizations, to “**integrate” the attack with the alliance’s collective defense operations**. For cyberspace specifically, this coordination and integration role is played by the new Cyber Operations Center. It’s as a logical extension of CYOC’s “situational awareness” mission to share information among the member states about what each of them is observing and doing in cyberspace. “NATO doesn’t do offense, but it will integrate **sovereign effects** from the nations that are **capable and willing to provide them**,” Lewis said. “Some nations have stated their willingness to [provide those effects](https://breakingdefense.com/tag/cyber-warfare/). The role of the CYOC is simply to integrate it into the operations in the same way we integrate all the other arrows in the quiver.”

#### The US contributes to NATO’s cyber capabilities now, but that’s worthless without increased info sharing – US cooperation is key.

Sophie Arts, 12-13-2018, [Sophie Arts is the program officer for security and defense policy (SDP) at The German Marshall Fund of the United States (GMF) in Washington, DC, "Offense as the New Defense: New Life for NATO’s Cyber Policy," GMFUS, https://www.gmfus.org/news/offense-new-defense-new-life-natos-cyber-policy]

Deter, then Defend?

NATO’s defenses are only as strong as the sum of those of its members. Like in other domains, alliance cyber assets are not NATO-owned but provided by member states.[19] U.S. capabilities in the cyber domain are by far the most sophisticated among the allies. Besides having an edge over most competitors in the field of cyber security,[20] the United States tops rankings as a global leader in offensive cyber capabilities.[21] The recent announcement that it would contribute its capabilities to NATO operations consequently could help the alliance bolster its deterrence posture against hostile cyber-attacks.

Until recently, NATO and member states, including the United States, have relied on strictly defensive cyber tools to protect their infrastructure. However, given that this approach has done little to discourage hostile actors, the strategic value of incorporating offensive cyber operations has long been discussed. In late 2017, Stoltenberg announced that NATO would integrate cyber weapons of its members into military operations to deter and defend against threats, marking the “biggest overall policy shift in decades,” according to officials.[22]

The U.S. decision to commit offensive and defensive capabilities to NATO follows on the heels of this move. The addition of offensive cyber tools to the defense and deterrence toolbox is not only new for NATO, it also tracks a recent shift in the U.S. posture. The White House authorized the use of offensive cyber weapons to deter foreign adversaries in September with the publication of the Department of Defense’s 2018 Cyber Strategy.[23] The strategy also incorporates a new mission of “defending forward” as a means to “disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict.”[24] While defending forward is, as the name suggests, defensive in nature, it entails targeting foreign cyberspace infrastructure to pre-empt incoming attacks through offensive cyber operations.

"This shift from reactive to preemptive action in cyberspace marks the most significant departure from the previous U.S. cyber strategy.”

This shift from reactive to preemptive action in cyberspace marks the most significant departure from the previous U.S. cyber strategy, published in 2015, and comes in response to persistent cyber campaigns against the United States directed by Russia and China. Taken individually, these offenses may fall short of provoking an official response, but their cumulative impact over time is a significant concern and needs to be addressed. The new forward-leaning posture of the United States seeks to address this threat preemptively without risking an escalation to conventional military uses of force.[25]

Superior cyber capabilities will not be a deterrent per se, but they can add to NATO’s resilience against threats.[26] Aggressive cyber operations have already become an important element in the hybrid warfare tool kit of many adversaries. Adding offensive cyber capabilities will likely not stop this. That is why it is critical that deterrence against cyber threats not only relies on cyber operations, but also draws on the full spectrum of conventional and unconventional responses, as outlined in the 2018 Brussels summit declaration.[27]

Defensive and offensive cyber capabilities can reinforce NATO members’ ability to deter and deny cyber-attacks by disincentivizing other actors from developing cyber weapons in the first place, and by convincing those with or without offensive cyber capabilities that attacks will be largely ineffective or come at an equal or greater cost to them. Proactive cyber defense also can help to anticipate and prevent an attack on computers and networks, which requires active monitoring of hostile actors. This is where offensive cyber operations provide the most strategic value. For instance, they could interfere directly with operations of adversaries by manipulating their devices and infrastructure through malware, or by shutting off power and networks from which an attack originates. They can also affect the calculations of hostile actors who may judge that the potential cost of an attack outweighs its strategic gains.

"Countering cyber threats with offensive operations could have a cascading effect that eventually precipitates conventional conflict."

On the other hand, countering cyber threats with offensive operations could have a cascading effect that eventually precipitates conventional conflict.[28] A more assertive U.S. posture on cyber could thus potentially heighten the risk of an unanticipated crisis in the cyber and conventional domains. This could have serious implications for other NATO allies that might be pulled into a conflict, especially if the lines between NATO and U.S. cyber operations are blurred, based on Mattis' recent statement.

Challenges Remain

While there are still many unknowns in NATO’s cyber policy, the United States’ announcement did clarify how its capabilities would be used in the event of a joint NATO cyber operation. As indicated by the Pentagon, the United States would maintain control over its own personnel and capabilities. This is by no means unusual and not necessarily a surprise. As in most areas, NATO does not rely on commonly owned assets for cyber defense but on national capabilities.[29] Similarly, NATO members retain command and control of cyber operations they provide. However, as the former team leader of NATO’s Task Force Cyber (CISO), Col. Rizwan Ali, has pointed out, this poses a significant challenge to NATO commanders who may not have access to many critical details implicating their decision-making process. In effect, Ali explained, commanders “will request an effect using cyber weaponry during an operation and one of the allies will provide that effect without any further information.”[30] As a result, NATO commanders will be flying blind, lacking many important details regarding limitations of capabilities and potential conflicts with other ongoing operations.

Related to this challenge, NATO’s constraints on information sharing could hurt strategic decision-making processes and cyber operations. While most experts acknowledge that intelligence capabilities within NATO are significant, these remain isolated and well-guarded by national intelligence communities.[31] More advanced information sharing, among allies and with other partners such as the EU, is critical for situational awareness and NATO’s preparedness. Yet, due mostly to a lack of trust between allies, this process is far from being at an optimal level.[32]

When it comes to intelligence sharing, some allies fear that infiltration and attacks against countries with lower resilience could potentially compromise information shared by other member states. Pushback against greater transparency is especially strong on the part of the United States, which owns a large share of NATO’s intelligence capabilities, making it a critical player in alliance intelligence operations from a tactical as well as strategic perspective.[33] Due to the country’s outsized role in this field, NATO’s intelligence adaptation is largely dependent on U.S. inclinations to share capabilities and information with other allies.[34] Although efforts to protect intelligence by minimizing sharing may be justified, elevating the role of the United States in NATO’s cyber policy without increasing transparency could potentially limit tactical effectiveness.

#### US-NATO info sharing is key to set global cyber norms and prevent miscalc.

David Mussington, 2019, [David Mussington is a senior fellow at the Centre for International Governance Innovation, director of the Center for Public Policy and Private Enterprise at University of Maryland, adjunct member of the research staff at the Institute for Defense Analyses, and former senior adviser for cyber policy in the US Department of Defense, later serving on the Obama administration’s National Security Council staff as director for surface transportation security policy., "Strategic Stability, Cyber Operations and International Security," Centre for International Governance Innovation, https://www.jstor.org/stable/pdf/resrep26129.13.pdf]

As a response to grey zone conflict and offence dominance in cyberspace, many national governments, such as the United States, Germany and Canada, have concluded that a static defence is no longer adequate and have been adjusting to allow pre-emptive cyber operations intended to disrupt hostile actors before they can act (Herpig 2018; Nakashima 2018; Grigsby 2017). Organizations at the international level have mirrored this trend. In 2017, the North Atlantic Treaty Organization (NATO) adjusted its policy away from ambiguity on cyber effects to a more responsive stance, establishing a Cyber Operations Centre to integrate the cyber capabilities of its members into military operations (Ricks and Ali 2017). While this may be necessary to cope with the attribution problem and grey zone hostilities, whether or not this will re-enable effective deterrence or cause further destabilization through tit-for-tat escalation remains unclear.

Due to many of its members being on the receiving end of grey zone cyber attacks, NATO has been a leading light in trying to resolve the current uncertainty plaguing international governance of cyber conflict. It has attempted, through efforts such as the establishment of the Cooperative Cyber Defence Centre of Excellence and publication of the Tallinn Manual, to arrive at a clear interpretation of which acts in cyberspace are permissible or not under current international law (Arts 2018). The alliance relies on all members following through on their commitment to collective defence as stipulated under article 5 of the alliance’s treaty. This makes the attribution challenge in cyberwarfare especially problematic, as it can give members a plausible reason to demur on this potentially costly commitment. This is forcing NATO to consider what kind of activity in cyberspace would be serious enough to invoke the collective defence clause. While NATO has affirmed that article 5 could be triggered by a significant cyber attack, as of yet it has not determined a precise threshold (ibid.).

Implications and Policy Consequences

Global strategic stability is undermined by the failure of states to take seriously the erosion of defence capabilities caused by growing reliance on ICT technologies in critical infrastructures and weapon systems. At present, COTS and the ICT supply chain that services critical infrastructure present a particularly vulnerable point of entry for malicious actors. Existing governance and oversight mechanisms concerning the deployment of ICT will prove too lenient for the developing threat environment. Enhanced communication and tighter cooperation between government and the private sector will prove crucial to bolstering defences in this area. More arrangements like the Information Sharing and Analysis Centers, which facilitate intelligence sharing on cyber threats between the public and private sector, would be of great benefit (Lord and Mussington 2017).

Superior coordination and information sharing are also required at the international level. In the face of an offence-dominant environment, efforts must be taken to assuage the uncertainties felt by various actors as to each other’s capabilities and intentions. The technical and political difficulties in attributing cyber attacks, combined with their affordability, will continue to encourage attackers. Those defending against cyber attacks must therefore take a firmer, less equivocal stance than they have so far displayed. Absent an international consensus on what constitutes use of force in cyberspace, the United States and fellow NATO members must collectively decide upon a clear code of conduct for responding to grey zone activities, in order to banish ambiguity and the risk of miscalculation. A red line should be drawn around the most pernicious types of cyber hostilities now being perpetrated, such as attempts to sway foreign elections, the violation of which should trigger a measured yet firm response. Restoring clarity to the “action-reaction” dynamic is necessary both to dissuade hostile actors by guaranteeing reprisal for certain offences, and to solidify an understanding among allies as to when they must come to one another’s assistance. In the long term, the United States and its allies should promote more effective international governance by pushing to have these red lines enshrined as international norms in fora such as the United Nations. There is an urgency to this effort — failure to do so will only entrench the idea that the constant grey zone hostilities we are now witnessing have become a tolerable part of international behaviour

#### Specifically, info-sharing is key to integrate US capabilities below the level of warfare – that solves Russian gray-zone aggression.

Lonergan and Montgomery 22 - Erica D. Lonergan is a former senior fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace and with the New American Engagement Initiative at the Scowcroft Center for Strategy and Security in the Atlantic Council, holds a PhD in political science from Columbia University, and serves as a senior director on the U.S. Cyberspace Solarium Commission, a Congressional commission established to develop a comprehensive national strategy to defend the United States in cyberspace. Mark Montgomery serves as the Executive Director of the Cyberspace Solarium Commission and formerly served as Policy Director for the Senate Armed Services Committee.

Erica D. Lonergan and Mark Montgomery, “PRESSING QUESTIONS: OFFENSIVE CYBER OPERATIONS AND NATO STRATEGY,” Modern War Institute, 1-25-2022, https://mwi.usma.edu/pressing-questions-offensive-cyber-operations-and-nato-strategy/

NATO members are in the midst of a crisis. With Russia massing troops along its border with Ukraine and moving additional forces to Belarus ostensibly to conduct joint military exercises, policymakers fear that Russia is on the precipice of invading Ukraine and taking additional territory by force—similar to Russia’s annexation of Crimea in 2014. But, even if Russian President Vladimir Putin ultimately chooses not to launch a direct, conventional invasion of Ukraine, it is highly likely that he will continue to pursue Russian strategic objectives in the gray zone short of war. The crisis over Ukraine underscores the challenges NATO faces in competing with Russia in the gray zone—especially in cyberspace.

Russia has no such limitations in the gray zone. In addition to traditional forms of irregular warfare, such as the use of plausibly deniable proxy forces (Putin’s “little green men”), Russia has long relied on cyber operations to subvert and undermine rival governments while avoiding actions that would cross a threshold prompting an overwhelming retaliation. Indeed, in tandem with Russia’s conventional military buildup, Ukrainian government agencies were struck with a spate of website defacements. Microsoft also revealed that it had discovered destructive malware in some Ukrainian government systems, which Ukrainian officials have linked to the Belarusian group GhostWriter. Belarus has close ties to Russia, and observers have speculated that Belarus may have been operating in cyberspace on Russia’s behalf.

While Ukraine is not a NATO member, the current situation underscores the enduring strategic challenge the alliance faces in addressing the cyber threat posed by Russia and other actors. In particular, because cost imposition is an integral part of any deterrence strategy (and has been part of NATO’s conventional deterrence strategy), the alliance has begun to explore how it could incorporate offensive cyber operations as a component of its cyber deterrence posture. But, while NATO took important steps to address cyber defense, it took nearly a decade after Russia’s 2007 cyberattack against Estonia to begin to seriously address the issue of offensive cyber operations. Moreover, NATO cyber policy has traditionally focused on cyber operations in a warfighting context—a focus that comes at the expense of considering cyber operations below the level of warfare. As the recent cyberattacks against Ukraine illustrate, the gray zone just beneath the threshold of armed conflict is where NATO faces its most significant cyber threats. With NATO in the middle of conducting a comprehensive initiative, NATO 2030, to strengthen the alliance, it should incorporate an assessment of the role of cyber operations in routine competition.

Offensive Cyber Operations in NATO Strategy Above and Below the Level of Warfare

Historically, NATO’s cyber posture has largely focused on defense and resilience—and this continues to form the bulk of NATO’s approach. The alliance maintains that its “main focus in cyber defence is to protect its own networks (including operations and missions) and enhance resilience.” At the 2014 Wales summit, NATO endorsed the Enhanced Cyber Defence Policy, which affirmed that cyber defense is part of collective defense and that the alliance would incorporate cyber defense into its planning and operations. In 2016, NATO members pledged to improve their cyber defenses through training, education, exercises, and information sharing.

But the seeds were also planted in 2016 for NATO to consider a potential role for offensive cyber operations. That year, the alliance recognized cyberspace as a domain of military operations, comparable to land, sea, and air. At the 2018 Brussels summit, NATO began to more seriously consider offensive cyber operations. Specifically, NATO created the Cyberspace Operations Centre to coordinate requests for member states to provide offensive cyber effects through the Sovereign Cyber Effects Provided Voluntarily by Allies process. Following the 2018 summit, then-Secretary of Defense James Mattis stated in a press conference that five states—the United States, the United Kingdom, Denmark, the Netherlands, and Estonia—were contributing cyber forces to “help NATO fight in this important domain.” More recently, in June 2021, NATO convened in Brussels and committed to a Comprehensive Cyber Defence Policy. A key feature of the new policy is the prominent role of offensive cyber operations. In Brussels, member states committed to “employ the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats.”

NATO’s shift to incorporating offensive cyber operations into existing strategy and policy has focused on integrating offensive effects into conventional military plans and operations in the context of a conflict. While NATO’s updated strategy is a positive development, its limited focus on conflict scenarios for employing cyber power fails to accurately account for the cyber threat environment NATO faces—particularly the mismatch between the alliance’s clear distinction between wartime and peacetime and the approach of adversaries like Russia, who adopt a competition-conflict continuum. Additionally, the focus on employing offensive cyber during a high-end conventional fight is also not consistent with how several NATO members are already engaged in gray zone offensive cyber operations.

The primary threat to NATO allies in the cyber domain is not from high-end, decisive cyberattacks. Instead, cyber threats more frequently and effectively manifest as gray zone tactics designed to have a corrosive effect without rising to the level of warfare. There are numerous examples of this type of threat. For instance, in July 2021, NATO publicly condemned a range of malicious cyber behavior, including the Microsoft Exchange hack (which NATO attributed to China) and ransomware attacks targeting critical infrastructure. Russia has leveraged cyber and disinformation operations to interfere in democratic elections in the United States in 2016, 2018, and 2020; France in 2017; and Germany in 2017 and 2021—to name just a few examples. Russia also conducted distributed denial-of-service cyberattacks against government websites in Montenegro during the lead-up to, and following, Montenegro’s ascension to NATO in 2017. And when NATO forces were positioned in the Baltics beginning in 2017 as part of NATO’s enhanced forward presence, two threat actors, GhostWriter and Secondary Infektion, conducted a range of disinformation campaigns.

Additionally, the reality is that several NATO members are already speaking publicly about offensive cyber operations below the level of warfare and their statements and actions have an effect on the entire alliance. In particular, NATO member nations have not reached a political consensus about the role of offensive cyber operations. In 2018, the US Department of Defense and US Cyber Command issued new strategy and policy documents that articulated a role for the military in conducting offensive cyber operations below the level of armed conflict outside of US-controlled cyberspace (part of the “defend forward” strategy), and there has been some reporting about US offensive cyber operations. For instance, in 2018 the United States disrupted the Russian-linked Internet Research Agency from interfering in the midterm elections. And, more recently, in December 2021 General Paul Nakasone, commander of US Cyber Command, publicly acknowledged that the military played a role in disrupting ransomware groups targeting critical infrastructure. The United States has also worked with other NATO allies, such as Estonia and Montenegro, to conduct “hunt forward” cyber operations on allied and partner networks to uncover and disrupt malicious cyber activity.

Other NATO allies have also been more transparent about offensive cyber operations. In 2020, the United Kingdom announced a significant investment in its National Cyber Force, its organizational arm for offensive cyber operations, and its 2022 National Cyber Strategy emphasized the role of offensive cyber operations. In November 2021, General Nakasone and the director of Government Communications Headquarters—the UK government’s principal signals intelligence agency—stated jointly that the two governments were collaborating to “impose consequences” in cyberspace to disrupt adversary operations. The Netherlands has also publicly alluded to conducting offensive cyber operations.

Next Steps: Addressing Challenges and Mitigating Risks

Given the threat environment facing NATO, as well as the activities of several NATO members, the alliance should deliberately—but purposefully—consider incorporating offensive cyber operations below the level of armed conflict into its deterrence strategy. Any effort to explore a role for offensive cyber operations should also consider the challenges and risks that may come with doing so. A central challenge is that, at the political level, NATO allies lack consensus on the appropriate application of offensive cyber power—especially below the level of armed conflict. Addressing these disagreements among member states is essential because conducting offensive cyber operations often requires maneuvering through or operating on networks controlled by an ally or allies. Right now, NATO members do not collectively agree on the protocols and processes for partner actions in allied networks—and they also disagree on how to define sovereignty in cyberspace, or when an offensive cyber operation would rise to the level of an armed attack.

Offensive cyber operations for NATO also present real interoperability challenges. The role of intelligence in cyber operations is likely to complicate NATO planning processes. Even close allies are likely to be wary about sharing sensitive intelligence for a number of reasons. For instance, they may be averse to sharing information gleaned from signals intelligence collection or because a member state may be using the same exploits for both offensive action and their own espionage—including intelligence collection against allies. Or, allies may simply be worried that sensitive information may become exposed. On top of this, it’s challenging to adjudicate intelligence requirements among allies and to deconflict intelligence and military priorities. It is also not clear whether the alliance has established consensus thresholds that specify the conditions and timeline under which a state would have to notify others of its activities on their networks—if at all.

The alliance should account for, and address, these issues as NATO explores the prospect of incorporating offensive cyber operations below the level of armed conflict into existing NATO simulations and exercises that span the strategic, operational, and tactical levels. A number of important questions about how to coordinate offensive cyber operations and define roles and responsibilities remain unanswered. For instance, how could allies improve intelligence sharing to conduct more rapid attribution, enabling one state or the alliance to respond to adversary cyber activity? What are the conditions under which allies should consider dividing responsibilities for cyber campaign planning and developing accesses and capabilities against strategic targets in, for example, Russia? If some allies are responsible for offensive cyber operations against certain targets, what are the information-sharing and notification requirements?

#### Otherwise, Russia will use cyber and information attacks to escalate

Stanage, 18 (Niall Stanage, Irish journalist and Associate Editor of the American political newspaper, 2-25-2018, accessed on 8-11-2021, TheHill, "The Memo: Russia finds weapon in US divisions", <https://thehill.com/homenews/administration/375382-the-memo-russia-finds-weapon-in-us-divisions>)

Growing political polarization in the United States is a vulnerability that foreign adversaries are exploiting — and experts worry the trend will accelerate. The threat was brought into sharp relief by the indictment of 13 Russians as part of special counsel Robert Mueller’s probe into allegations of collusion between Moscow and the 2016 Trump campaign. The Russian efforts, according to the indictment, were part of a broader effort “to sow discord in the U.S. political system,” achieved mostly by fanning the flames of divisive debates already raging in the country. There is bipartisan concern that the constant tearing of America’s political fabric provides an **opening for Russia**, or any other hostile power, to exploit. “It’s just so easy in today’s polarized environment to take advantage of the biases that people have, and their addiction to social media, and their seeking out information that confirms their preconceived views,” said former Rep. Jason Altmire (D-Pa.). Altmire, who served three terms in Congress, recently authorized a book on political polarization, called "Dead Center: How Political Polarization Divided America and What We Can Do about It." Former New Jersey Gov. Christine Todd Whitman, a centrist Republican, expressed a similar view of the threat. “We can’t accept doing nothing — just shrugging our shoulders,” Whitman told The Hill. She said there’s a need to provide states and localities with funding and training to help them identify and rebuff efforts to meddle in elections. But she acknowledged that the broader shift toward the political extremes would be difficult to counteract, especially when the media has become so fractured. “There is no Walter Cronkite anymore,” Whitman said, referring to the legendary CBS News anchorman whose word carried weight with Americans of all political persuasions during his prime in the 1960s and 1970s. Foreign policy specialists have also sounded the alarm. In a New York Times op-ed last month, former President Obama’s national security adviser Susan Rice argued that “the most significant, long-term threat to our security may be our domestic political polarization.” Rice added, “We need to decide whether we want to remain the world’s pre-eminent power — a strong, cohesive beacon of democracy — or if we are content to allow our national autoimmune disorder, like a flesh-eating disease, to devour our body politic.” Skeptics of the Russia story have noted that there is nothing particularly new or unusual about attempts by Moscow, or by other adversaries, to try to affect public opinion in the United States — just as Washington has meddled in other nation’s affairs for decades. But experts in the area argue that the difference now is that the depth of America's divide makes such attacks more effective. John Sipher spent 28 years in the CIA’s National Clandestine Service. He told The Hill that the Kremlin had been seeking to influence American public opinion “for 70, 80 years.” But, he added, two factors make today’s landscape more fertile ground for such efforts. One, he said, was the way in which “the ability to weaponize information via social media has changed.” In addition he said, “the big problem is us. Our hyperpartisanship and our tribal behavior are dry tinder for the Russians.” The recent indictments make clear the extent to which Russians apparently sought to inflame divisions. Prosecutors allege that they sought to capitalize on racial and religious tensions, backed left-wing Sen. Bernie Sanders (I-Vt.) as well as President Trump in the 2016 campaign, falsely suggested Hillary Clinton harbored sympathies for Sharia law, and even promoted competing pro- and anti-Trump rallies following the 2016 election. Efforts to fuel the flames of American enmity are allegedly ongoing.

#### Ukraine is uniqueness --- Sanctions increase the risk of a shift to catastrophic cyber attacks

Alemany, 22 (Jacqueline Alemany, Jacqueline Alemany is a Congressional Investigations reporter for The Washington Post. Alemany studied government at Harvard University, 3-8-2022, accessed on 6-18-2022, The Washington Post, "Lawmakers wonder whether NATO is ready to robustly defend against a cyberattack against one of its own", <https://www.washingtonpost.com/politics/2022/03/08/lawmakers-wonder-whether-nato-is-ready-robustly-defend-cyber-attack-against-one-if-its-own/>)//Babcii

Lawmakers wonder whether NATO is ready to robustly defend against a cyberattack against one of its own The other battlefield: It isn't only Russia's military might that has some U.S. **lawmakers and experts concerned** about what's next in the conflict with Ukraine. They're also worried about a stealthy but possibly just as damaging enemy: **cyber warfare.** They believe that as Russian President Vladimir Putin is pressed on the battlefield and continues to be squeezed by the sharp bite of U.S. and European sanctions, NATO's newly evolved cyber policy might not be prepared to respond. Over the past decade, **NATO** — like most organizations and entities — has modernized its cyber defensive posture and practices, prompting NATO to say last year that it would “weigh ‘on a case-by-case basis’ whether a cyberattack would trigger its Article 5 collective defense principle, which establishes that an attack against one ally is an attack against all allies,” our colleagues [Cat Zakrzewski and Joseph Menn reported last month.](https://www.washingtonpost.com/technology/2022/02/24/russia-cyberattacks-global/?itid=lk_inline_manual_9) “We will not speculate on how serious a cyberattack would have to be in order to trigger a collective response,” a NATO official [told reporters month](https://www.reuters.com/world/europe/cyberattack-nato-could-trigger-collective-defence-clause-official-2022-02-28/). “Any response could include diplomatic and economic sanctions, cyber measures, or even conventional forces, depending on the nature of the attack,” the official added. The updated policy, according to former U.S. ambassadors to NATO and experts who work closely with the organization, has come a long way since Russian-based attackers launched [massive cyberattacks on Estonia](https://www.bbc.com/news/39655415) over the removal of a Soviet war memorial in the small Baltic country in 2007. As it currently stands, NATO leaders were **deliberately ambiguous** in defining what would qualify as an Article 5 attack when revising the group's cyber policy, “so as not to create a clear-cut threshold beneath which an opponent could operate freely,” said Douglas Lute, a former U.S. ambassador to NATO. But there is some concern the ambiguity might muddle a potential response to a cyberattack. Key quote: “If you have a catastrophic cyberattack that shuts down your [power] grids or shuts down your ability to keep your people warm in the winter or fed or what have you, we've got to figure that out. I think NATO needs to get together and have those very difficult [discussions] because it is a component of war, as I said before, **and I think it needs to be viewed as such**,” Rep. John Katko (R-N.Y.), the top Republican on the House Homeland Security panel, told The Washington Post in [an interview last week](https://www.washingtonpost.com/washington-post-live/2022/03/01/117th-congress-rep-john-katko-r-ny/?itid=lk_inline_manual_16). **“I think it's evolving**. Do **they have more to go**? Absolutely,” Katko added of NATO.

#### Failure to successfully check Russia causes cascading conflicts throughout Europe --- great power war.

Graham 22 — Thomas Graham, Distinguished Fellow at the Council on Foreign Relations, Cofounder of the Russian, East European, and Eurasian Studies Program at Yale University, 2022 (“Preventing a Wider European Conflict,” *Council on Foreign Relations,* March 8th, Available Online at https://www.cfr.org/report/preventing-wider-european-conflict#chapter-title-0-1)

The large-scale Russian invasion of Ukraine now underway could quite plausibly precipitate a wider conflict in Europe. The United States is focused primarily on raising the costs to Russia with punishing sanctions and reassuring North Atlantic Treaty Organization (NATO) allies neighboring Russia of its commitment to collective defense. Less attention has been given to containing the war to Ukraine and preventing its escalation into a broader European conflict.

The stakes are enormous. The ripple effects of a wider conflict in Europe would spread across the globe, stressing the geopolitical, economic, and institutional foundations of the international order the United States has fashioned and underwritten since the end of the Second World War. It would test the resilience of the U.S. global system of alliances, the international financial system, global energy markets, arms control regimes, and global institutions in the face of ever more violent great power competition. No region of the world would be spared, although developments on the Eurasian supercontinent, the other locus of world power and economic might outside North America, would bear the gravest consequences for U.S. interests.

The Contingency

The Russian military intervention in Ukraine could easily escalate into a larger conflict stretching from the Baltic to the Black Sea and further west into Europe. Although Russia, wielding massive military superiority, might overrun Ukrainian forces in a matter of weeks, stabilizing and pacifying the country will likely prove to be a grueling and costly affair. A significant Ukrainian resistance movement is almost certain to emerge. With sustained Western support, it could prolong the warfare for months, if not years. The first wave of sanctions that Washington has levied on Moscow could be followed by others in a continuing effort to raise the cost to Moscow and force it to yield. A negotiated end to the conflict will not come easily, since Washington has framed it in Manichean terms as a world historical struggle between the democratic West and the aggressive, malevolent, and autocratic Russia. Anything short of “victory” will be decried as surrender or appeasement in the West, while Russia will not capitulate on a matter it considers vital to its security and prosperity.

The stage is thus set for an escalating cycle of violence, with Moscow seeking to stamp out a Ukrainian insurgency and retaliate against Western efforts to stop Russia’s advance. If the conflict wears on, Moscow could be increasingly tempted to expand its military operations further into Europe to achieve its goals.

As a first option, Russia could intensify pressure on states neighboring Ukraine (e.g., Hungary, Poland, Romania, and Slovakia) that could provide safe havens for insurgents or the inevitable government-in-exile. It will doubtless reinforce its military presence in Kaliningrad and elsewhere in the Baltics and patrol the Baltic Sea more aggressively. It could deploy hybrid-war tactics—cyberattacks, disinformation campaigns, and economic sabotage—to destabilize countries providing safe havens. If those actions did not sufficiently degrade the resistance, Moscow could even launch direct attacks on insurgents and their supporters outside Ukraine, as well as attempt to assassinate leading figures in the government-in-exile, akin to the attacks it has made on Chechen rebels and Federal Security Service (FSB) defectors in Europe in recent years. Such steps could, at a minimum, draw frontline NATO states directly into the military conflict with Russia, obligating the United States and other allies to come to their defense.

To build up further pressure, Moscow could also “weaponize” the inevitable refugee flows into neighboring states. Refugees, who would likely number in the millions, would move first into unoccupied Ukrainian territory but eventually into adjacent European states, which have shown little tolerance for outsiders. Moscow could use harsh military and police tactics that would increase the number of refugees and seek to guide them into countries where they would create the greatest socioeconomic stress, such as Moldova. In addition, Moscow could increase the tension by pushing Belarusian President Aleksandr Lukashenko to again seek to push thousands of Middle Eastern migrants across the borders into Poland and Lithuania. That could lead to border clashes, as it almost did on occasion last fall, with Russia supporting its ally, Belarus, and NATO states coming to the defense of allies under attack.

A second option Moscow could pursue is opening up a second front in the Balkans. In recent years, Russia has taken a number of destabilizing actions in the region, seeking to weaken Montenegro after its accession to NATO, exacerbate tensions between Serbs and Bosniaks in Bosnia-Herzegovina, and undermine relations between Serbia and Kosovo. As it fought in Ukraine, Russia could encourage Republika Srpska leader Milorad Dodik to press for separation from Bosnia, threatening to reignite the bitter wars of the 1990s in the former Yugoslavia. A Balkans war would complicate the security calculus of all countries in the region, as well as that of Germany and France, which have significant interests there. To quell the fighting, NATO countries could decide to use military force against Bosnian Serb forces enjoying Russian support.

A third, riskier, option would be to directly attack the United States, the country that Moscow believes is orchestrating a larger anti-Russia campaign. In response to Western sanctions designed to crater Russia’s financial system and undermine critical industries, Moscow could launch major cyberattacks against U.S. critical infrastructure. If a cyberattack were to take down a major financial institution or corrupt its records, the ensuing havoc in U.S. markets could prompt overwhelming public and congressional pressure for a forceful response.

The U.S. and NATO response to Russian actions will impact Moscow’s decisions on the conduct of the conflict. Both a weak response and an excessively harsh one could lead to escalation. In the first case, Moscow could be tempted to press militarily even further into Europe to enlarge its sphere of influence. Vladimir Putin has demanded that NATO withdraw its forces back to the lines they held in 1997, when the NATO-Russia Founding Act was signed and the first wave of post−Cold War expansion remained in the future. His remarks announcing the start of hostilities against Ukraine hinted at a broader effort to restore Russia’s control over all of the former Soviet Union. That could include military action against the Baltic states, especially Lithuania, through which Moscow could try to carve out a land corridor to Kaliningrad, a Russian exclave on the Baltic Sea. NATO would have little choice but to provide military aid to those states if it did not want to forfeit its role as the central pillar of European security.

Crippling sanctions, meanwhile, could provoke Putin to lash out with greater violence. If Putin felt cornered, he could escalate the conflict either horizontally to other countries or vertically to the nuclear level in a desperate effort to save himself, his regime, and, in his mind, Russia itself. And he could find considerable public support for such a reaction. Already, some Russians believe that U.S. and EU sanctions are aimed not simply at the leaders behind the war but, by cratering the economy, at all Russians.

Warning Indicators

As is the case with the current crisis in Ukraine, Moscow’s intentions will remain ambiguous. The indicators of an approaching escalation in the conflict beyond Ukraine are likely to fall into three categories.

The first indicators that political and military conditions are increasing the risk of broader conflict include a breakdown in channels of communication with Moscow. The absence of active diplomatic ties would preclude a negotiated resolution of the conflict in Ukraine. An end to U.S.-Russian military-to-military channels would undermine any effort to avoid direct military conflict between the two countries. Another indicator would be major insurgent successes that dramatically increase Russian casualties. Moscow would be tempted to move more aggressively against insurgent safe havens rather than capitulate on what it considers to be its vital interest in Ukraine.

Second are the indicators that Moscow is preparing for a broader conflict, which it would undoubtedly argue had been forced by Western actions. Such signs include Kremlin efforts to prepare the Russian public for a wider conflict, which could entail official statements, greater media focus on escalating Western “aggression,” an increased pace of civil defense drills, and mobilization of reserves. Another indicator includes the massing of Russian forces in the Baltic region. It could include such moves as aggressive hybrid actions to destabilize Poland and the Baltic states, coupled with efforts to rally indigenous ethnic Russian communities against their governments.

Third are the indicators that Moscow is intentionally seeking to widen the conflict. This could include greater support for Bosnian Serb leader Dodik, such as diplomatic and financial backing, and provision of weapons. They could also encourage Serb leaders to more assertively pursue their grievances against Kosovo.

Implications for the United States

A wider European conflict would pose the stiffest challenge to the global standing of the United States since the end of the Cold War and to the international system it has built and underwritten for decades longer. It would test the durability of its global system of alliances and the efficacy of international regimes and institutions that have guarded world peace, security, and prosperity. The challenge would come at a time when the United States itself is in immense disarray, as a deeply polarized polity confronts massive domestic problems—the pandemic, inflation, racial justice, and cultural wars—that leave less time and fewer resources for foreign matters. The United States will be tested to see whether it can muster the will, energy, and creativity to execute an effective policy toward the unfolding crisis in Europe.

#### Overcomes historical checks to nuclear war.

Fisher 15 — Max, foreign policy editor at Vox. former reporter at the Washington Post and foreign editor at The Atlantic, M.A. international security, Johns Hopkins University, “How World War III became possible,” Vox, 6-29-2015, http://www.vox.com/2015/6/29/8845913/russia-war

How World War III became possible A nuclear conflict with Russia is likelier than you think It was in August 2014 that the real danger began, and that we heard the first warnings of war. That month, unmarked Russian troops covertly invaded eastern Ukraine, where the separatist conflict had grown out of its control. The Russian air force began harassing the neighboring Baltic states of Estonia, Latvia, and Lithuania, which are members of NATO. The US pledged that it would uphold its commitment to defend those countries as if they were American soil, and later staged military exercises a few hundred yards from Russia's border. Both sides came to believe that the other had more drastic intentions. Moscow is convinced the West is bent on isolating, subjugating, or outright destroying Russia. One in three Russians now believe the US may invade. Western nations worry, with reason, that Russia could use the threat of war, or provoke an actual conflict, to fracture NATO and its commitment to defend Eastern Europe. This would break the status quo order that has peacefully unified Europe under Western leadership, and kept out Russian influence, for 25 years. Fearing the worst of one another, the US and Russia have pledged to go to war, if necessary, to defend their interests in the Eastern European borderlands. They have positioned military forces and conducted chest-thumping exercises, hoping to scare one another down. Putin, warning repeatedly that he would use nuclear weapons in a conflict, began forward-deploying nuclear-capable missiles and bombers. Europe today looks disturbingly similar to the Europe of just over 100 years ago, on the eve of World War I. It is a tangle of military commitments and defense pledges, some of them unclear and thus easier to trigger. Its leaders have given vague signals for what would and would not lead to war. Its political tensions have become military buildups. Its nations are teetering on an unstable balance of power, barely held together by a Cold War–era alliance that no longer quite applies. If you take a walk around Washington or a Western European capital today, there is no feeling of looming catastrophe. The threats are too complex, with many moving pieces and overlapping layers of risk adding up to a larger danger that is less obvious. People can be forgiven for not seeing the cloud hanging over them, for feeling that all is well — even as in Eastern Europe they are digging in for war. But this complacency is itself part of the problem, making the threat more difficult to foresee, to manage, or, potentially, to avert. "There’s a low nuclear threshold now that didn’t exist during the Cold War" There is a growing chorus of political analysts, arms control experts, and government officials who are sounding the alarm, trying to call the world's attention to its drift toward disaster. The prospect of a major war, even a nuclear war, in Europe has become thinkable, they warn, even plausible. What they describe is a threat that combines many of the hair-trigger dangers and world-ending stakes of the Cold War with the volatility and false calm that preceded World War I — a comparison I heard with disturbing frequency. They describe a number of ways that an unwanted but nonetheless major war, like that of 1914, could [cause] break out in the Eastern European borderlands. The stakes, they say, could not be higher: the post–World War II peace in Europe, the lives of thousands or millions of Eastern Europeans, or even, in a worst-case scenario that is remote but real, the nuclear devastation of the planet. [Update, Nov. 24: If you're reading this in response to Turkey reportedly shooting down a Russian warplane today, read here for why that incident will not lead to war, and why it's very different from the scenarios described in this story.] I. The warnings: "War is not something that's impossible anymore" Everyone in Moscow tells you that if you want to understand Russia's foreign policy and its view of its place the world, the person you need to talk to is Fyodor Lukyanov. Sober and bespectacled, with an academic's short brown beard, Lukyanov speaks with the precision of a political scientist but the occasional guardedness of someone with far greater access than your average analyst. Widely considered both an influential leader and an unofficial interpreter of Russia's foreign policy establishment, Lukyanov is chief of Russia's most important foreign policy think tank and its most important foreign policy journal, both of which reflect the state and its worldview. He is known to be close to Russian Foreign Minister Sergei Lavrov. I met Lukyanov around the corner from the looming Foreign Ministry compound (his office is nearby), at a small, bohemian cafe in Moscow that serves French and Israeli food to a room packed with gray suits. He was candid and relaxed. When the discussion turned to the risks of war, he grew dire. "The atmosphere is a feeling that war is not something that’s impossible anymore," Lukyanov told me, describing a growing concern within Moscow's foreign policy elite. "A question that was absolutely impossible a couple of years ago, whether there might be a war, a real war, is back," he said. "People ask it." Read the full interview with Fyodor Lukyanov I asked how this had happened. He said that regular Russian people don't desire war, but rather feared it would become necessary to defend against the implacably hostile United States. "The perception is that somebody would try to undermine Russia as a country that opposes the United States, and then we will need to defend ourselves by military means," he explained. Such fears, vague but existential, are everywhere in Moscow. Even liberal opposition leaders I met with, pro-Western types who oppose Putin, expressed fears that the US posed an imminent threat to Russia's security. I had booked my trip to Moscow in December, hoping to get the Russian perspective on what were, at the time, murmurings among a handful of political and arms control analysts that conflict could come to Europe. By the time I arrived in the city, in late April, concerns of an unintended and potentially catastrophic war had grown unsettlingly common. Lukyanov, pointing to the US and Russian military buildups along Eastern Europe, also worried that an accident or provocation could be misconstrued as a deliberate attack and lead to war. In the Cold War, he pointed out, both sides had understood this risk and installed political and physical infrastructure — think of the "emergency red phone" — to manage tensions and prevent them from spiraling out of control. That infrastructure is now gone. "All those mechanisms were disrupted or eroded," he said. "That [infrastructure] has been degraded since the end of the Cold War because the common perception is that we don’t need it anymore." That the world does not see the risk of war hanging over it, in other words, makes that risk all the likelier. For most Americans, such predictions sound improbable, even silly. But the dangers are growing every week, as are the warnings. "One can hear eerie echoes of the events a century ago that produced the catastrophe known as World War I," Harvard professor and longtime Pentagon adviser Graham Allison — one of the graybeards of American foreign policy — wrote in a May cover story for the National Interest, co-authored with Russia analyst Dimitri Simes. Their article, "Russia and America: Stumbling to War," warned that an unwanted, full-scale conflict between the US and Russia was increasingly plausible. In Washington, the threat feels remote. It does not in Eastern Europe. Baltic nations, fearing war, have already begun preparing for it. So has Sweden: "We see Russian intelligence operations in Sweden — we can't interpret this in any other way — as preparation for military operations against Sweden," a Swedish security official announced in March. In May, Finland's defense ministry sent letters to 900,000 citizens — one-sixth of the population — telling them to prepare for conscription in case of a "crisis situation." Lithuania has reinstituted military conscription. Poland, in June, appointed a general who would take over as military commander in case of war. Though Western publics remain blissfully unaware, and Western leaders divided, many of the people tasked with securing Europe are treating conflict as more likely. In late April, NATO and other Western officials gathered in Estonia, a former Soviet republic and NATO member on Russia's border that Western analysts most worry could become ground zero for a major war with Russia. At the conference, Deputy Secretary General Alexander Vershbow spoke so openly about NATO's efforts to prepare for the possibility of Russia launching a limited nuclear strike in Europe that, according to the journalist Ahmed Rashid, who was in attendance, he had to be repeatedly reminded he was speaking on the record. One of the scenarios Vershbow said NATO was outlining, according to Rashid's paraphrase, was that Russia could "choose to use a tactical weapon with a small blast range on a European city or a Western tank division." A few weeks later, the Guardian reported that NATO is considering plans to "upgrade" its nuclear posture in Europe in response to Russia's own nuclear saber-rattling. One proposal: for NATO's military exercises to include more nuclear weapons use, something Russia already does frequently. II. The gamble: Putin's plan to make Russia great again Should the warnings prove right, and a major war break out in Europe between Russia and the West, then the story of that war, if anyone is still around to tell it, will begin with Russian President Vladimir Putin trying to solve a problem. That problem is this: Putin's Russia is weak. It can no longer stand toe to toe with the US. It no longer has Europe divided in a stalemate; rather, it sees the continent as dominated by an ever-encroaching anti-Russian alliance. In the Russian view, the country's weakness leaves it at imminent risk, vulnerable to a hostile West bent on subjugating or outright destroying Russia as it did to Iraq and Libya. This is made more urgent for Putin by his political problems at home. In 2012, during his reelection, popular protests and accusations of fraud weakened his sense of political legitimacy. The problem worsened with Russia's 2014 economic collapse; Putin's implicit bargain with the Russian people had been that he would deliver economic growth and they would let him erode basic rights. Without the economy, what did he have to offer them? Putin's answer has been to assert Russian power beyond its actual strength — and, in the process, to recast himself as a national hero guarding against foreign enemies. Without a world-power-class military or economy at his disposal, he is instead wielding confusion and uncertainty — which Soviet leaders rightly avoided as existential dangers — as weapons against the West. Unable to overtly control Eastern Europe, he has fomented risks and crises there, sponsoring separatists in Ukraine and conducting dangerous military activity along NATO airspace and coastal borders, giving Russia more leverage there. Reasserting a Russian sphere of influence over Eastern Europe, he apparently believes, will finally give Russia security from the hostile West — and make Russia a great power once more. Knowing his military is outmatched against the Americans, he is blurring the distinction between war and peace, deploying tactics that exist in, and thus widen, the gray between: militia violence, propaganda, cyberattacks, under a new rubric the Russian military sometimes calls "hybrid war." "This was the theory of the Kaiser before World War I: The more threatening you are, the more people will submit to your will. Putin’s going to threaten and threaten and hope that NATO bends. But the long run of international relations suggests that it goes the other way." Unable to cross America's red lines, Putin is doing his best to muddy them — and, to deter the Americans, muddying his own. Turning otherwise routine diplomatic and military incidents into games of high-stakes chicken favors Russia, he believes, as the West will ultimately yield to his superior will. To solve the problem of Russia's conventional military weakness, he has dramatically lowered the threshold for when he would use nuclear weapons, hoping to terrify the West such that it will bend to avoid conflict. In public speeches, over and over, he references those weapons and his willingness to use them. He has enshrined, in Russia's official nuclear doctrine, a dangerous idea no Soviet leader ever adopted: that a nuclear war could be winnable. Putin, having recast himself at home as a national hero standing up to foreign enemies, is more popular than ever. Russia has once more become a shadow hanging over Eastern Europe, feared and only rarely bowed to, but always taken seriously. Many Western Europeans, asked in a poll whether they would defend their own Eastern European allies from a Russian invasion, said no. Russia's aggression, born of both a desire to reengineer a European order that it views as hostile and a sense of existential weakness that justifies drastic measures, makes it far more willing to accept the dangers of war. As RAND's F. Stephen Larrabee wrote in one of the increasingly urgent warnings that some analysts are issuing, "The Russia that the United States faces today is more assertive and more unpredictable — and thus, in many ways, more dangerous — than the Russia that the United States confronted during the latter part of the Cold War." Joseph Nye, the dean of Harvard University's school of government and one of America's most respected international relations scholars, pointed out that Russia's weakness-masking aggression was yet another disturbing parallel to the buildup to World War I. "Russia seems doomed to continue its decline — an outcome that should be no cause for celebration in the West," Nye wrote in a recent column. "States in decline — think of the Austro-Hungarian Empire in 1914 — tend to become less risk-averse and thus much more dangerous." III. The drift: How the unthinkable became possible The Cold War was a dangerous game, but it was a game in which everyone knew and agreed upon the stakes and the rules. That is not the case today. The Western side believes it is playing a game where the rules are clear enough, the stakes relatively modest, and the competition easily winnable. The Russian side, however, sees a game where the rules can be rewritten on the fly, even the definition of war itself altered. For Russia, fearing a threat from the West it sees as imminent and existential, the stakes are unimaginably high, justifying virtually any action or gamble if it could deter defeat and, perhaps, lead to victory. Separately, the ever-paranoid Kremlin believes that the West is playing the same game in Ukraine. Western support for Ukraine's government and efforts to broker a ceasefire to the war there, Moscow believes, are really a plot to encircle Russia with hostile puppet states and to rob Russia of its rightful sphere of influence. Repeated Russian warnings that it would go to war to defend its perceived interests in Ukraine, potentially even nuclear war, are dismissed in most Western capitals as bluffing, mere rhetoric. Western leaders view these threats through Western eyes, in which impoverished Ukraine would never be worth risking a major war. In Russian eyes, Ukraine looks much more important: an extension of Russian heritage that is sacrosanct and, as the final remaining component of the empire, a strategic loss that would unacceptably weaken Russian strength and thus Russian security. Both side are gambling and guessing in the absence of a clear understanding of what the other side truly intends, how it will act, what will and will not trigger the invisible triplines that would send us careening into war. Today's tensions bear far more similarity to the period before World War I During the Cold War, the comparably matched Western and Soviet blocs prepared for war but also made sure that war never came. They locked Europe in a tense but stable balance of power; that balance is gone. They set clear red lines and vowed to defend them at all costs. Today, those red lines are murky and ill-defined. Neither side is sure where they lie or what really happens if they are crossed. No one can say for sure what would trigger war. That is why, analysts will tell you, today's tensions bear far more similarity to the period before World War I: an unstable power balance, belligerence over peripheral conflicts, entangling military commitments, disputes over the future of the European order, and dangerous uncertainty about what actions will and will not force the other party into conflict. Today's Russia, once more the strongest nation in Europe and yet weaker than its collective enemies, calls to mind the turn-of-the-century German Empire, which Henry Kissinger described as "too big for Europe, but too small for the world." Now, as then, a rising power, propelled by nationalism, is seeking to revise the European order. Now, as then, it believes that through superior cunning, and perhaps even by proving its might, it can force a larger role for itself. Now, as then, the drift toward war is gradual and easy to miss — which is exactly what makes it so dangerous. But there is one way in which today's dangers are less like those before World War I, and more similar to those of the Cold War: the apocalyptic logic of nuclear weapons. Mutual suspicion, fear of an existential threat, armies parked across borders from one another, and hair-trigger nuclear weapons all make any small skirmish a potential armageddon. In some ways, that logic has grown even more dangerous. Russia, hoping to compensate for its conventional military forces' relative weakness, has dramatically relaxed its rules for using nuclear weapons. Whereas Soviet leaders saw their nuclear weapons as pure deterrents, something that existed precisely so they would never be used, Putin's view appears to be radically different. Russia's official nuclear doctrine calls on the country to launch a battlefield nuclear strike in case of a conventional war that could pose an existential threat. These are more than just words: Moscow has repeatedly signaled its willingness and preparations to use nuclear weapons even in a more limited war. This is a terrifyingly low bar for nuclear weapons use, particularly given that any war would likely occur along Russia's borders and thus not far from Moscow. And it suggests Putin has adopted an idea that Cold War leaders considered unthinkable: that a "limited" nuclear war, of small warheads dropped on the battlefield, could be not only survivable but winnable. "It’s not just a difference in rhetoric. It’s a whole different world," Bruce G. Blair, a nuclear weapons scholar at Princeton, told the Wall Street Journal. He called Putin's decisions more dangerous than those of any Soviet leader since 1962. "There’s a low nuclear threshold now that didn’t exist during the Cold War." Nuclear theory is complex and disputable; maybe Putin is right. But many theorists would say he is wrong, that the logic of nuclear warfare means a "limited" nuclear strike is in fact likely to trigger a larger nuclear war — a doomsday scenario in which major American, Russian, and European cities would be targets for attacks many times more powerful than the bombs that leveled Hiroshima and Nagasaki. Even if a nuclear war did somehow remain limited and contained, recent studies suggest that environmental and atmospheric damage would cause a "decade of winter" and mass crop die-outs that could kill up to 1 billion people in a global famine. IV. How it would happen: The Baltics scenario In September of last year, President Obama traveled to Estonia, a nation of 1.3 million people that most Americans have never heard of, and pledged that the United States would if necessary go to war with Russia to defend it. Estonia, along with Latvia and Lithuania — together known as the Baltic states — are at the far edge of Eastern Europe, along Russia's border. They were formerly part of the Soviet Union. And they are where many Western analysts fear World War III is likeliest to start. These small countries are "the most likely front line of any future crisis," according to Stephen Saideman, an international relations professor at Carleton University. Allison and Simes, in their essay warning of war, called the Baltics "the Achilles’ heel of the NATO alliance." A full quarter of Estonia's population is ethnically Russian. Clustered on the border with Russia, this minority is served by the same Russian state media that helped stir up separatist violence among Russian speakers in eastern Ukraine. But unlike Ukraine, the Baltic states are all members of NATO, whose charter states that an attack on one member is an attack on them all. Whereas a Russian invasion of Ukraine prompted Western sanctions, a Russian invasion of Estonia would legally obligate the US and most of Europe to declare war on Moscow. "We'll be here for Estonia. We will be here for Latvia. We will be here for Lithuania. You lost your independence once before. With NATO, you will never lose it again," Obama pledged in his September speech in Estonia. Less than 48 hours after Obama's address, Russian agents blanketed an Estonia-Russia border crossing with tear gas, stormed across, and kidnapped an Estonian state security officer, Eston Kohver, who specialized in counterintelligence. Kohver has been held illegally in a Russian prison for nine months now. It was something like an act of geopolitical trolling: aggressive enough to assert Russian dominion over Estonia, but not so aggressive as to be considered a formal act of war that would trigger a Western counterattack. And it was one of several signs that Putin's Russia is asserting a right to meddle in these former Soviet territories. The Russian military has already begun pressing the Baltic states. Russian warships were spotted in Latvian waters 40 times in 2014. Russian military flights over the Baltics are now routine, often with the planes switching off their transponders, which makes them harder to spot and increases the chances of an accident. Military activity in the region had reached Cold War levels. NATO, fearing the worst, is increasing military exercises in the Baltics. The US is installing heavy equipment. And in February, the US military paraded through the Russian-majority Estonian city of Narva, a few hundred yards from Russia's borders. "Without any intention to create the big conflict, it might happen. One step, another step, and reciprocity can become very dangerous." It's a textbook example of what political scientists call the security dilemma: Each side sees its actions as defensive and the other side's as offensive. Each responds to the other's perceived provocations by escalating further, a self-reinforcing cycle that can all too easily lead to war. It is considered, for example, a major contributor to the outbreak of World War I. That it is entirely foreseeable does little to reduce the risk. Even if Russia in fact has no designs on the Baltics, its bluffing and posturing has already created the conditions for an unwanted war. In early April, for example, a Russian fighter jet crossed into the Baltic Sea and "buzzed" a US military plane, missing it by only 20 feet. It was one of several recent near-misses that, according to a think tank called the European Leadership Institute, have had a "high probability of causing casualties or a direct military confrontation between Russia and Western states." Meanwhile, Russia has been flying its nuclear-capable strategic bombers along NATO airspace, often with the planes' transponders switched off, making an accident or misperception more likely. As if that weren't dangerous enough, the bombers — hulking, decades-old Tupolev Tu-95 models — have become prone to accidents such as engine fires. What if a Tu-95 went down unexpectedly, say, off the coast of Norway? What if it was carrying nuclear warheads, or it went down during a moment of high tension? Such incidents can lead to misunderstandings, and such misunderstandings can lead to war. By late April, when NATO officials gathered at the security conference in Estonia's capital of Tallinn, the severity of the danger had become unmistakable. As Ahmed Rashid wrote from the conference: Baltic presidents and NATO officials were unusually blunt in describing the extent to which the security architecture in Eastern Europe has collapsed, how Russia poses the gravest threat to peace since World War II, and how the conflict in Ukraine and the loss of the Crimea has left the Baltic states on the front line of an increasingly hostile standoff. Amid these tensions, the thought of a plane crash leading to war seems scarily plausible. It is not just Western officials who fear such an incident could spark war. Fyodor Lukyanov, the prominent Russian analyst who is considered close to the government, worried that the NATO military exercises in the Baltics meant to deter Russia were also contributing to the problem. "Russia reacts to that because Russia perceives it as a hostile approach to the Russian border," he explained. "And it’s a vicious circle." It is easy to imagine, Lukyanov said, any number of ways that the powder keg could explode. "Without any intention to create the big conflict, it might happen," he said. "One step, another step, and reciprocity can become very dangerous. Say a Russian aircraft comes very close to an area that NATO believes is prohibited while Russia believes it’s not prohibited, and then British aircraft respond. It might be manageable, and in most cases of course it will be, but who knows." V. How it would happen: A plot to break NATO It was Andrei Piontkovsky, a Russian political analyst and frequent Kremlin critic, who first suggested the theory, last August, that Putin's plan for the Baltics was more sophisticated, and more calculated, than anybody realized. Piontkovsky was trying to answer a question that Western analysts and policymakers had been puzzling over since Russian provocations began in the Baltics last fall: What does Putin want? Unlike in Ukraine, with which Russia has a long shared history, there is little demand among the Russian public for intervention in the Baltic states. They are of modest strategic value. And the risks of Russia's aggression there are potentially catastrophic. Why bother? His is a theory that is now taken much more seriously by Western policymakers — and appears more plausible all the time. "This is his most cherished objective, to destroy NATO. The risk is big, yes? But the prize is enormous." Putin hopes to spark a conflict in the Baltics, Piontkovsky wrote, so as to force Western European leaders into an impossible choice: Fulfill their NATO obligation to defend the Baltics and counterattack, even if it means fighting World War III over a tiny post-Soviet republic most Europeans couldn't care less about — or do nothing. The implications of doing nothing, Piontkovsky pointed out, would extend far beyond the Baltics. It would lay bare NATO's mutual defense provision as a lie, effectively dissolving the military alliance, ending a quarter-century of Europe's security unification under Western leadership, and leaving Eastern Europe once more vulnerable to Russian domination. In this way, Putin could do what Soviet leaders never came close to: defeat NATO. "This is his most cherished objective," Piontkovsky told me when we talked in his kitchen, in a leafy Moscow neighborhood across the river from Gorky Park. "It's an enormous temptation. He may retreat at any stage, but the temptation is enormous, to destroy NATO. ... The risk is big, yes? But the prize is enormous." "To destroy NATO, to demonstrate that Article V does not work, the Baltic republics of Estonia and Latvia are the best place for this," he said. "It's happening now, every day. Intrusions into the airspace, psychological pressure, the propaganda on TV." He suggested that Putin, rather than rolling Russian tanks across the border, would perhaps seed unmarked Russian special forces into, say, the Russian-majority city of Narva in Estonia, where they would organize localized violence or a phony independence referendum. A handful of such unacknowledged forces, whom Putin referred to as "little green men" after they appeared in Crimea, would perhaps be dressed as local volunteers or a far-right gang; they might be joined by vigilantes, as they were in eastern Ukraine. They would almost certainly be aided by a wave of Russian propaganda, making it harder for outsiders to differentiate unmarked Russian troops from civilian volunteers, to determine who was fighting where and had started what. Such an intervention would force NATO into an impossible choice: Are you really going to open fire on some hoodlums stirring up trouble in Estonia, knowing they might actually be unmarked Russian troops? Would you risk the first major European war since 1945, all to eject some unmarked Russian troops from the Estonian town of Narva? Putin, Piontkovsky believes, is gambling that the answer is no. That NATO would not intervene, thus effectively abandoning its commitment to defend its Eastern European member states. Piontkovsky's scenario, once considered extreme, is now widely seen by Western security experts and policymakers as plausible. At the end of 2014, the military intelligence service of Denmark, a member of NATO, issued a formal paper warning of precisely that: Russia may attempt to test NATO’s cohesion by engaging in military intimidation of the Baltic countries, for instance with a threatening military build-up close to the borders of these countries and simultaneous attempts of political pressure, destabilization and possibly infiltration. Russia could launch such an intimidation campaign in connection with a serious crisis in the post-Soviet space or another international crisis in which Russia confronts the United States and NATO. "The concern is that what Putin wants to do is break NATO, and the best way to do that would be to poach on the Baltics," Saideman, the political scientist, told me on a call from a European security conference where he said the scenario was being taken very seriously. "And if Germany doesn’t respond to incursions in the Baltics, if France doesn’t respond and it’s just an American operation, then it will lead to the breaking of NATO, is the theory," he said. "That’s the biggest concern." Saideman described a variation on this scenario that I heard from others as well: that Putin might attempt to seize some small sliver of the Baltics quickly and bloodlessly. This would make it politically easier for Western European leaders to do nothing — how to rally your nation to war if hardly anyone has even been killed? — and harder to counterattack, knowing it would require a full-scale invasion. "I think they’re very serious about this," Saideman said. "There’s a real concern." VI. How it would happen: The fog of hybrid war In early 2015, Pew pollsters asked citizens of several NATO states the exact question that analysts and policymakers from Washington to Moscow are gaming out: "If Russia got into a serious military conflict with one of its neighboring countries that is our NATO ally, do you think our country should or should not use military force to defend that country?" The numbers from Western Europe were alarming: Among Germans, only 38 percent said yes; 58 percent said no. If it were up to German voters — and to at least some extent, it is — NATO would effectively surrender the Baltics to Russia in a conflict. This poll is even worse than it looks. It assumes that Russia would launch an overt military invasion of the Baltics. What would actually happen is something far murkier, and far more likely to leverage European hesitation: the playbook from Ukraine, where Russia deployed its newly developed concepts of postmodern "hybrid war," designed to blur the distinction between war and not-war, to make it as difficult as possible to differentiate grassroots unrest or vigilante cyberattacks from Russian military aggression. Putin may already be laying the groundwork. In March of 2014, shortly after Russia had annexed Crimea, Putin gave a speech there pledging to protect Russians even outside of Russia, which many took as a gesture to the substantial Russian minorities in the Baltics. "That kind of misperception situation is definitely possible, and that’s how wars start" Then, in October, Putin warned that "open manifestations of neo-Nazism" had "become commonplace in Latvia and other Baltic states" — repeating the language that he and Russian state media had earlier used to frighten Russian speakers in Ukraine into taking up arms. This April, several Russian outlets issued spurious reports that Latvia was planning to forcibly relocate ethnic Russians into Nazi-style ghettos — an echo of similar scaremongering Russian propaganda broadcast in the runup in Ukraine. Martin Hurt, a former senior official of the country's defense ministry, warned that his country's ethnic Russian minority could be "receptive to Kremlin disinformation." Moscow, he said, could generate unrest "as a pretext to use military force against the Baltic states." In early 2007, Estonia's parliament voted to relocate a Soviet-era military statue, the Bronze Soldier, that had become a cultural symbol and annual rallying point for the country's ethnic Russians. In response, Russian politicians and state media accused the Estonian government of fascism and Nazi-style discrimination against ethnic Russians; they issued false reports claiming ethnic Russians were being tortured and murdered. Protests broke out and escalated into riots and mass looting. One person was killed in the violence, and the next day hackers took many of the country's major institutions offline. Russia could do it again, only this time gradually escalating further toward a Ukraine-style conflict. NATO is just not built to deal with such a crisis. Its mutual defense pledge, after all, rests on the assumption that war is a black-and-white concept, that a country is either at war or not at war. Its charter is from a time when war was very different than it is today, with its many shades of gray. Russia can exploit this flaw by introducing low-level violence that more hawkish NATO members would consider grounds for war but that war-averse Western European states might not see that way. Disagreement among NATO's member states would be guaranteed as they hesitated over where to declare a moment when Russia had crossed the line into war. Meanwhile, Russian state media, which has shown real influence in Western Europe, would unleash a flurry of propaganda to confuse the issue, make it harder to pin blame on Moscow for the violence, and gin up skepticism of any American calls for war. Germany, which is widely considered the deciding vote on whether Europe would go to war, would be particularly resistant to going to war. The legacy of World War II and the ideology of pacifism and compromise make even the idea of declaring war on Russia unthinkable. German leaders would come under intense political pressure to, if not reject the call to arms, then at least delay and negotiate — a de facto rejection of NATO's collective self-defense. In such a scenario, it is disturbingly easy to imagine how NATO's European member states could split over whether Russia had even crossed their red line for war, much less whether to respond. Under a fog of confusion and doubt, Russia could gradually escalate until a Ukraine-style conflict in the Baltics was foregone, until it had marched far across NATO's red line, exposing that red line as meaningless. But the greatest danger of all is if Putin's plan were to stumble: By overreaching, by underestimating Western resolve to defend the Baltics, or by starting something that escalates beyond his control, it could all too easily lead to full-blown war. "That kind of misperception situation is definitely possible, and that’s how wars start," Saideman said, going on to compare Europe today with 1914, just before World War I. "The thing that makes war most thinkable is when other people don’t think it’s thinkable." In 1963, a few months after the Cuban missile crisis had almost brought the US and Soviet Union to blows, President John F. Kennedy gave a speech drawing on the lessons of the world's brush with nuclear war: "Above all, while defending our vital interests, nuclear powers must avert those confrontations which bring an adversary to a choice of either a humiliating retreat or a nuclear war." That is the choice that Putin may well force upon NATO. VII. How it would happen: The Ukraine scenario Evgeny Buzhinsky has spent much of his professional life with the threat of global nuclear destruction hanging over his head. A lifelong Russian military officer, he earned his PhD in military sciences in 1982, just as the Cold War entered one of its most dangerous periods, and rose to the General Staff, where he remained for years after the Soviet Union's collapse, through periods of calm and of tension. He retired in 2009 as a lieutenant general and remains active in Russian national security circles, now heading the PIR Center, a well-respected Russian think tank that focuses on military, national security, and arms control issues. Buzhinsky, when I met him in Moscow, had a warning for me. Those in the West who worried about the possibility of a major war breaking out in the Baltics were missing the real threat: Ukraine. The US, he feared, does not appreciate how far Russia is willing to go to avoid a defeat in Ukraine, and this miscalculation could pull them into conflict. "Ukraine, for Russia, is a red line," he warned. "And especially a Ukraine that is hostile to Russia is a definite red line. But the US administration decided that it's not." This was a concern I heard more than once in Russia. When Fyodor Lukyanov, the Moscow foreign policy insider, warned that Russian foreign policy officials saw a major war as increasingly possible, and I asked him how they thought it would happen, he cited Ukraine. "For example, massive military help to Ukraine from the United States — it could start as a proxy war, and then ..." he trailed off Lukyanov worried that the US does not understand Russia's sense of ownership over Ukraine, the lengths it would go to protect its interests there. "It’s seen by many people as something that’s actually a part of our country, or if not part of our country then a country that’s absolutely essential to Russia’s security," he said. Buzhinsky is one of those people. Like Lukyanov and other Russian analysts, he worried that the United States had wrongly concluded that Putin would ultimately acquiesce if he faced likely defeat in Ukraine. The Americans, he said, were dangerously mistaken. Gregarious, bear-sized, and clearly accustomed to dealing with Westerners from overseeing arms control treaties during much of the 1990s, Buzhinsky sipped a grapefruit juice when we met in downtown Moscow. "A year ago, I was absolutely convinced Russia would never intervene militarily," he said about the possibility of a full, overt Russian invasion of Ukraine. "Now I'm not so sure." The view of the Russian government, he said, was that it could never allow the defeat of the pro-Russia separatist rebels in the eastern Ukraine region sometimes called Donbas. (In August, when those rebels appeared on the verge of defeat, Russia provided them with artillery support and covertly sent troops to fight alongside them, none of which Moscow has acknowledged.) If Ukrainian forces were about to overrun the separatist rebels, Buzhinsky said, he believed that Russia would respond not just with an overt invasion, but by marching to Ukraine's capital of Kiev. "A massive offensive on the Ukrainian side" against the rebels, he said, would lead Russia to openly enter the war. "A war with Russia in Ukraine — if Russia starts a war, it never stops until it takes the capital." When I asked Buzhinsky if he really believed Putin would launch a full Russian invasion of Kiev in response to a Ukrainian effort to retake Donbas, he answered, "Yes, definitely. He said twice publicly, 'I won't let it happen.' As he is a man of his word, I am sure he will." Such a scenario, he said, could lead to a larger conflict no one wants. The Americans believe that "Russia will never dare, Putin will never dare, to interfere," leaving the US unprepared in case it should happen. "And then I could not predict the reaction of the United States and NATO." Buzhinsky outlined another way he feared Ukraine could lead to a larger war. If the US provided sophisticated military equipment to Ukraine that required putting American trainers or operators near the front lines, and one of them was killed, he believed the US might feel compelled to intervene outright in Ukraine. Would Russia really risk a major war over Ukraine, one of Europe's poorest countries? For months, Moscow has been suggesting that Western military involvement in Ukraine, even something as mild as providing the Ukrainian military with certain arms, would be taken as an act of war against Russia. Like Putin's threats to use nuclear weapons, this has been shrugged off as bluster, mere rhetoric, just for scoring domestic political points. What Buzhinsky was trying to underline to me was that the threats are real — that Russia might consider its interests in Ukraine so vital that it would risk or even fight a war to protect them. He was not alone in saying this — I heard it from many others in Moscow, including Russian analysts who are critical of their country's Ukraine policy as too aggressive. Buzhinsky explained that Russia had set this as a red line out of the fear that a Ukrainian reconquest of eastern Ukraine would lead to "the physical extermination of the people of Donbas," many of whom are Russian speakers with cultural links to Russia. Russian state media has drilled this fear into the peoples of Ukraine and Russia for a year now. It does not have to be true to serve as casus belli; Moscow deployed a similar justification for its annexation of Crimea. "You don't get to walk this back" The connection to Ukraine is often expressed by everyday Russians as an issue of cultural heritage; Kievan Rus, a medieval Slavic federation with its capital in the present-day Ukrainian capital of Kiev, is something like Russia's predecessor state. But this is likely about more than nationalism or kinship with Russian-speaking Ukrainians. Moscow is notorious for its conviction that the US is bent on Russia's destruction, or at least its subjugation. It is paranoid and painfully aware of its isolation and its comparative weakness. A hostile and pro-Western Ukraine, Putin may have concluded, would pose an existential threat by further weakening Russia beyond what it can afford. Allison and Simes, in their essay on the risk of war, described Ukraine as a potential ground zero for wider conflict because of this. "Russia’s establishment sentiment holds that the country can never be secure if Ukraine joins NATO or becomes a part of a hostile Euro-Atlantic community," they wrote. "From [Moscow's] perspective, this makes Ukraine’s non-adversarial status a non-negotiable demand for any Russia powerful enough to defend its national-security interests." It is practically a cliché in international relations: "Russia without Ukraine is a country, Russia with Ukraine is an empire." Putin's Russia appears to believe that reclaiming great-power status is the only way it can guarantee security against a hostile West. Jeffrey Lewis, an arms control expert, traced this Russian government obsession with Ukraine back to Putin's political weakness at home, as well as Russia's sense of military insecurity against a hostile and overwhelmingly powerful West. "I suspect that the desire to unite the Russian world and to subjugate the non-Russian neighbors is driven by a fundamental sense of insecurity," Lewis said in a much-circulated September podcast on Putin's nuclear threats. "That, like the Soviet leadership, he has to try very hard to stay in power, and so there’s a tendency as his legitimacy declines to try to blame outside forces. And the problem is that when you try to look at the world in that conspiratorial way, there’s always a justification for subjugating the next set of neighbors." This means that should the US or other Western countries become sufficiently involved in Ukraine that Russia cannot maintain control of the conflict, then Russia may feel this puts it at such existential threat that it has no choice but to escalate in response. Even at the risk of war. Russia knows it would lose a full-blown war with NATO, of course, but it has other options. An official with the Russian Defense Ministry's public advisory board told the Moscow Times that should Western countries arm Ukraine's military, it would respond by escalating in Ukraine itself as well as "asymmetrically against Washington or its allies on other fronts." Russian asymmetrical acts — cyberattacks, propaganda operations meant to create panic, military flights, even little green men — are all effective precisely because they introduce uncertainty and risk. If that sounds dangerous, it is. American and NATO red lines for what acts of "asymmetry" would and would not trigger war are unclear and poorly defined. Russia could easily cross such a line without meaning to, or could create enough confusion that the US believes it or its allies are under a severe enough threat to demand retaliation. "You don't get to walk this back," Matthew Rojansky, the director of the Kennan Institute, warned in comments to the New York Times about what could happen if the US armed Ukraine's military, as Congress is pushing Obama to do. "Once we have done this we become a belligerent party in a proxy war with Russia, the only country on Earth that can destroy the United States," Rojansky said. "That’s why this is a big deal." VIII. The nuclear dangers: The red line is closer than you think This August, as the Russian military launched its undeclared and unofficial invasion of eastern Ukraine to defend separatist rebels there against defeat, Putin attended an annual youth conference at Lake Seliger, just north of Moscow. During a Q&A session, a teaching student asked an odd question about the "cyclical" nature of history and concerns that Russia could be "drawn into a new, open global conflict." Putin, in his answer, did something that the leaders of major nuclear powers generally avoid doing — he rattled the nuclear saber a bit: Let me remind you that Russia is one of the world’s biggest nuclear powers. These are not just words — this is the reality. What’s more, we are strengthening our nuclear deterrent capability and developing our armed forces. They have become more compact and effective and are becoming more modern in terms of the weapons at their disposal. There is a certain fear in Russia, never far from the surface, that the only thing preventing the West from realizing its dream of destroying or subjugating Russia is its nuclear arsenal. (Three months later, Putin warned that the West wanted to tame the Russian bear so as to "tear out his fangs and his claws," which he explained meant its nuclear weapons.) "There is a widespread belief that the only guarantee for Russian security, if not sovereignty and existence, is the nuclear deterrent," Lukyanov, the Russian foreign policy expert, explained. "After the Yugoslavia wars, Iraq War, Libyan intervention, it’s not an argument anymore, it’s conventional wisdom: 'If Russia were not a nuclear superpower, the regime change of an Iraqi or Libyan style would be inevitable here. The Americans are so unhappy with the Russian regime, they would do it. Praise God, we have a nuclear arsenal, and that makes us untouchable.'" But Russia faced a problem: Its conventional military forces are now so much weaker than NATO's, and its capital city so close to NATO's forces in the Baltics, that it feared NATO tank divisions could push all the way to Moscow and quickly win a war without ever using a nuclear weapon. Both the US and Russia had pledged to use nuclear weapons only to deter one another from nuclear attacks. This kept the Cold War cold. But because the US would not need its ICBMs to win a war, that deterrence is no longer enough to keep Russia safe. In response, Russia has been gradually lowering its bar for when it would use nuclear weapons, and in the process upending the decades-old logic of mutually assured destruction, adding tremendous nuclear danger to any conflict in Europe. The possibility that a limited or unintended skirmish could spiral into nuclear war is higher than ever. Russia's nuclear doctrine, a formal document the Kremlin publishes every few years outlining when it will and will not use nuclear weapons, declares that the Russian military can launch nuclear weapons not just in the case of a nuclear attack, but in case of a conventional military attack that poses an existential threat. In other words, if Russia believes that American tanks could be bound for the Kremlin, it has declared it may respond by dropping nuclear bombs. The danger that this adds to any possible confrontation, particularly along the Baltic states, is difficult to overstate. If an accident or miscalculation were to lead to a border skirmish, all it would take is for the Kremlin to misperceive the fighting as the beginning of an assault toward Moscow and its own doctrine would call for using nuclear weapons. Indeed, it would be the only way to avoid total defeat. There is another layer of danger and uncertainty to this: It is not clear what Russia would consider a conventional threat worthy of a nuclear response. A few months after he'd annexed Crimea, Putin revealed that during Russia's undeclared invasion of the territory he had considered putting his country's nuclear forces on alert; his government has signaled it would consider using nuclear force to defend Crimea from an attack, something Russian analysts told me was not just bluster. The United States, of course, has no intention of militarily retaking Crimea, despite surprisingly common fears to the contrary in Russia. But Russian paranoia about such a threat, and a possible willingness to use nuclear weapons to avert it, adds more danger to the already dangerous war in eastern Ukraine and the fears that greater Russian or Western involvement there could spark a broader conflict. And the Crimea revelation raises a disconcerting question: Where exactly does Moscow place the line for a threat severe enough to use nuclear weapons? Its doctrine says they should be used only against an existential threat, but an attack on Crimea would be far from existentially dangerous. We can only guess where the real red line lays, and hope not to cross it by mistake. IX. The nuclear dangers: How Putin is pushing us back to the brink There is a specific moment that arms control experts often cite to highlight the dangers of nuclear weapons, how they kept the world poised, for years at a time, mere minutes away from nuclear devastation. That moment was September 26, 1983. That evening, a Russian lieutenant colonel named Stanislav Petrov settled in for his shift overseeing the Soviet Union's missile attack early warning system. Petrov had a top-secret network of satellites, all pointed squarely at the United States and its arsenal of nuclear-armed intercontinental ballistic missiles, which pointed back at him. The US and Soviet Union were ramping up development of ICBMs, which could circle the globe in 30 minutes and reduce an enemy city to ash. Both sides were driven by fear that the other could one day gain the ability to launch a preemptive nuclear strike so devastating and so fast that it would start and win the war within hours. Each sought to develop ever more sensitive warning systems, and ever more rapid mechanisms for retaliation, to deter the threat. Petrov ran one such warning system. If he caught an American attack as soon as it crossed his sensors, it would give the Soviet leadership about 20 minutes of warning time. That was their window to determine how to respond. The space for mistakes was effectively zero. Five hours into Petrov's shift that night, something he had never encountered in his 11-year career happened: The system went into full alarm. The word "LAUNCH" displayed in large red letters. The screen announced a "high reliability" of an American ICBM barreling toward the Soviet Union. Petrov had to make a decision: Would he report an incoming American strike? If he did, Soviet nuclear doctrine called for a full nuclear retaliation; there would be no time to double-check the warning system, much less seek negotiations with the US. If he didn't, and he was wrong, he would have left his country defenseless, an act tantamount to treason. His gut instinct told him the warning was in error, but when he flipped through the incoming imagery and data and he could reach no hard conclusion from it. After a few moments, he called his superiors and stated categorically that it was a false alarm. There was, he insisted, no attack. Petrov waited in agony for 23 minutes — the missile's estimated time to target — before he knew for sure that he'd been right. Only a few people were aware of it at the time, but thanks to Petrov, the world had only barely avoided World War III and, potentially, total nuclear annihilation. The US and Soviet Union, shaken by this and other near-misses, spent the next few years stepping back from the brink. They decommissioned a large number of nuclear warheads and signed treaties to limit their deployment. One of their most important measures was a 1987 agreement called the Intermediate-Range Nuclear Forces (INF) Treaty, which saw both sides conclude that the medium-range, land-based nuclear missiles they'd stuffed across Europe were simply too dangerous and destabilizing to be allowed. Because the missiles could reach Moscow or Berlin or London at lightening speeds, they shortened the "response time" to any crisis — the window in which a Soviet or Western leader would have to decide whether the country was under attack before such an attack would hit — to just a few minutes. They made the danger of an unintended escalation, or of an error like the that one Petrov only barely prevented, far greater. The risk they posed was deemed, in the 1987 INF Treaty, unacceptable to the world. And the weapons were removed. Putin has taken several steps to push Europe back toward the nuclear brink, to the logic of nuclear escalation and hair-trigger weapons that made the early 1980s, by many accounts, the most dangerous time in human history. Perhaps most drastically, he appears to have undone the 1987 INF Treaty, reintroducing the long-banned nuclear weapons. In March, Russia announced it would place nuclear-capable bombers and medium-range, nuclear-capable Iskander missiles in the Russian enclave of Kaliningrad — only an hour, by commercial airliner, from Berlin. Meanwhile, it has been testing medium-range, land-based missiles. The missiles, to the alarm of the United States, appear to violate the INF Treaty. This is far from Putin's only nuclear escalation. He is developing more nuclear weapons, and calling frequent attention to them, as apparent cover for his aggression and adventurism in Europe. There are suspicions, for example, that Russia may have deployed nuclear-armed submarines off of the US Eastern Seaboard. What makes this so dangerous is that Putin appears to believe, as the scholar Edward Lucas outlined in a recent report for the Center for European Policy Analysis, that he has a greater willingness than NATO to use nuclear weapons, and thus that his superior will allows him to bully the otherwise stronger Western powers with games of nuclear chicken. This is a substantial, and indeed terrifying, break from Cold War–era nuclear thinking, in which both sides rightly feared nuclear brinksmanship as too dangerous to contemplate and used their weapons primarily to deter one another. "Russia’s nuclear saber-rattling is unjustified, destabilizing and dangerous," NATO Secretary-General Jens Stoltenberg said in a May speech in Washington. Putin is acting out of an apparent belief that increasing the nuclear threat to Europe, and as a result to his own country, is ultimately good for Russia and worth the risks. It is a gamble with the lives of hundreds of millions of Europeans, and perhaps many beyond, at stake. X. The nuclear dangers: An atomic gun to the world's head The view among many Western analysts is that the nuclear-capable missiles are meant as a gun against the heads of the Americans and the Europeans: You better not mess with us Russians, or who knows what we'll do. Putin himself endorsed this view in a 2014 speech in Sochi, where he approvingly cited Soviet leader Nikita Khrushchev's 1960 address to the United Nations, when he hammered his shoe on the podium. "The United States and NATO thought, 'This Nikita is best left alone, he might just go and fire a missile. We better show some respect for them,'" Putin said. This sort of a nuclear threat could be a perfect way for Putin to attempt the sort of NATO-splitting scenario described by analysts like Piontkovsky. What if, Lucas asked as an example in his report, Putin found some excuse to declare a Russian "military exclusion zone" in the Baltic Sea, thus physically cutting off the Baltic states from the rest of NATO? "Would America really risk a nuclear standoff with Russia over a gas pipeline?" Lucas asked. "If it would not, NATO is over. The nuclear bluff that sustained the Western alliance through all the decades of the Cold War would have been called at last." Putin's love of brinksmanship, while perhaps born of Russia's weakness, is also deeply worrying for what it says about the leader's willingness and even eagerness to take on huge geopolitical risk. "Either he has a very weird theory of nuclear weapons, or he just doesn’t take the West seriously and is trying to cow us with whatever threat he can make," Saideman, the political scientist, said, going on to draw yet another of the many parallels analysts have drawn to the onset of World War I. "There are two visions of international relations: One is that threats work, and one is that threats don’t, where they cause counter-balancing," Saideman continued. "This was the theory of the [German] Kaiser before World War I: the more threatening you are, the more people will submit to your will. That might be Putin’s logic, that he’s just going to threaten and threaten and hope that NATO bends. But the long run of international relations suggests that it goes the other way, where the more threatening you are the more you produce balancing." In other words, Putin is hoping to compensate for his weakness by expressing his willingness to go further, and to raise the stakes higher, than the more powerful Western nations. But his actions are premised on a flawed understanding of how the world works. In fact, he is virtually forcing the West to respond in kind, raising not just the risk of a possible war, but the ease with which such a war would go nuclear. XI. The nuclear dangers: Does Putin believe nuclear war can be "won"? There is a corollary in Russia's nuclear doctrine, a way in which the Russians believe they have solved the problem of Western military superiority, that is so foolhardy, so dangerous, that it is difficult to believe they really mean it. And yet, there is every indication that they do. That corollary is Russia's embrace of what it calls a "de-escalation" nuclear strike. Go back to the scenario spelled out in Russia's military doctrine: a conventional military conflict that poses an existential threat to the country. The doctrine calls for Russia to respond with a nuclear strike. But imagine you're a Russian leader: How do you drop a nuclear bomb on NATO's troops without forcing the US to respond with a nuclear strike in kind, setting off a tit-for-tat cycle of escalation that would end in total nuclear war and global devastation? Russia's answer, in the case of such a conflict, is to drop a single nuclear weapon — one from the family of smaller, battlefield-use nukes known as "tactical" weapons, rather than from the larger, city-destroying "strategic" nuclear weapons. The idea is that such a strike would signal Russia's willingness to use nuclear weapons, and would force the enemy to immediately end the fight rather than risk further nuclear destruction. Nikolai Sokov, a nuclear weapons expert and former official in the Russian Foreign Affairs Ministry, explained in the Bulletin of Atomic Scientists that this is not a far-fetched option of last resort; it has become central to Russian war planning. "Such a threat is envisioned as deterring the United States and its allies from involvement in conflicts in which Russia has an important stake, and in this sense is essentially defensive," Sokov wrote. "Yet, to be effective, such a threat also must be credible. To that end, all large-scale military exercises that Russia conducted beginning in 2000 featured simulations of limited nuclear strikes." Buzhinsky, the recently retired member of Russia's General Staff, confirmed in our meeting that this is something the military sees as a viable option. "If Russia is heavily attacked conventionally, yes, of course, as it's written in the doctrine, there may be limited use of nonstrategic nuclear weapons," he said. "To show intention, as a de-escalating factor." It is difficult to imagine a more dangerous idea in the world of military planning today than of a "limited" nuclear war. Scholars have debated for decades, and still debate today, whether the concept of limited nuclear war is realistic, or whether such a conflict would inevitably spiral into total nuclear war. Put another way, no one knows for sure whether Russia's military planners have sown the seeds for global nuclear destruction. Seen from the Russian side, it is at least possible to imagine how this doctrine might make sense: The threat of NATO's conventional forces is widely seen as both overwhelming and imminent, making such an extreme step worth considering. Ever since the fall of the Soviet Union, Russia's strategic culture has increasingly emphasized its nuclear arsenal, the one remaining legacy of its fearsome great-power status. It is a sort of Russian cult of the nuclear weapon, or even a certain strategic fetish. With nukes so central to Russian strategic thinking, it is little wonder Moscow sees them as the solution to its greatest strategic problem. But when you consider this doctrine from the American side, you begin to see what makes it dangerous, even insane. Imagine that you are an American leader and your forces in Eastern Europe have somehow been drawn into conflict with the Russians. Perhaps, as artillery and planes from within Russia hammer your forces, you counterattack on Russian soil to take them out. The Kremlin, fearing the start of an invasion to take Moscow, drops a tactical nuclear warhead on your forces in Estonia or Latvia. You have no idea whether more Russian nuclear strikes are coming, either on the battlefield, more widely on Europe, or even against Washington or New York. Do you respond with an in-kind tactical nuclear strike, opening the risk of gradual escalation to total nuclear war? Do you, fearing the worst, move to take out the Russian leadership before they can order more attacks? Or do you announce a unilateral ceasefire, drawing your forces back in humiliation, rewarding Russia with a victory? It is difficult to imagine a more dangerous idea than "limited" nuclear war Russia's nuclear doctrine is betting that any American leader — not to mention the leaders of nuclear-armed France and the UK — would choose the last of those three options. If that prediction turned out to be wrong, it would mean nuclear war, perhaps global nuclear war and thus annihilation. This doctrine, in other words, is gambling with the fate of the world. Such a scenario, to be clear, is remote, as are all of the nuclear scenarios. It would require a cascading series of events, and for neither side to pull back in time as those events built. The odds of this happening are quite low. But they are greater than zero, and growing. Such a scenario is within the realm of possibility — if it were not, then Russia would not regularly conduct military exercises that imagine exactly this outcome. And recall that Alexander Vershbow, the deputy secretary general of NATO, told a conference in late April that NATO is gaming out exactly such a crisis. There are yet more worrying implications to this Russian doctrine. Its logical conclusion is that Russia sees itself as able to fight a war with the conventionally superior United States without losing, and that it can do this by using battlefield nuclear weapons. Under this doctrine, Moscow is deeming not only full-blown war against the US as imaginable, but a full-blown war with at least one nuclear detonation. That, perhaps, can help explain why Putin has seemed so willing to ratchet up the possibility of a real war with the United States, even one involving nuclear threats — he may believe that through his superior will and brinksmanship, he can avoid defeat. Adding a nuclear element to any conflict would also seem to increase the odds of NATO's Western European members splitting over how to respond, particularly if Russian propaganda can make the circumstances leading up to the detonation unclear. But this also shows the degree to which his entire strategy may rest in part on a shoddy premise — that "limited" nuclear war can be winnable — and one that puts the entire world at risk. XII. The nuclear dangers: End games President Dwight Eisenhower held office at a time when the prospect of a nuclear war was relatively new and military planners unsure how to account for the possibility of a conflict with the Soviet Union in which both sides might use nuclear weapons. Though some in his administration urged him to consider plans for nuclear conflict, Eisenhower, no stranger to war, rejected the idea as unthinkable. "You just can't have this kind of war," Eisenhower said in 1957. "There aren't enough bulldozers to scrape the bodies off the streets." Putin believes he has found a way around this problem, relying on smaller, battlefield-use warheads that could win a war without escalating to a global conflict in which whole cities were sacrificed. But even a limited nuclear war could be catastrophic, and not just for the nations where the bombs would fall, but for the whole world. A 2008 study (updated in 2014) on the environmental effects of a "small" nuclear war described what would happen if 100 Hiroshima-strength bombs were detonated in a hypothetical conflict between India and Pakistan. This is equivalent to less than 1 percent of the combined nuclear arsenals of the US and Russia. The explosions, the study found, would push a layer of hot, black smoke into the atmosphere, where it would envelop the Earth in about 10 days. The study predicted that this smoke would block sunlight, heat the atmosphere, and erode the ozone for many years, producing what the researchers call without hyperbole "a decade without summer." As rains dried and crops failed worldwide, the resulting global famine would kill 1 billion people. "We escaped the Cold War without a nuclear holocaust by some combination of skill, luck and divine intervention, and I suspect the latter in greatest proportion," General George Lee Butler of the US Strategic Air Command told the journalist Eric Schlosser for his book on the dangers of nuclear weapons. We may have escaped the Cold War, but we have not escaped the nuclear threat, which not only remains but is growing. The sense that this danger is resigned to history books, common in Washington and other Western capitals, is precisely part of its danger. It is another echo of the months and years before World War I, when the world drifted unknowingly toward disaster. In April of last year, just after Russia had annexed Crimea, the London-based think tank Chatham House published a report on the dangers of unintended nuclear conflict. It was not pegged to the events in Ukraine, and at that point few people, including the report's authors, saw Crimea as the potential beginning of a larger conflict. Even still, it was dire in its warnings. "The probability of inadvertent nuclear use is not zero and is higher than had been widely considered," it stated. "The risk associated with nuclear weapons is high" and "under-appreciated." Their warnings were widely ignored. As the report itself noted, the world has concluded, wrongly, that nuclear weapons no longer pose an imminent threat. Attention has moved on. But the seeds of a possible war are being sown in Europe. Should the worst happen, which is a remote but real possibility, the consequences will follow all Americans to their homes.

#### Cooperative OCO’s are essential to prevent meltdowns and grid collapse --- Enhanced coop and integration is key

Iftimie, 20 (Ion Iftimie, Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business, 5-28-2020, accessed on 6-17-2022, NDC, "NATO’s needed offensive cyber capabilities", https://www.ndc.nato.int/news/news.php?icode=1441)//Babcii

Cyber as a hybrid threat to, and enabler of, military operations All future **military confrontations** are expected to be **fought** with cyber weapons. These **offensive cyber capabilities** in the hands of **adversaries** pose a **significant threat** to the military forces and **critical infrastructure** of NATO member states; and the Alliance recognizes that cyber-attacks (as hybrid threats) can be as damaging as conventional ones. This is because malicious cyber activities against computers that control physical processes can be as dangerous as threats that are purely physical in nature and could lead to explosions, **nuclear meltdowns, blackouts, or financial crises**. As put by NATO Secretary General, “in just minutes, a single cyberattack can inflict billions of dollars’ worth of damage to our economies, bring global companies to a standstill, ~~paralyze~~ **(destroy) our critical infrastructure**, undermine our democracies and ~~cripple~~ **(undermine) our military capabilities**”.4 Over the past decade, Allies have identified a steep increase in cyber activities targeting the critical infrastructure sectors that NATO military operations rely upon. Directly or indirectly, these malicious cyber activities can also disrupt the Alliance’s logistics and forward operations. NATO’s commitment to “operate and defend itself ”5 in the cyber domain as effectively as in the geographic domains came, thus, as a direct recognition of cyber as a hybrid threat to both the Allies and the Alliance. Compared to the air, land and sea domains, the cyber domain is not constrained by national borders (although certain physical aspects of it might be located within them). This distinction between the cyber and the geographic domains is important to note, because NATO was founded in response to external military threats without the right to intervene in internal security matters, where member states maintain the monopoly over the use of force. In the cyber domain, the distinction between internal and external security threats is harder to ascertain. When integrating offensive cyber capabilities into its defence and deterrence mandate, NATO would inevitably tackle certain aspects inherent to internal security; and yet, not legally infringe on the sovereignty of the Allies as long as effects amounting to force or intervention are not employed against the physical systems residing in these nations.6 Operating in the cyber domain requires, thus, that member states better integrate their offensive cyber capabilities into NATO operations not just **to win future wars**, but also to avoid elements of friction between Allies, which may arise from unilateral cyber effects to defend critical infrastructure. NATO’s adversaries in the cyber domain Warfare in the cyber domain is already conducted against NATO member states by both state and nonstate actors. It is also conducted by NATO member states against these external threats. Within the Alliance, however, offensive cyber effects are not yet part of the mission planning process and integration of national offensive cyber capabilities into joint NATO operations is voluntary. Integrating these national offensive cyber capabilities into NATO operations, thus requires, not only a clear understanding of these capabilities, but also agreement on the cyber threat environment, characterized by the intent and capabilities of NATO’s current and/or potential future adversaries. State adversaries in the cyber domain include Russia, China and/or Iran. These are countries known to be building offensive cyber capabilities specifically for the purpose of using them against NATO member states.7 In Russia’s case, cyber attacks were conducted against the critical infrastructure of NATO member states and partner nations, as for example against US energy infrastructure in 2017 (including against a nuclear powerplant near Burlington, Kansas)8 or against the Ukraine power grid in December 2015. China has also been conducting persistent cyber espionage using offensive cyber capabilities against core military and critical infrastructure of NATO member states for years. For this reason, the US Secretary of Defense, Mark T. Esper, remarked at the 2020 Munich Security Conference that the 5G Huawei infrastructure is a serious threat to NATO.9 Lastly, Iran’s offensive cyber capabilities have also been observed during multiple attacks against the critical infrastructure of NATO partner nations in the Middle East.

**Meltdowns cause extinction.**

Majia **Nadesan 14**, professor of communication at ASU, their interdisciplinary research examines the ethical implications of societal governing logics and risk-management strategies, 9/13/14, "The Nuclear Energy Paradigm Collides with Earth Changes and Technospheric Breakdown", Will Fukushima Become An Extinction Level Event?, The Millenium Report, themillenniumreport.com/2014/09/will-fukushima-become-an-extinction-level-event/

**As Technospheric Breakdown Accelerates, Nuclear** Power Generation **Mishaps will Increase and Intensify** There is really no way around this eventuality. As all the nuclear power plants age, they will succumb to the **micro-stresses** which **inevitably** occur in such **a**n ever-**deteriorating environment**. Most people are **unaware** of the true depth and breadth of technospheric breakdown since it is a concept **rarely taken up by academia** or the media. The following excerpts provide a wider perspective of this unavoidable byproduct of the Industrial Revolution. Technospheric breakdown is something that occurs **everywhere** around the globe, **24/7**, without interruption, and with tremendous repercussions. Let’s start with anything that has been manufactured in the factories of the modern world or built on the surface of the Earth. Simply put, everything is in the constant state of breaking down, degeneration, deterioration. What does this really mean when we say that every bridge is slowly breaking down, every road is in greater disrepair with each passing day, every reservoir is gradually degrading, every office building, every factory, every school, every home, etc. most of which adhered to very low building standards in the first place? What does it mean when the infrastructure for every sewer system, municipal water division, electrical grid, airport, railway station, etc. is in a slow but sure process of degrading and breaking down. So, unfortunately, is **every nuclear power plant across the planet**. (Cosmic Convergence) What makes this ongoing process of physical degradation so insidious is that it almost always occurs **subliminally**. Through a gathering array of various forces throughout post-modern civilization, there does exist a sort of conspiracy of circumstances which has greatly magnified the effects of technospheric breakdown. The completed marriage between the industrial base of the Western powers and the financial class throughout the world has guaranteed that this slow motion collapse will continue unabated. How so? Because so many corporate decisions are made according to their impact on the bottom line, many inferior nuclear power plants have been constructed around the globe. Likewise, because the mega-banks and investment houses are now dictating to a financially-strapped Nuclear Energy Industry, **substandard** nuclear **reactors** have been designed, engineered and **continue to be** put **in**to **operation** across the planet. One only has to take a close look at the websites dedicated to decommissioned nuclear reactors or cold shutdowns or partially closed nuclear power plants or emergency actions taken at various nuclear power generation sites to grasp just how precarious a position the entire industry is currently in. Unknown to even many of the nuclear engineers who address these issues ‘in the office’, or who fix the cascade of problems at nuke plants themselves, is the notion of slow motion, subclinical, pernicious technospheric breakdown. It often manifests in ways where cause and effect cannot be easily established because of some of the unseen forces produced by atomic fission. With that said, it should be noted that a chapter could easily be dedicated to this particular issue alone, so significant is it to the future of nuclear power generation Then there is the problem of **nuclear wastes** and natural rights, yes? No one has articulated this point better than Albert Bates in his definitive essay entitled The Karma of Kerma: Nuclear Wastes and Natural Rights (Bates, A.K., 1988) This extremely lucid and illuminating, sober and sane treatment of the **greatest ongoing environmental disaster** of our times lays bare the most basic legal and human rights issues which converge around the production, treatment and storage of nuclear wastes. Were the governments of the world to read and take to heart its simple and straightforward thesis, the current incarnation of nuclear energy production would have been abandoned years ago: The disposal of radioactive substances in a manner that anticipates their eventual partial release into the human environment imposes a **health burden** upon **future generations** that **cannot be justified** by any moral or legal rationale. Like an irresistible force meeting an immovable object, the concept of the greater good for the many in the present generation runs against the concept of the inalienable rights of each individual in future eras. At present, in matters involving nuclear power, our governmental agencies have taken the side of the irresistible force. But when federal agencies venture to tread beyond of the scope of the foundation principles with which the federal government was fashioned, they endanger more than human lives. At risk in the nuclear waste debate are long-held concepts of ordered liberty. (Bates A. K., 1988) Fukushima has illustrated exactly why this elegantly stated legal concept of human rights and moral imperative is so pertinent to the public discourse. When massive amounts of radioactive wastewater are dumped into the Pacific Ocean, not only **human life** will be adversely affected. Marine life has been negatively impacted in ways that will take decades to observe and comprehend. The outright destruction of the environment in and around Fukushima and the Pacific Ocean must also be considered in any meaningful assessment of collateral damage. Perhaps even more than Chernobyl, Fukushima has allowed the global community to view the whole event through the lens of legal responsibility and ethical outcomes so that new international standards can be written and implemented regarding nuclear waste conveyance and disposal. If nothing else, this discussion has raised awareness about the most nagging issue concerning the NEP. Whereas the human rights aspect confers the legal right to not be contaminated by nuclear radiation has barely been addressed by those responsible for it consequences, it now enjoys a prominent place throughout the worldwide debate. Accidents and mishaps, manmade and natural disasters happen. Things are fixed fairly quickly in this postmodern age, and life goes on. Whether these events occur in a full-blown war zone or in the wake of a hurricane, the affected population usually does everything it can to rebuild and move on. However, when these events take place in or near nuclear power plants, **life** doesn’t just go on. It often **stops**. Depending on the circumstances and seriousness of a nuclear event, sometimes life stops in that area for a long time. Our **civilization** has now been given three unmistakable **wakeup calls** since the advent of the nuclear power generation era. First there was Three Mile Island in Pennsylvania, then there was Chernobyl in the Ukraine, and lastly the world is still reeling from the specter of possibilities which are presented by Fukushima. Surely it is not by chance that these three flagrant examples of nuclear Perfect Storms occurred around the globe affecting major nations and populations centers. Each of these disasters has served to wake up whole swaths of humanity to the dangers and risks which are associated with the current Nuclear Energy Paradigm. To ignore, or deny, or refute the obvious lessons which all three nuclear catastrophes have given to humankind would be folly of the highest order. The **global impact** of Fukushima, which has disseminated radionuclides (radioactive contaminants) by air and by way of the largest of the seven seas, stands as dramatic testimony to all that can go wrong — seriously wrong — with the current nuclear energy business model and method of power generation. **Can it get any worse** than Fukushima? That we are compelled to even ask this question speaks volumes about the true state of the affairs on that 25 square mile patch of land and contiguous sea which surround the Fukushima Daiichi nuclear disaster site. Given this inescapable testament of nuclear folly, it is now incumbent upon the community of nations to rally around the obvious necessity of terminating the current form of the Nuclear Energy Paradigm. Why? Because when a “China Syndrome” occurs anywhere in the world, **it will inevitably affect the entire planet**. In other words, an INES Level 7 (Wikipedia, International Nuclear Event Scale) nuclear catastrophe does not respect borders. Nor does it discriminate between the young and old, healthy and sick, or those who live close to ground zero from those who live far away. Therefore, any nation that chooses to set up a nuclear energy-producing operation from this point forward has an inviolable responsibility to its neighbors, as it does to the rest of the world. Likewise, those nations have a moral obligation to proceed in a manner that guarantees its neighbors will not be exposed to the consequences of its nuclear accidents, even when they are caused by duel **natural disaster** events as we saw at Fukushima. Just as Europe was contaminated with radiation from Chernobyl (Yablokov, A.V., 2009), and North America has been contaminated from Fukushima, it is understood that once a nuclear catastrophe spirals out of control, the genie of radioactive **contamination cannot be put back in the bottle**. The entire Pacific Rim, in fact, has varying degrees of exposure to the radioactive waste water being conveyed by the ocean from Fukushima, as does the Western Hemisphere to seaborne radioactive isotopes like Cesium-137 and airborne isotopes such as Iodine-131(Center for Marine and Environmental Radiation). Consequently, Japan is responsible for the damage wrought to the largest ocean on Earth. Have they acknowledged this? Have they approached the nations both near and far which have been affected by their cavalier and irresponsible approach to siting reactors up and down their seismic shorelines? Has the United Nations even addressed this extremely important issue known as national accountability? Or territorial sovereignty? Conclusion It doesn’t get very much more weighty than the ‘fallout from Fukushima’. All of the affected nations have been curiously silent on this issue. It is almost as though a conspiracy of silence has descended upon the concerned countries because of how unpredictable and intractable the nuclear containment problems have been at the Daiichi plant. At the end of the day the current race of **humanity** will look back on the Fukushima Nuclear Disaster as the **defining moment** for both the industry and the underlying paradigm. If they haven’t already, the various stakeholders will be forced to re-evaluate the integrity of their nuclear enterprises around the globe. **Hopefully**, they will begin to take aggressive **preemptive measures** to address whatever needs to be addressed at every nuclear site still in operation. If a **decisive response** is not formulated and implemented on a global scale, in light of the hard lessons learned from Fukushima, the current planetary **civilization** will be compelled to face up to these **fatal flaws** in most unpleasant ways, which will continue to manifest with each major Earth change. In a similar way, the inherent defects of the NEP will only be accentuated as technospheric breakdown accelerates. The profound and fundamental shortcomings which pervade the entire nuclear energy industry can no longer be hidden or ignored. After all, it was the dangerous combination of willful blindness and feigned ignorance which got the world into this position in the first place. “Does anyone in their right mind believe that nuclear power plants can ever be designed, engineered or constructed to withstand 9.0 earthquakes followed by 15 meter high tsunamis? Sorry if we offend, but such a display of so deadly a combination of ignorance and arrogance must represent the very height of hubris. Particularly in view of the inevitable consequences which have manifested at Fukushima, how is it that so few saw this pre-ordained and disastrous outcome, except by willful blindness?”

**So does grid collapse.**

Matthew **Weiss and** Martin **Weiss 19**, Matthew Weiss is National Sales Director at United Medical Instruments, UMI and Research assistant at the American Jewish University, Martin Weiss is Neurosurgeon at UCLA-Olive View Medical Center, “An assessment of threats to the American power grid”, 5/29/2019, Energy, Sustainability and Society, Volume 9, No. 18, <https://energsustainsoc.biomedcentral.com/articles/10.1186/s13705-019-0199-y#Sec2>

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

#### DAs are thumped – Everyone already knows the general contours of our OCO’s due to leaks BUT Refusal to integrate them broadly undermines NATO credibility --- Disclosing capabilities is key

Lewis, 15 (James Lewis, Director and Senior Fellow, Strategic Technologies Program, Center for Strategic and International Studies, 2015, accessed on 6-17-2022, NDC, "NATO’s needed offensive cyber capabilities", https://www.ndc.nato.int/news/news.php?icode=1441)//Babcii

Cyber defence has become a central component of NATO planning, given the success of Russia and others in compromising NATO networks. US intelligence sources assess that any unclassified NATO network that is directly connected to the internet should be considered potentially compromised and that cyber espionage is the principle threat to NATO systems over the next three years. They also assess that Russia, given its record of effective cyber collection, poses the greatest espionage threat to NATO computer networks.3 The vulnerable state of many NATO members’ national networks makes defence a priority, but it cannot be the only priority. Discussion within NATO has focused on a defensive role and on the issue of when a cyber incident could trigger the collective defence provision of Article 5 of the North Atlantic Treaty. NATO’s Computer Incident Response Capability (NCIRC), co-located with Allied Command Operations (ACO), is responsible for defending NATO networks. NATO is improving its cyber defence and helping member states improve their own cyber defences through information sharing, training, and if necessary, the deployment of rapid reaction cyber defence teams. **These topics are essential** for planning purposes, but leave NATO in a reactive mode when it comes to cyber warfare.4 **The central question for NATO**’s cyber doctrine is how the **lack of an articulated** offensive **cyber capability** affects its ability to deter or defend. Put another way, **can any military force credibly claim to have advanced capabilities if it does not include** offensive cyber operations in its arsenal? Offensive capabilities, unlike NATO’s current defensive posture, involve deliberate intrusions into opponent networks or systems with the intention of causing disruption, damage or destruction. The question of NATO and offensive cyber capabilities touches on a **range of sensitive political issues** that militate against any change in policy in the near term. The US has always been **overly secretive** about its offensive **cyber capabilities**, even after a flood of media leaks have made the most sensitive doctrine publicly available. This secrecy has carried over into NATO, and is unhelpful in that it increases the likelihood of opponents miscalculating as they consider the risks of using force or coercion against NATO members or interests. A lack of public discourse on offensive cyber operations undercuts the **legitimacy of NATO operations** **by failing to build public understanding**, and leaves NATO open to charges of sinister plots, since **denial of offensive capabilities is not credible** when two NATO members are world leaders in cyber operations. Parallels between cyber operations and nuclear strategy are usually misleading, but cannot always be dismissed. The parallel for NATO is that cyber attack is a “weapon” with both strategic and tactical uses, which only a few NATO members possess. Unlike nuclear weapons, however, the procedures for integrating offensive cyber operations into NATO’s defensive actions **are not at all obvious**, if they exist. NATO will need to describe how the cyber capabilities possessed by a few of its members will support NATO’s defensive activities, and **NATO’s credibility** in defence **requires** some public discussion on the use of offensive **cyber operations.** There has been a confusing debate over the merits of cyber deterrence, but one conclusion that we can draw from this discussion is that both the contribution of cyber operations to deterrence and the ability to deter cyber attack work best when embedded in a larger military force structure. Adding offensive cyber capabilities to NATO’s force structure and response doctrine will increase its deterrent capabilities – by how much is unclear, but what is clear is that a failure to add cyber capabilities will erode a credible deterrent as cyber operations are increasingly embedded into military operations.5 Beyond deterrence, two other factors point to the need for additional consideration of NATO’s public posture on offensive cyber operations. The first is that cyber techniques are essential for the kinds of combat operations that NATO forces may carry out in the future. No modern air force would enter into combat without electronic warfare (EW) capabilities; as cyber and EW merge into a single activity, air operations will require cyber support. The same is true for special forces operations. Offensive cyber capabilities will shape the battlefields of the future. Second, NATO’s **potential opponents** will use **cyber techniques** in new ways, in what some have called “hybrid warfare”.6 These include countries traditionally of concern to NATO, but cyber threats could also come from new actors, such as Iran or North Korea, and proxy or non-state actors such as the Syrian Electronic Army. These nations and groups, using cyber techniques, now have new ways to strike NATO countries. Military doctrine is **changing** as opponents seek to **circumvent** US military power and use a blend of political action and “influence operations”, special forces, proxies and irregular units, unconventional tactics and cyber techniques to apply force to gain their ends. Cyber techniques for political action and “influence operations” are not intended to destroy or disrupt, but rather to put coercive political pressure on targets. This new style of warfare will **challenge planning for mutual defence**. For these reasons, the need for more than defensive or technical cyber capabilities will increase.7

### 1AC --- Adv --- Cohesion

#### Advantage two is COHESION:

#### Diverging OCO policies between NATO members undermines alliance commitments

Max Smeets, 8-6-2021, [Senior Researcher at the Center for Security Studies, "NATO allies’ offensive cyber policy: A growing divide?", The Hague Centre for Strategic Studies, https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/]

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] 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] 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] 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] 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] 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] 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]

Steady divergence

Yet when it comes to the direction of allies’ cyber policy, growing differences are apparent – especially in the development and deployment offensive cyber capabilities. First, even though most states now have – or are in the process of – establishing a cyber command, operational capabilities vastly differ across states. Whereas some governments are increasingly allocating significant resources to conduct cyber operations – and are now starting to benefit from these investments – the majority of allies still run their cyber commands on a budget of a few million a year –an amount that is insufficient for effective operations in the cyber domain.

Secondly, until a few years ago, NATO members’ strategic visions were largely aligned. National cyber strategies shared a common threat focus on operations that could potentially cause major societal havoc, such as taking down the power grid. Allies’ national strategies were also largely unified in their vision to address this threat, discussing the need for deterrence, resilience, and norms. However, this changed with the publication of the US Department of Defense’s strategy on Defend Forward and US Cyber Command’s vision on Persistent Engagement.[8] The United States emphasizes the need to cause friction “wherever the adversary maneuvers,” operating “globally, continuously and seamlessly” (potentially) below the threshold of armed attack. “We must…maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries,” in the words of NSA director and Cyber Command head Gen. Paul Nakasone.[9] Whereas deterrence is about changing your adversary’s cost-benefit calculus, Persistent Engagement is about taking the opportunity away from the adversary to act.[10]

Third, NATO member positions on how international law applies – particularly the obligations of states vis-a-vis sovereignty – are now more divergent than a decade ago. Whereas countries like the Netherlands and France are located on the side of the “sovereignty as a rule” camp, the United Kingdom has taken the position that a remote cyber operation by one state into another’s cyber systems or network does not violate the latter’s sovereignty.

Where to go from here?

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

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

#### Inability of NATO to cohere integration of OCO’s into the alliance risks fracturing the alliance

Iftimie, 20 (Ion Iftimie, Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business, 5-28-2020, accessed on 6-17-2022, NDC, "NATO’s needed offensive cyber capabilities", https://www.ndc.nato.int/news/news.php?icode=1441)//Babcii

NATO Cyber Rapid Reaction teams are already equipped to conduct defensive cyber operations in support of member states if called upon. A mandate of cyber defence and security implies, however, that NATO also starts to engage in active military measures to deny, degrade, disrupt, deceive, or destroy an adversary’s offensive cyber capabilities. This requires the development of not only **offensive cyber A2/AD capabilities by Allies**, but also the restructuring of the NATO command structures, policies, processes (procurement, intelligence, operations, etc.) and engagements needed to integrate them by the Alliance. **NATO coordination** with both national and regional entities charged with cyber security aspects **will, in particular, need to be enhanced**. Many agreements already exist in the realm of defensive cyber at national and regional levels (as seen with the 2016 NATO-EU Technical Arrangement on Cyber Defence), but **political consensus among Allies is missing** on whether they should be expanded to incorporate the collective **use of offensive cyber** A2/AD capabilities. Conclusion The lack of integrated offensive cyber A2/AD capabilities **undermines both the unity of the Alliance and its mandate of defence** and deterrence. On the former, the lack of coordination between Allies during unilateral cyber operations could lead to friction when resulting effects infringe on Allied cyber-physical infrastructures. It could also lead to cyber fratricide, when failure to properly attribute Allied digital personas occurs during these military operations. On the latter, while most Allies are **developing offensive cyber capabilities**, some remain unable to face the growing number of cyber threats unilaterally. Successful defence and deterrence in the cyber domain calls, thus, for ready collective offensive cyber A2/AD capabilities that, when **integrated with NATO operations**, would complement national and/ or regional responses to malicious cyber activities. If and when this integration occurs, NATO Flexible Deterrence Options would also need to be agreed upon in order to signal cyber adversaries that Allies will respond with **one voice** if attacked in the cyber domain. Ultimately, political consensus within the Alliance would still need to be **built on** the type of needed collective offensive cyber capabilities (such as for A2/ AD purposes) and on how to **integrate them** into NATO’s existing operations and missions.

#### Two reasons ---

#### 1---Secrecy---Refusal to disclose capabilities causes internal strife amongst allies --- Undermines faith in the US and NATO that “tears apart the alliance”

Porter and Jordan, 19 (Christopher Porter and Klara Jordan, hristopher Porter is the chief intelligence strategist of cybersecurity company FireEye and a nonresident senior fellow at the Atlantic Council., Klara Jordan is director of the Cyber Statecraft Initiative at the Atlantic Council’s Scowcroft Center for Strategy and Security, 2-14-2019, accessed on 6-17-2022, Lawfare, "Don’t Let **Cyber Attribution Debates Tear Apart the NATO Alliance**", https://www.lawfareblog.com/dont-let-cyber-attribution-debates-tear-apart-nato-alliance)//Babcii

Therein lies the rub. Both formal alliances, such as NATO, and more ad hoc arrangements, such as what the [Cyber Deterrence Initiative](https://www.google.com/url?q=https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-is-strengthening-americas-cybersecurity/&sa=D&ust=1550163045895000&usg=AFQjCNEu7BExy1iQm54r7K7WfRJutMhLHw) [imagines](https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-is-strengthening-americas-cybersecurity/), will require members to share intelligence and eventually, to the best of their ability and perhaps in different domains, contribute to joint action against a presumably well-armed foreign aggressor. **States including the United States**, the United Kingdom, the Netherlands, Estonia, and Denmark have publicly declared their willingness to lend sovereign offensive cyber effects to deter, defend against and counter the full spectrum of threats. Sharing intelligence and information is a key element of NATO’s core decision-making process **enshrined in Article 4** of the Washington Treaty. Political consultations are part of the preventive diplomacy between member states, but they are also an avenue to discuss concerns related to the security threats member states face. These consultations can be a catalyst for **reaching a consensus on policies** to be adopted or actions to be taken—including those on the use of sovereign cyber effects to support a NATO operation. The alliance has a track record of collective action and cooperative security measures. For example, Operation Active Endeavour helped to deter, disrupt and protect against terrorist activity in the Mediterranean in the aftermath of the 9/11 terrorist attacks, in solidarity with the United States. For the seventh time, the Atlantic Council’s Cyber Statecraft Initiative will be among the organizations privileged to organize an event on the sidelines of the Feb. 15–17 [Munich Security Conference](https://www.google.com/url?q=https://www.securityconference.de/en/activities/munich-security-conference/munich-security-conference/msc-2019/&sa=D&ust=1550163045881000&usg=AFQjCNG0SJ7ETPilO9UxMCe9HqUtjeJGyw). This year in particular, the Atlantic Council’s event, “Defending Human Dignity: Limiting Malicious Cyber Activity Through Diplomacy,” will complement the topics high on the agenda of the main conference, such as transatlantic collaboration, the consequences of a resurgence of great power competition and the future of arms control. In the United States, the greatest failures of response and deterrence to foreign aggression in cyberspace have not been caused by a lack of intelligence, capability or imagination. Rather, U.S. policy has been serviceable in theory but impotent in practice because of an inability to translate technical findings and **intelligence into public support** for sufficiently tough responses ordered by elected political leaders. North Korea’s repeated operations targeting U.S. companies and critical infrastructure have been met with public skepticism over their culpability, limiting the strength of retaliatory options needed to deter further events. Chinese cyber economic espionage continued for years despite widespread knowledge of China’s activities because political leaders found it difficult to confront Beijing without undermining U.S. companies in return. Russian information operations did not sow enough doubt to mislead experts, but they succeeded in exacerbating the partisan polarization of an already-divided electorate and its leaders. That inability to translate the findings of cyber experts into public sentiment and therefore political action has sidelined America’s cyberwarriors, by far the most technologically advanced and well-resourced in the world. Imagine the political response of an ally that is asked to burden-share in response to cyber aggression but is probably much closer to any resulting kinetic fight than the United States. Now imagine the response of that ally when it’s being asked to take causus belli on faith: The United States is presenting attribution for a cyberattack elsewhere in the world, but perhaps is depending on the ally lacking critical details due to classification, and is presenting that information alongside a request for help that might well put the ally in the crosshairs of its own cyberattack or lethal action. **How can allies** with different capabilities to collect, analyze and understand intelligence be part of a consensus on using sovereign **cyber effects** to support a NATO operation? How can a commander **achieve a common operational picture** to authorize the use of sovereign effects in a NATO operation if all the allies are not on the same page with respect to critical attribution and other technical information needed for a use of effect in an operation? We all know what a tank looks like on a shared satellite image, but if you ask three cyber experts to interpret the attribution for a set of indicators, you are likely to get at least four answers. For most U.S. allies in Europe and elsewhere, there is simply a dearth of technical know-how within the government when it comes to cyber attribution and **operations**. This is already a [challenge](https://www.nextgov.com/cybersecurity/2015/04/fierce-battle-cyber-talent-even-nsa-struggles-keep-elites-staff/110158/) for the United States, with a massive defense budget, Silicon Valley innovation and an educated workforce to pull into [government service](https://www.usds.gov/). But for many U.S. allies, tech-savvy public servants will have long fled for the private sector, nongovernmental organizations (NGOs) and academia before reaching ministerial positions. To its credit, the U.S. National Cyber Strategy does propose capacity-building measures to support allies. This means building up law enforcement, intelligence, and military operational and investigative capability. But even with successful capacity-building programs, many nations could, in a crisis, end up in the same place the United States is—with good options stuck on the shelf while political leaders and their electorates lack a critical mass of informed voters to trust, understand and act on expert findings. For countries weighing whether to risk their own blood and treasure in support of an ally’s cyber attribution findings, this **hurdle could well prove insurmountable** if not addressed well before a crisis emerges. Many such countries will no doubt recall being burned when placing too much confidence in U.S. technical and human sources without an **ability** to evaluate the evidence for themselves, as with the Iraq weapons of mass destruction findings. The private sector will probably play a crucial role in providing intelligence to support alliance responses to cyberattacks, especially as a stopgap over the next few years. FireEye and its peer competitors and partners regularly produce analyses of major world cyber events—many that fly below the radar of Western leadership, in fact—sometimes at a near-government quality and often covering much of the same “classified” evidence. More important, private-sector analysts are accustomed to writing for impact with both their technical counterparts, like chief information security officers (CISOs) and threat hunters, and nontechnical stakeholders such as boards of directors, CEOs and other persons controlling the purse strings. In this sense, unclassified, private-sector and NGO-driven cyber threat intelligence can become the lingua franca of discussions. Relying on commercial reporting generated by international teams, rather than declassified government-generated reports, both broadens the audience enough to make alliance discussions feasible and mitigates against disparities in terminology across national lines—the tendency of even closely integrated allies to describe cyber “attack,” “information operations,” and attribution findings with different implicit assumptions or implications. Long-Term Thinking In the long run, though, **the U.S.** and its more technologically advanced allies—such as its fellow Five Eyes (Australia, Canada, New Zealand and the U.K.), France and Japan—will have to make important policy changes in the interests of **furthering alliance cooperation** in cyberspace: a willingness to sometimes risk sensitive sources and methods in order to get cyber threat intelligence into the hands of other countries better positioned to take policy action, an end to classifying public information like IP addresses solely because of their acquisition via classified means, and greater transparency on their own decision-making. Government cyber leaders within the alliance should consider taking another page out of the private-sector playbook as well: running cyber-crisis exercises that involve more than the IT department. In the commercial world, the more successful practice runs involve leaders at both the CISO level and some presence from nontechnical teams that would weigh in during a crisis, such as communications and legal. The best exercises involve executives, too, who despite their busy schedules must see for themselves how their companies would survive and respond during a potentially ruinous cyberattack, and work through the minutiae of leading a response themselves. The experience and confidence is invaluable if ever called on during a real-life crisis, and the organizational introspection by involving decision-makers at all levels is irreplaceable. Military-to-military cyber training as part of cross-country force standardization and joint operational planning could pull in more senior national leadership, beyond battlefield commanders, and be coupled with increased funding for foreign affairs-led training for nontechnical leaders. The private sector could also meaningfully contribute during NATO consultations when developing Allied Joint Publications to make sure that definitions and requirements for threat intelligence incorporate the best practices of NATO member countries’ private sectors. If a U.S. diplomat reaches out to his or her counterpart in an allied country to ask for assistance responding to malware that’s damaging critical infrastructure, and that counterpart has to ask what malware is, the **response isn’t going to happen.** NATO’s essential and enduring purpose is to safeguard the freedom and **security of all its members** by political and military means. Tolerating cyberattacks, especially those deliberately targeting civilians and the political legitimacy of governments—without the alliance having the capability to **jointly discuss** attribution **and have the confidence to act and assist one another**—**undermines this core purpose of the alliance**. Likewise, pursuing only deterrence and response without an active role for the alliance in reaching peaceful [diplomatic agreements](https://www.lawfareblog.com/private-sector-cyber-intelligence-could-be-key-workable-cyber-arms-control-treaties) with potential adversaries **abrogates member responsibilities** to their citizens but is impossible without a common language and operational picture to discuss enforcement of such agreements. The U.S. is stronger with allies, and with attention to these issues its cybersecurity can be too.

#### 2---Intrusions---Squo policy of unilateral OCO frameworks cause network intrusions from allies that undermines trust, cohesion, and cooperation --- Integration solves

Smeets, 20 (Max Smeets, Max Smeets is a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich and Director of the European Cyber Conflict Research Initiative., 2-15-2020, accessed on 6-18-2022, Taylor & Francis, "U.S. cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection", https://www.tandfonline.com/doi/abs/10.1080/02684527.2020.1729316?journalCode=fint20)//Babcii

Benefits and the creation of partnerships The strategy of persistent engagement and defend forward can help less capable cyber actors defend themselves against adversaries. Both the U.S. Cyber Command vision and the DoD cyber strategy stress the importance of working closely with **international** and private sector **partners** to successfully operate in cyberspace.xxix The DoD strategy states the following: “Our strategic approach is based on mutually reinforcing lines of effort to build a more lethal force; compete and deter in cyberspace; expand alliances and partnerships; reform the Department; and cultivate talent.” xxx On international partnerships, it more explicitly states: “Many of the United States’ allies and partners possess advanced cyber capabilities that complement our own. The Department will work to strengthen the capacity of these allies and partners and increase DoD’s ability to leverage its partners’ unique skills, resources, capabilities, and perspectives. **Information-sharing relationships with allies and partners will increase** the **effectiveness of combined cyberspace operations** and enhance our collective cybersecurity posture.” xxxi The United States has also signed several memoranda of understanding and over the years addressed cyber cooperation in some way, shape or form. In 2008, a MoU was signed between the Department of Defense and the German Federal Ministry of Defence about computer network defense and information assurance.xxxii A year later, a similar MoU on computer network defense was signed with South-Korea. xxxiii More recently, the Cyber Command worked alongside Montenegrin cyber defenders with as aim “to increase interoperability, build partner capability, and deter malign influence on the democratic processes of our allies, partners and the U.S.” xxxiv It was reported that U.S. Cyber Command personnel operated in the networks of Ukraine and Macedonia as well to help those countries defend against malicious cyber activity.xxxv At the 2019 Cyber Command symposium, specific examples were discussed on how cooperation can also help in not just detecting or deterring adversaries but also cause friction in their operational activity.xxxvi For example, the U.S. might upload foreign APT malware samples on VirusTotal, an online malware repository and file scanning service, forcing adversaries to go back to the drawing broad and adapt.xxxvii One can think of several other scenarios how international partnerships (also with the private sector) can help to ensure **more coordinated take down** of adversarial operations - actions beneficial to both the US and its partners. Risks for Allies and Intelligence Collection This section addresses four connected risks associated with US strategy. The first risk is perhaps the most obvious: if U.S. Cyber Command directly operates in allied networks without consent, it creates friction by allies undermining trust. Operating instantly makes sense considering the potential operational tempo of adversaries: You cannot have protracted diplomatic discussions for two months with an ally about whether or not to take down some command and control infrastructure of an adversary hosted in the allied country. You don’t have days, let alone months. As a participant mentioned at the 2019 Cyber Command Symposium on strategy: “Opportunities within this domain are fleeting.” xxxviii Operating seamlessly could also make sense if an ally does not mind the U.S. coming into its networks to address the malicious activity. In this vein, the U.S. can continue to build partnerships with countries that do not have the capacity to defend against cyber attacks on their own, as described above. But, what if an allied country is not keen on having the U.S. military in its networks, actively, seamlessly, and continuously disrupting an adversary’s cyber operations? As the German case shows, this **scenario will likely come up a lot more in the near future**. Second, it is not just about cyber effect operations taking place in systems or networks in allied territory. There could also be a negative impact on allied intelligence operations and capabilities beyond these systems and networks. The U.S Cyber Command - and other military cyber organizations - are operating in a global environment historically dominated by intelligence agencies, and the Five Eyes has always been the most dominant actor in cyberspace.xxxix But the anglophone intelligence alliance is not the only intelligence actor operating across the world. **Recent cases**—such as the infiltration of the Dutch General Intelligence and Security Service into the Russia-based network of the infamous hacking group Cozy Bear—have illustrated the continued global prevalence and value of allies’ intelligence operations beyond the Five Eyes alliance.xl If U.S. Cyber Command increasingly take up the role of ‘disrupter’ it may negatively impact **global intelligence** collection of allies—particularly those countries that favor long-term access over immediate effect. It will also more likely uncover and burn allied capabilities. **The risks of occurring are higher than one may think** as intelligence agencies have a tendency and incentive to target and track the same entities. For example, in late 2014, cybersecurity company Kaspersky Lab reported on the so-called "Magnet of Threats”. The cybersecurity company discovered a server belonging to a research organization in the Middle East that simultaneously hosted implants for at least five Advanced Persistent Threat (APT) actors: Regin and the Equation Group, Turla and ItaDuke, Animal Farm, and Careto. xli All of these APTs have been associated with prominent national security and intelligence agencies. Equation group and Regin are connected to the Five-Eyes. As said, Animal Farm has been attributed to France's external intelligence agency. Turla Group has been associated with the Russian federal security service (FSB). ItaDuke is said to be linked to the Russian government too. Finally, it is theorized that Spain is behind Careto, also known as ‘The Mask’. Consider what would have happened if one of those five APT groups had sought to cause a disruptive effect - rather than collect intelligence - against the target in the Middle East. It likely would have resulted in much earlier discovery and analysis by threat intelligence companies (or other actors) exposing the tactics, techniques and procedures (TTPs) of each actor group. Also, even the anticipation of more cyber effect operations in non-allied networks from one allied state could lead to a change in operations by another state. Indeed, states have shown in the past that the anticipation of early discovery of an operation has led to a change in their TTPs. For example, the National Security Agency (NSA) created an "exploit orchestrator" called FoxAcid, an internet-enabled system capable of attacking target computers in a variety of different ways, depending on whether it is discovered—or likely to be discovered—in a given network.xlii FoxAcid has a modular design, with flexibility allowing the NSA to swap and replace exploits and run different exploits based on various considerations. Against technically sophisticated targets where the chance of detection is high, FoxAcid would normally choose to run low-value exploits. Third, **allied friction could potentially be exploited by adversaries**. Adversaries do not randomly choose which intermediate nodes to direct their operations through. If Russia has the choice to go through a network that would raise some serious diplomatic friction between the U.S. and a U.S. ally, or operate through a network that would cause no diplomatic friction for the U.S., what would it prefer? It would make sense for adversaries to operate through the networks of exactly those countries with which the U.S. has a strong relationship but that do not want the U.S. to operate within their networks causing any effects. Russia is already good at exploiting divisions between the U.S. and its allies. Cyber Command’s new strategy might give it another avenue to do so. Fourth, whilst **allies can integrate their cyber efforts into U.S. strategy** of persistent engagement, if **allies would adopt their own strategy** of persistent engagement - mirroring U.S. current doctrine and practice - **it would likely further undermine the alliance relationships**. If US strategy of persistent engagement leads allies to adopt their own strategy of persistent engagement, it would mean **allies also seek “superiority in cyberspace”;** “continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver”; and operating “seamlessly, globally and continuously” - as stated in the Cyber Command vision. More specifically, it would mean that allies seek to **swiftly achieve effects in systems and networks that are potentially located on U.S. territory**, without necessarily notifying the U.S. government before. In other words, it means that **networks and systems turn into red space and gray space for allies** - like allied networks are now gray and red space for the U.S. to actively disrupt and degrade adversarial operations. It is unlikely that the U.S. government would react positively if Germany, or any other allied country for that matter, hacks into a server hosting Russian propaganda that was located in the United States, with some form of notification but without Pentagon’s consent.xliii There are numerous reasons why the US government would be **upset** with this type of behavior. It would likely be seen as reckless from Germany - especially if the US was already on those same networks for intelligence collection purposes. An important dimension of this scenario is derived from the fact that the U.S. is a vast target rich environment, potentially even prioritized as a target by adversaries such as China, Russia, North Korea, Iran - as well as non-state actors. As stated above, red space and gray space are defined, according to U.S. Joint Publication 3-12 on Cyberspace Operations, based on what “nodes” adversaries “control”. There are many nodes adversaries (of US allies) want to control in the US. In other words, if US allies would seek to swiftly disrupt and degrade cyber operations in red space and gray space on a constant-basis, much of that would be in the United States. Last year the NATO alliance reached a landmark that went largely unnoticed: there are now more NATO member states that have publicly declared they are seeking to establish an institutional capacity within the military forces to conduct cyber effects operations than there are member states that have remained publicly silent on this issue.xliv Yet, most NATO members are still at the early stages of organizational development - and pour relatively few resources into their military cyber organizations to conduct cyber effects operations.xlv Their operational capacity is limited. France and Germany stand out for the extent of resources officially allocated to their military cyber organizations (beyond the Five-Eyes) - but public statements about these figures are generally hard to interpret and compare given distinct institutional design across military cyber organizations of states.xlvi This risk is therefore less significant for the short term, but is **likely to grow in the medium to long term**. Conclusion and Discussion The purpose of this paper was to provide a benefit-risk assessment of US strategy for its allies and intelligence collection. Whilst the U.S. government’s mission to persistently engage with adversaries may have benefits for allied states, the paper identified several avenues how the strategy leads to negative implications for the alliance. To conclude, it is therefore worth considering how these risks can be mitigatedFirst, the principles of persistent engagement and defend forward are often jointly discussed. How the two principles relate to each other, however, remains unclear. According to some, persistent engagement is an ‘operationalization’ of the defend forward concept. Others believe there is a difference between the two concepts. If the latter is the case, it is important to assess to what degree a strategy of persistent engagement necessitates ‘defending forward’ and contesting adversaries wherever they are. In other words, the question is whether sufficient friction can be created without causing disruption in allied networks. Second, terminology about terrain in cyberspace is frequently confused by policymakers and experts. The U.S. government **needs to (re)assess** how its terminology of terrain in the physical domains applies to cyberspace. Last, NATO allies should consider establishing memoranda of understanding on offensive cyber effects operations in systems or networks based in allied territory.xlvii The goal of the proposed memorandum would be to reduce discord among the allies; enhance trust, transparency and confidence between allies; and improve the effectiveness of disrupting and deterring adversaries’ operations in cyberspace. The scope of the memorandum would include: i) developing a common notification equity framework for out-of-networks operations which seek to achieve cyber effects in allied systems or networks; ii) identifying procedures for communicating the consideration and conduct of offensive cyber effects operations between states against systems or networks in allied territory; and iii) identifying technical solutions and administrative documentation required for the continuous exchange of information on offensive cyber operations. In writing the memorandum, states first and foremost should agree on the equities involved in permitting signatories to conduct cyber effect operations in each other’s networks—and the relative weight of those equities. Equities that should be considered include: i) the ability of an actor to take action to negate known threats on or to the other parties’ networks and systems; ii) the likelihood that an action will negate known threats; iii) the imminence and scale of the threat; iv) the risk of collateral damage; v) whether the computer system or network is government-owned or privately owned; and vi) the certainty that the system or network will be used to achieve strategic effects by the adversary.xlviii Finally, though the memorandum of understanding may help in promoting stability and enhancing confidence amongst allies, it is not a silver bullet. It can only reduce allied concerns rather than mitigate them. Military cyber organizations may still conduct effect-based operations in allied territory without consent, leading allies to assert that their sovereignty has been violated.

#### Allied mistrust sparks conflict in every region---nuclear war

Dr. A. Wess Mitchell 10, President of the Center for European Policy Analysis, Doctorate in Political Science from the Otto Suhr Institut für Politikwissenschaft at Freie Universität, Master’s Degree from the Center for German and European Studies at Georgetown University’s Edmund A. Walsh School of Foreign Service, and Robert Kron, Research Association at the Center for European Policy Analysis, 2/1/2010, “Counting the Costs of Insecurity in North Central Europe”, http://www.cepa.org/ced/view.aspx?record\_id=219

America’s deprioritization of allies creates opportunities for revisionist powers. Such transition is recurrent in geopolitics; international relations are always characterized by uncertainty. Policy makers have to navigate a landscape that is often difficult to delineate, full of strategic actors whose purposes are often obscure and whose power is difficult to assess. Intentions are notoriously hard to divine, in part because rival states obfuscate them but in part because often the states themselves do not have a clear and consistent perception of what they want to achieve. Uncertainty arises also out of a more quantifiable source of knowledge, an assessment of hard power, which is imperfect and results in widely different estimates. It is sufficient to recall the challenges of assessing Soviet power throughout the Cold War. Moments characterized by alleged large shifts in relative power present particularly acute problems of assessing power and intentions, adding an additional layer of ambiguity and uncertainty. Rumors of change put in doubt the relatively well- known, or at least familiar, geopolitical situation. All parties involved are unsure about their position relative to the others, the extent of their political sway, and the match between their commitments and their power. The established great powers may have a crisis of confidence, while emboldened rising states are uncertain how far their influence extends as well as how solid and credible is the power reach of their weakening rival. Revisionist powers now openly but cautiously question what was the grudgingly accepted geopolitical status quo. Rising powers are thus curious but careful. They are interested in pushing the existing boundaries of their influence but do not know how far they can do so without meeting a firm opposition of the other power. In the current case, U.S. rivals— China, Russia, and Iran— appear keen to assert their influence and establish what they deem their rightful position in their respective regions and in the world but are also eager to avoid a direct confrontation with the United States. Uncertain about their own power relative to the United States, they test the hypothesis of a growing American economic and military fragility and decaying political reach. To figure out the new map of power, and possibly to redraw it at low cost, revisionist powers engage in probing. In this chapter we examine this behavior— the probing by revisionist powers. We define probing as a low- intensity and low- risk test aimed at gauging the opposing state’s power and will to maintain security and influence over a region. It is a set of actions that studiously avoids a direct military confrontation with the leading power by targeting the outer limits of its commitments and interests. There, along the outer rim of its influence, the hegemon is at the furthest of its commitments and power projection. The perception, or rather the suspicion, of its decline is most consequential along these frontiers of power because the revisionist state senses opportunities in its own neighborhood and searches for confirmation of the rival’s weakness. Probing is an opportunistic behavior. It occurs when the revisionist states detect a permissive international situation, namely, when they think that the existing great power is retreating. It is still a behavior that is characterized by self- doubt and uncertainty, although if unanswered it results in the confirmation of the belief in the rival’s decline and may lead to ever more assertive challenges to the international order and expansions of influence by the geopolitical challenger. Over the past few years, and with greater frequency and brazenness, regional powers opposed to the United States have been engaging in probing. Russia, Iran, and China in their respective regions have been working under the hypothesis that the United States is retreating, out of choice, fatigue, or weakness, or all three combined. The American retrenchment is more pronounced in the Middle East, with the ending of U.S. combat presence in Iraq and the drawdown in Afghanistan as well as the unwillingness to intervene in Syria, leaving a vacuum for Iranian influence. But there is an equally pervasive perception of American withdrawal or decline in the other two key regions, Europe and Asia. In Europe, the perception is that Washington is redirecting its strategic focus and resources toward Asia and has limited willpower to back its extended deterrent, giving Moscow a window of opportunity to redraw the map in Europe’s eastern “borderlands. ” And in Asia, a rising and confident China looks at a United States hobbled by financial crises, fiscal imbalances, and a decade- long military overstretch in the Middle East. The reasons are different, but the broad perception is similar: the revisionist states sense an opening left by a distracted and weakening United States. And they probe along the periphery of American influence, from Ukraine to the South China Sea through the Persian Gulf. ORIGINS OF PROBING BEHAVIOR Probing stems out of a tentative belief that the existing geopolitical order is amenable to change, and it seeks to confirm this suspicion. A perceived geopolitical change remains only that, perceived, until facts on the ground confirm it. An assessment of a state’s power is merely an estimate of how that state may fare in a clash with others. As such, it informs a set of expectations for the future, and it may or may not reflect reality. Often there is little agreement among powers as well as within those powers as to which assessment of power is correct.1 Today, for instance, questions about the continued resilience of American power abound both abroad and in the United States, and there are analysts on both sides of the argument.2 Regardless of where one stands on the issue of American relative decline or retrenchment, the mere existence of such a debate is a source of concern because it points to an absence of clarity on the geopolitical scene. The various strategic actors no longer know where they stand on the international pecking order and are confused as to how far their own influence can reach and what the responses of their rivals may be.3 These are periods of a tense peace but also of great uncertainty about the nature of the security environment. As a scholar put it, it is the “fog of peace” that makes strategic planning more difficult because it is unclear who the enemy is, how much power a potential rival may have, and where the boundaries of political influence are.4 As history indicates, often such an uncertain strategic environment degenerates into war, which is a “dispute about the measurement of power. ”5 The outcome of a war is the violent clarification of such confusion. It settles the dispute about the assessment of power. A victory or defeat in war, followed by changes in boundaries, military bases, or political affiliations of governments, is one way to prove or disprove a perceived alteration in relative power. As British historian A.J.P. Taylor observed, the “test of a Great Power is . . . the test of strength for war. ”6 After its defeat in the 1853– 1856 Crimean War, Russia was clearly militarily inferior to European states (even though the victorious powers, Britain, France, Turkey, and later Austria, also encountered serious difficulties in projecting power to the Black Sea theater) and consciously chose to retreat, reform, and rebuild its foundations of power, known as a policy of recueillement, in order to maintain its status as a European great power.7 There is no clearer confirmation of a state’s decline than a loss in a direct confrontation with a rising power; there is equally no better proof that the perception of relative decline was incorrect when the aspirant revisionist state is soundly defeated. In the immediate aftermath of a war it is therefore easier to assess one’s own power relative to that of the other players. War lifts the “fog of peace. ” But war is rarely pursued simply to clarify one’s own uncertain standing relative to the other strategic actors. To engage in war, the ultimate test of power, is exceedingly dangerous, and no leader wants to enter into a violent conflict simply as a way of assessing the power of its own state relative to the target. Wars are realms of luck and un knowns as much as of more calculable kinetic clashes, and consequently the outcomes do not always align with the expectations preceding them.8 In fact, the losing party in a conflict has often entered that war having overestimated its own capability relative to the rival. Many in Europe, for instance, expected in summer 1914 to be “home for Christmas, ” only to remain in the bloody trenches for several years. Given this inherent uncertainty, the risk of being proven wrong for both the perceived rising and declining powers is high, and great powers in history seem to stumble into wars rather than consciously pursue them as tests of strength. The risks of war are incalculable and thus extremely high. A less risky way of assessing a changing equilibrium of power is through probing. This is a form of strategic behavior meant to test existing perceptions of power relations, seeking at the same time to draw the presumably new boundaries of influence. The rising or revisionist state, in particular, is strongly motivated to test the will of its seemingly declining rival power. It has the aspiration, mitigated by the fear of the rival great power, to alter the existing geopolitical map. Such states, unhappy with the existing international order, which they perceive perhaps as imposed on them and certainly as increasingly not reflective of their own rising aspirations and power, have the most to gain from probing. If this behavior confirms the perception that the existing great power is on the wane and that the map drawn by it is no longer supported by its strength and will, the revisionist state may be able to reassert lost influence over its neighborhood and revise a previous settlement. At the same time, such a state has also a strong incentive to avoid a direct clash with its main antagonist lest the perception of its relative weakening turns out not to match reality. A strategy of direct confrontation is risky because its success is predicated on the relative weakness of the targeted power, the existing hegemon, and this is exactly what is unknown. If the probing power becomes convinced that its hypothesis of its own superiority (and of the relative decline of the rival) is true, then a direct clash may occur. But until that confirmation, a safer, less risky course of action is to engage in a probing behavior, akin to testing the water before jumping in. Probes target the frontier of the rival power’s influence, where its interests are less pronounced, its power is at its farthest projection, and its political clout at its weakest. At these outer edges the response of the great power is expected to be most restrained, while the gains of the probing state are most likely to occur. The purpose of probing, therefore, is to gauge the resolve of the targeted powers. We will return to this later, but here it is important to note that a probing action is also a way of showing the renewed or freshly acquired capabilities and aspirations that otherwise would remain latent and without tangible effects. One cannot revise an established order by keeping one’s own intentions and capabilities hidden. Showing a new military platform, often in a carefully choreographed event, is one way of signaling growing power. The 1907– 1909 voyage of the American “Great White Fleet, ” meant to showcase the emergent global naval strength of the United States, was one such episode. The round- the- globe cruise was not targeted at a specific power and did not aim to extend American influence over a particular state or region. Rather, it was a broad assertion of American capabilities and global reach, and the other powers, Great Britain in particular, certainly received it as a sign that the United States was a power to be reckoned with. But probing is more than showing off. It is not simply an action of strutting on the world stage with newly acquired military gadgets and political confidence but a precisely targeted action with clear objectives. Through probing, a revisionist state aims at changing the existing geopolitical order where it thinks it can, namely, at the farthest points of the ruling great power’s influence. Probing, therefore, is not just mere signaling of displeasure with the rules of the international order and the map of power; it aims to revise the order gradually and carefully, starting from the outer layers of the rival great power’s influence. FEATURES OF PROBING The purpose of probing is threefold. First, a probing state aims to check whether the rumors of its rival’s weakening are true. A probe is a test, meant to elicit a response from the targeted power. Second, the revisionist state that engages in probing behavior wants to avoid a direct military clash with the existing great power. The risks of being wrong about the rival’s resolve and capability are simply too big. Third, the state’s objective is to achieve, if possible, low- cost revision of the existing regional order. These purposes can be seen in the features that characterize a probe and distinguish it from other types of behavior, ranging from fullout aggression to commercial pressures and diplomatic démarches. First, probes are low intensity, vigilantly avoiding a direct war with the main rival power. They are below the horizon of direct military confrontation. The revisionist state has no interest in starting an allout military conflict with the rival great power, perhaps declining but still more than a match. The level of violence used, therefore, is low, and probes are limited projections of power in areas of less pronounced interest to the rival. A probing power engages in a lot of selfrestraint; it intentionally elects to keep the use of force at a minimum. It can but chooses not to escalate. A probe is a calculated gamble, not a foolish thrashing around. The desire to avoid a war with the existing hegemon often leads the revisionist to project power under cover of civilian or paramilitary forces, part of a larger trend of “civilianization” of conflict.9 By using unmarked units to harass a U.S. protégé, a state is able to de ny authorship of provocative actions and thereby avoid a more violent and direct war while at the same time chipping away at the rival’s influence and wealth. The possibility of denying that an aggression has occurred drives costs of revisionism lower. For instance, the sixteenth- century privateer Sir Francis Drake acted on behalf of Queen Elizabeth I, raiding Spanish shipping but never in an official capacity. The queen went so far as to tell a Spanish ambassador that “Drake was a private adventurer, and that she had nothing to object to his alleged execution. ” She was careful in not provoking Spain too much but eager to “singe the King of Spain’s beard. ”10 A similar approach can be seen around the world today. The initial Russian push into Crimea in 2014 was done anonymously with unmarked special forces, dubbed by Ukrainians as the “little green men, ” a clear example of a long- standing Russian practice of tactical deception and disguise (maksirovka).11 It was an indication that Moscow was unsure whether Ukrainian forces would react, and, in the event of a determined opposition, it maintained the option of either escalating with larger conventional forces or halting operations and denying. Moscow seemed to be more careful in masking the identity of its forces in eastern Ukraine, where the local opposition was more assertive and the Western displeasure with Russian aggression more pronounced. The greater the risk of a strong response from the actors targeted, the more carefully tailored, dissimulated, and low- intensity is the probe. The use of unmarked troops and paramilitary forces allows Russia to claim that no aggression has occurred, and thus no military response from Ukraine or from the West is warranted. China has been testing the limits of the influence of the United States and its allies in the South China Sea using an array of civilianlooking vessels. Its fishing fleet, combined with a fishery- enforcement fleet, is integrated into its military institutions and plays an active role in expanding China’s maritime reach. As Lyle Goldstein observes, this is part of a “strategy of ‘defeating harshness with kindness’ (yi rou ke gang)” whereby China deploys “unarmed fishing vessels or fisheries enforcement vessels to confront foreign vessels operating in its EEZ and claimed waters. ”12 This low- intensity push tests the fron tier of American influence in a way that makes a U.S. response difficult.13 A foray by a Chinese naval vessel into contested waters can be countered with the might of the United States and its ally’s navy; a probe by fishing vessels manned by Chinese fishermen does not warrant the involvement of the U.S. Seventh Fleet. This is risky behavior, but it also indicates a desire by China to avoid a war with the other regional powers as well as with the United States.14 If it is openly a military attack, a probe is conducted with a strong and perhaps warranted belief that the rival power will not intervene because it is distracted elsewhere and because it deems the targeted region to be of little immediate interest. This was the case of the Russian war with Georgia in 2008, when Moscow felt emboldened by NATO ambivalence to extending its membership process to Tbilisi and by the American strategic distraction by the wars in Afghanistan and Iraq (where a small Georgian contingent was deployed). The Russian gamble was based on the expectation of no meaningful Western, and American in particular, response. The objective was to chip away at the unwelcome Western influence in Russia’s neighborhood but without spurring an equally unwelcome Western military reply— to “singe America’s beard, ” as it were. Second, a revisionist state engages in probing because it sees it as a low- risk but high- reward behavior. The low risk stems in part from the first feature, the carefully tailored level of aggressiveness that is expected not to elicit a full- out military response by the rival. It is also related to the third feature, explained below, namely, the fact that the immediate target of probing is geographically and political peripheral to the interests of the rival great power, and consequently contributes to the low likelihood of a forceful military response. But on top of being pursued as a low- risk action, a probe can yield high strategic rewards. Most often the revisionist power seems to direct probing behavior to its immediate vicinity, hoping to expand its influence over neighboring and thus more controllable regions.15 It is there that it has the greatest chances of extending its own political shadow successfully. Probes are rarely long- distance projections of power because incursions deep into the rival’s sphere of influence are more liable to be met with more assertive responses as well as being less likely to establish durable control by the probing state. The farther the revisionist state engages in probing behavior, the more high risk and low reward it is, and vice versa. Hence the more likely locations for probing behavior are in the near neighborhood of the revisionist power. Furthermore, probes focus on strategically important regions, either resource rich or located along lines of communication, or both. Elizabethan England, for example, conducted raiding probes of Spain’s vulnerable transatlantic arteries bringing gold from the New World— not its stronger positions in the Mediterranean. Imperial Germany’s probes of the Anglo- French alliance targeted Morocco, located near the strategically important choke point of Gibraltar but beyond easy reach of the main British fleet. Today China’s probes of U.S. allies in Asia often target oil and gas fields in the South China Sea. In all these cases, since the goal of probing is to test the power and commitment of a rival state, it has to be directed at regions where the rival’s influence is present but not preponderant. It is unlikely that regions of no geostrategic value or with few resources have much of a presence of the rival great power, and as such they are not prime material for probing. A state may still have imperial aspirations in such regions, but not every extension of power is a probe. Probing is not simply grabbing new areas of influence but first and foremost to test the will of the rival. There may be, of course, the bonus that if the probe is successful, it may result in the addition of strategically important regions. The third feature of probing is that it is peripheral or indirect. The target of the probe is the periphery or the frontier of the tested power where the rival’s presence is at its farthest reach, its interests are less pronounced, and thus its response is expected to be muted. Fearful of a militarily assertive response, the state that is probing is careful not to target areas that are clearly considered of primary and existential interests, such as the rival’s homeland or its immediate neighbors. Hence the visits of Russian or Iranian naval vessels to Venezuelan ports are less a probe per se than an act of grandstanding, since all sides know that the United States could quickly bring overwhelming force to bear in the event of a crisis. These are temporary publicity stunts rather than a calculated attempt to test the hegemon’s commitment to maintaining the status quo. Probes test for perceived weaknesses, not strengths, and it is on the outer boundaries of the existing great power that its influence is likely to appear the most fragile. The revisionist power is interested in probing the power and influence of its rival in places where that influence is at its weakest, overstretched, and uncertain. During the Peloponnesian War the Spartan general Brasidas adopted such a peripheral strategy, but only a decade into the conflict. The initial Spartan approach of annual invasion of Attica, Athens’s immediate neighborhood, failed to inflict sufficient damage to end the war. It was only with Brasidas, sent north with a small force of helots (minimizing thus the risk to Spartan manpower), that Sparta changed its strategy to one similar to probing, by persuading or forcing distant Athenian allies in Thrace to switch sides. And many did reconsider their allegiance to Athens, because, as Thucydides observes, there did not seem to be much risk given the distance from Athens and their belief that this empire was on the wane.16 Striking the rival’s periphery, and its allies, not only was cheaper than assaulting it directly but also forced it to devote a lot of resources to reasserting the lost influence. Global powers in particular have a “periphery or frontier problem” that invites probing. A lengthy frontier, distant from the homeland and thus from key logistical bases, is difficult to protect. The sheer amount of power needed to outfit the distant outposts, combined with the uncertainty as to the location and timing of potential attacks, makes it impossible to have an impermeable frontier. When a power assesses threats, the key questions of “where, when, and by whom” are directly related to the length of the imperial frontier. A regional power has well- delimited borders and a clear idea of who the rival is. For instance, from the final decade of the nineteenth century on, Germany was burdened with the possibility of a two- front war, with France on one side and Russia on the other; a serious problem of military planning caused by poor diplomacy but not a source of strategic confusion. For a global power, it is that strategic clarity that is missing, resulting in the need to prepare for multiple contingencies and ultimately to stretch resources in several theaters of potential action.17 While imperial Germany could concentrate on its two- front problem, Great Britain at the turn of the twentieth century had to consider threats from Russia (in Central Asia, pushing toward India), Japan (in the Asian littoral sphere), France (in Africa as well as the Mediterranean), and Germany (in Europe and the North Sea in particular). Through deft diplomacy, it managed to neutralize the first three, allowing it to focus on the German naval threat, thereby limiting its “frontier problem. ” In practice, probing the periphery of a rival’s great power often translates into testing the strength of its alliances. Most great powers, or empires, expand their influence in informal ways, through political arrangements with local elites and formal alliances.18 The security of these great powers, in particular of ones with global reach, therefore resides not only in the safety of their borders but in their ability to hold rivals at a distance and thwart their challenges to faraway interests. They do so only in part through their own forces and rely heavily on the presence of allies that provide additional military strength and local deterrence (see chapter 5). Allies are at the periphery of influence and strength of great powers, and it is there that the powers’ commitment and influence are at their weakest. It is clear that a state will respond to an encroachment on its territorial possessions or to an attack against its forward deployed forces. It is less certain, however, that a state will respond in the same strong fashion to similar actions directed against its allies and their interests. The security guarantee extended to them, the foundation of the alliance, is a promissory note that carries a high degree of uncertainty. Placing bases with troops on the territory of an ally is a time- tested way of diminishing this uncertainty. As Thomas Schelling put it, the role of U.S. troops in South Korea was simply to die, buttressing the American security guarantee to its ally.19 The loss of American soldiers to an initial attack by the enemy would, so the argument goes, create powerful pressures for Washington to respond. French general Ferdinand Foch, when asked before World War I how many British troops would be needed for the security of France, replied, “One single private soldier . . . and we would take good care that he was killed. ”20 Probes by the revisionist power are not attacks against these bases and forces that underwrite the credibility of the extended deterrent. Rather, they target areas that may be of great importance to the ally but not necessarily to the security patron. That is the periphery of the periphery, so to speak, the tip of the great power’s commitment. The United States has a particularly pronounced “periphery” problem. There are few direct threats to the continental United States, short of a large- scale assault with weapons of mass destruction or the tragic yet relatively small and isolated terrorist attack. While the absence of a contiguous threat is a geopolitical blessing, it also means that most of the menaces to U.S. interests and security are outside of the North American continent. Hence, in the competitive international environment, “the strategic position of the United States rests ultimately on its ability to project power over great distances. ”21 In practice this entails managing alliances that maintain stability and keep U.S. rivals on the defensive in key regions of the world, in particular along an arc from Europe to East Asia through the Middle East. And historically this has been, and continues to be, achieved by extending U.S. deterrence beyond the North American continent to the countries, some allied by treaty and some neutral. Such an extended deterrence is a “ ‘three- nation problem’ involving an aggressor nation, the United States, and some smaller nation which is the object of the aggressor’s designs and which Washington seeks to protect. ”22 Probing by an “aggressor nation” aims to test U.S. commitment to these “smaller nations, ” which constitute the periphery of American interests and power. In the most successful case, probing could achieve a dual purpose: first, it tests the level and credibility of the commitment of the distant security patron, and second, it can weaken the rival alliance. It does so by targeting the foundation of the alliance, the belief that the alliance is beneficial to both parties and that it is effective. As Michael Mandelbaum has observed, alliances need to manage two concurrent fears: one of entrapment, namely, of being dragged into undesirable wars of limited significance and local interest, and one of abandonment, the apprehension of often the weaker ally of be ing abandoned by its security provider when the need comes. 23 Probing aims to increase the rival’s fear of entrapment while at the same time stoking worries of abandonment among its weaker and more dependent partners. By harassing the local interests of the rival’s peripheral allies, the revisionist power wants to drive up the risk of a local war, perceived by the rival as a distraction and a potential drain of resources. At the same time, it wants to indicate to the smaller allies that they may not rely on their security provider to defend their local, narrow interest, and that they may be abandoned. The goal is to drive a wedge in the opposing alliance by leveraging the fundamental dilemma of alliances— the fears of entrapment and abandonment. This is where probing becomes more than a simple test of the rival’s strength. By targeting the outer edges of the existing hegemon, and thus harassing its alliance system, the revisionist is engaging in a much more significant endeavor. The contest for regional, or global, control is in the end a contest for allies. A.J.P. Taylor observed that when Germany “was bidding for the domination of Europe” in the decade before the outbreak of World War I, “her chosen method was to isolate the independent Powers one from another. ”24 As we point out in chapter 5, allies are, among other things, an extension of the distant patron’s power. Were they to peel away from the side of their security guarantor— or vice versa, were the security guarantor to decide that the risk of continued support of a distant ally pressured by a regional revisionist power is too big— it would in either case signify a retrenchment of power for that offshore patron. The loss of allies is both a confirmation of the waning sway of that rival great power as well as a further reduction in its reach. To be alone in inter national relations is to be vulnerable, inviting further aggressive behavior from the rival. Walter Lippmann observed in 1943, “No one knew, not Hitler, not Stalin, not Chamberlain or Daladier, the relative strength of the Axis and of the opposing combination. Only when Hitler succeeded at Munich in separating the Franco- British allies from Russia, had he so altered the balance of power in his favor that a war for the conquest of Europe was from his point of view a good risk. ”25 War is an extension of successful probing. The benefits of targeting allies of a rival, rather than the rival itself, are well recognized in history. The astute observer of history and politics Niccolò Machiavelli noted in his Discourses that attacking a rival’s ally is always a preferred option: “For I know especially that if I assault his friend, either he will resent it and I will have my intention of making war with him, or by not resenting it he will uncover his weakness or faithlessness in not defending a client of his. Both the one and the other of these two things are able to take away his reputation and to make my plans easier . ”26 In the strategic behavior we describe, the probing power is not interested in “making war” with the rival, and therefore a probe is not a full- out attack on a rival’s ally or supported state. The risks of activating the security guarantees or assurances that ought to be at the foundation of that alliance are too big. But it is an offensive act of sorts, which threatens the interests of the rival’s ally. The security patron will either respond, thereby disproving the perception of its weakness, or will not, “taking away his reputation” and undermining its alliance. China has been particularly astute in picking geographic objectives that are important to U.S. allies but only indirectly important to the United States, such as the shoals and reefs around the Spratly and Paracel Islands. By ratcheting up the pressure in these areas, China causes the targeted states to intensify their demands for American assurance while diminishing U.S. willingness to back allies over seemingly petty issues that could lead to a larger conflict. Americans do not want to risk their lives for insignificant and distant rocks. Russia achieves a similar effect by reigniting NATO’s eastern frontier through its attack on Ukraine and a series of threats against exposed NATO members around the Baltic Sea. Those are areas that until recently have not been prominent on the U.S. strategic radar screen but are naturally vital to those smaller states inhabiting the region, which in turn are driven to make increasingly vocal requests for security reassurances from Washington. As in the case of the South China Sea, however, the local and limited nature of the rival’s probes generates in Washington as much a perception of threat as fear of a larger conflict, raising doubts about the benefits of extending security guarantees to these allies and partners. In the end, these peripheral probes pursued by U.S. rivals can create a wedge between Washington and its regional friends and allies. These three features— low intensity, low risk but high reward, peripheral— point also to the timing of the probing behavior. Probing is a strategic behavior that arises out of an uncertain assessment of power relations. It is the product of doubt, not confidence, in the resilience of the existing international order. As such it arises early on in the transition of power, when perceptions of rise and decline are not firm. The vagueness of the security environment creates among revisionist powers the perception of opportunities that a probing behavior aims to test. Hence probing should occur with less frequency in the immediate aftermath of a war, when, as we point out, an assessment of relative power carries the weight of the ultimate test, war. A defeated power may have all the incentives to upset the existing order, but unless it has no ability to evaluate its clearly weakened position, it has no capacity to do so. After a defeat probing may be tempting but is unfeasible. Such states are more likely to pursue a policy of recueillement (introspection, a moment of pause and strengthening), characterized by internal reforms, modernization, and very limited foreign engagements mostly aimed at dividing the opposing alliance.27 When, however, the perceived weakening of the founding power puts in doubt the existing international settlement, the desire to revise it is matched by the possibility of doing so. The perception of American weakening, or at least retrenchment, therefore opens up a window of opportunity for those powers that aspire to expand their own influence and resent the Western order and its institutions. THE AUDIENCES OF PROBING Another useful way of looking at the strategic behavior of probing is by considering the audiences involved. As we argued, a revisionist power pursues probing behavior to check whether new boundaries of influence are feasible given the perceived weakening of the rival. The main purpose is therefore to elicit a response from the targeted audiences. That response, or lack thereof, supplies information necessary to draw the new outline of the geopolitical map. Probing is first and foremost a violent and risky didactic exercise. The most direct audience is the immediate target of the probing behavior, usually an ally, or an aspirant to be an ally, of the rival great power. Probing here seeks to gauge the willingness and capacity of the targeted state to withstand pressure, and ultimately it aims to push that state to sever itself from its security patron. As we examine in chapter 4, vulnerable frontier allies of a great power actively consider alternative strategic options, especially when they perceive themselves to be under threat from a neighboring revisionist pow er and to have a fraying security guarantee from a distant patron. A probe is meant to ratchet up the threat perception while also attempting to establish a sense of strategic isolation and separation from the security provider. Hence as important as, if not more important than, the first audience is the second one: the distant but more powerful ally and security provider. Probing tests indirectly the regional staying power of the rival hegemon. While carefully avoiding direct confrontation, the revisionist power wants to assess the commitment of the opposing great power to its ally in the near neighborhood. What the revisionist is testing, therefore, is not the rival’s resolve to oppose other great powers, but the rival’s reliability to its own allies.28 Resolve is the willingness to risk war to achieve one’s own objectives: the more diffuse and distant the threatened interests, the less the resolve. Given that the target of probes is peripheral and not the rival’s homeland or troops and bases, the resolve is assumed to be small. Direct war between the revisionist probing state and the rival great power is unlike ly to erupt as a result. Moreover, the probing state is not interested in finding out whether the rival has the will to fight a direct war: the stakes would be simply too high and the outcome too uncertain. A direct challenge would test the resolve of the rival. Poking around the periphery, therefore, is a poor test of the rival’s willingness to fight a war. History seems to confirm this. For instance, as scholars have pointed out, Soviet leaders did not think that U.S. responses to peripheral threats (e.g., in the Third World) could serve as indicators of future American behavior when its core interests (NATO allies, Japan, or the U.S. homeland) were threatened.29 Whether the United States responded militarily or not to a Soviet foray in Angola or Ethiopia could not be easily translated into expectations of future American behavior in Europe. But it does affect the perception of whether the United States wants to fight in other peripheral areas. “If Soviet leaders were to gain the impression that the United States is firmly set upon a course of neo- isolationism and the absolute avoidance of intervention in local wars, they might become dangerously adventurous in the Middle East and elsewhere. ”30 Probing, however, tests the reliability of the rival great power— that is, its willingness to protect and stand by its ally or aspiring allies. The immediate target is not a test of the rival’s general credibility but only of its commitment to the security ties to the state. Probing wants to elicit a response (or lack thereof) from the rival great power regarding the seriousness of its commitment to the directly targeted state. To be perceived as a reliable ally means to instill the belief that promised security guarantees will hold even in cases of heightened tensions and, in final analysis, of conflict. Consequently a perception of low reliability results in the belief that the alliance is fragile and that it may be in the small state’s interest to seek accommodation with the nearby revisionist power. As delineated above, probes are care fully tailored to split the distant security patron from its regional allies, showing it to be unreliable. Even if it achieves nothing else, probing can introduce doubts about the security guarantees, forcing the security patron to renew its promises. The less reliable the security patron is perceived by its allies, the more insistent are their demands for continued security guarantees. Probing thus imposes an immediate cost on the rival great power by reactivating a frontier region that until then was dormant and by pressing the rival to expend more resources and political capital to reassert its security guarantees. Finally, the third audience is composed of the geopolitical onlookers, states that are watching the behavior and derive their own conclusions about the resilience of the existing great power. The strategic interaction spurred by a probe does not directly affect them, but they perceive it as a regionally circumscribed development with potentially more global repercussions. That is, a probe is limited to a specific region but has radiating effects as others also see it for what it really is: a test of the resilience and reliability of the great power that may be analogous in other regions. Recent academic literature puts in doubt the idea that reputation for commitment is interdependent. Thomas Schelling, among others, articulated that idea in his classic work from 1966 where he argued that U.S. reputation was global, and a loss in one region would have negative impact in other areas. Reputation was not compartmentalized in different regions, in large measure because the rival, the Soviet Union, was one and the same across the world map. Hence “we tell the Soviets that we have to react here because, if we did not, they would not believe us when we say that we will react there. ”31 Academics have relentlessly questioned this argument, resulting in copious writings asserting that reputation is not interdependent and, according to some, does not even matter.32 Reputation is merely a cult and does not exist in international relations.33 Policy makers, however, disagree and continue to speak of reputation for resolve and reliability as something that not only matters and requires constant work but also is interdependent. They prefer to rely on time- tested authors, from Thucydides to Machiavelli, who consider reputation as indispensable to political power.34 In brief, there is a deep gap between academics and policy makers on the issue of reputation. By observing recent events in the three frontier regions— Central Europe, the Middle East, and East Asia— we think that the truth is closer to Schelling’s view. It is clear that the effects of probing behavior do not remain confined to the immediate actors involved (the probing power, the direct target— usually a rival’s ally— and the rival great power). Other actors in the region are keenly aware of the revisionist state’s probing and of the responses of the United States. For instance, other states, from the Baltics to Poland and Ukraine, observed Russia’s war against Georgia in 2008 and its invasion of Crimea in 2014 with great trepidation.35 These wars were symptoms of a more assertive Russia; a source of worry in themselves. But they were also meant to elicit an answer from the United States. Any sign of American hesitation to respond quickly and firmly to Russian small wars in the two states was perceived as affecting directly these other states, not directly involved in the probing event. America’s reputation for reliability, in other words, was at stake, even though Georgia and Ukraine were not NATO members but only aspiring to closer security and political relations with the United States and the EU. Similarly, Pacific nations from Japan to Australia follow with great attention China’s probing behavior in the South China Sea that puts pressure on Vietnam, the Philippines, and Taiwan. They too seek to figure out whether the United States has the will to remain as a security provider in this region and to the “global commons” in general. How the United States responds to a probe in a particular region therefore affects its regional image. The question is whether there is also a wider, global audience to regional probes. Do Middle Eastern leaders watch American responses to Russia’s probing in Eastern Europe? Do Kremlin elites draw lessons from U.S. actions along the “first chain of islands” in East Asia? Or, do Chinese neo- Mahanian leaders think the United States is on the wane if it accommodates Putin’s imperial fantasies? According to the latest academic literature, the answer should be negative: how the United States is perceived to be doing in one region does not translate into a similar perception elsewhere. The practical implication of such a view is that the United States should not have fought in Vietnam to prove that it would stand its ground in Europe; similarly, it ought not to oppose Putin around the Black Sea basin simply to demonstrate that it will oppose China in the South China Sea. But we are not so confident that there are no connections between regional demonstrations of will and power. It is at least plausible, and perhaps safer, to argue that there are wider, global effects of probing. First, the world is indeed global, and regions are not hermetically separated from each other. As Nicholas Spykman observed, “Global war, as well as global peace, means that all fronts and all areas are interrelated. No matter how remote they are from each other, success or failure in one will have an immediate and determining effect on the others. It is necessary, therefore, to see the world as a whole and to weigh the measures taken to achieve victory in the light of conditions in all theaters. ”36 Leaders watch and learn from other regions, more than previously in history when conflicts were limited by technology and geographic knowledge to a contiguous region. Because of their domestic opacity, it is difficult to prove that America’s rivals learn from U.S. behavior in other regions, but the question whether they do so needs to be asked. Chinese military officials, for example, have commented publicly on lessons for China from the U.S. handling of the war in Ukraine.37 As one analyst noted, “It might be impossible to determine definitively whether the Ukraine Crisis has impacted China’s risk calculus in hotspots such as the South and East China Sea, but the evidence . . . certainly suggests that such eastern reverberations are quite plausible. ”38 At a minimum we have to recognize that some cross- regional analyses do occur, and it is safer to assume that the U.S. reputation does not stay limited to a region. Second, the much stronger effect of probing appears to be on U.S. allies and friends, the key geopolitical spectators. They watch how the United States treats other allies and form an opinion regarding American reliability. The former director of Saudi intelligence summed up the view of many officials from U.S. allied states in the Persian Gulf when he said in reaction to the Russian seizure of Crimea, “While the wolf is eating the sheep, there is no shepherd to come to the rescue. ”39 Israel was interested in the war in Georgia; Japanese analysts followed the Obama administration’s decision to cancel the Ballistic Missile Defense (BMD) program in Central Europe; and Polish experts watch U.S. moves in East Asia.40 The probing by revisionist states is first and foremost an attempt to test the strength of their rival’s commitment to its allies and friends. In sum, probing behavior by revisionist states targets these specific audiences in order to elicit responses from them. The goal is to figure out whether and how to draw the new map of power. And it puts the burden on the targeted audiences: their responses determine whether the probe is successful. EVALUATION OF PROBING: SUCCESS OR FAILURE From the perspective of the revisionist power that engages in probing, whether a probe has achieved its objectives determines its success or failure. The minimum objective of the probing state is to measure the rival’s staying power in its neighboring region, an objective that is achieved whether the targeted powers respond or not, but it is difficult to interpret. The targeted rival may be tempted to ignore the probe not out of a sense of its own weakness but in the belief that ignoring the test will send a signal of strategic insouciance from its pedestal of power. Also, because of the local and limited nature of a probe, directly involving only the regional actors, it is tempting for the distant security provider to leave the response to its allies and friends. A direct and strong intervention by the offshore patron would escalate the interaction, raising the chances of a larger war, an outcome that neither party desires. But the shrewdness of a probing strategy is that it puts the targeted rival power in the position of having either to escalate the tensions in order to respond or to choose a less confrontational approach but one that risks weakening its alliances. The response to the probe, not the probe itself, is perceived as a potential cause of war. This creates strong disincentives for the tested great power to react by opposing the revisionist state’s probe in a direct and forceful way, or to respond at all. For instance, in the case of China’s probing actions in the South China Sea, the Obama administration’s approach seems to have been to accommodate Beijing, acknowledging a decline in U.S. naval capabilities and welcoming a greater Chinese role in providing security to the global commons.41 Similarly, after Russia’s takeover of Crimea, Washington’s first response was to turn the episode into a strictly regional affair. As President Obama put it in February 2014, “Any violation of Ukraine’s sovereignty and territorial integrity would be deeply destabilizing, which is not in the interest of Ukraine, Russia, or Europe, ” tellingly not including the United States in the list of the affected parties.42 The problem is that the temptation of the existing great power to either ignore or regionalize the tension stemming from the revisionist state’s probes— an attempt to de- escalate the strategic interaction— also constitutes a response. It may, however, be one that serves for the revisionist power as a confirmation of its initial suspicion that the rival’s commitment to the region was on the wane. An unanswered— ignored or regionalized— probe is an indication that the existing map of power is open to revisions. Another way to put this is that a probe is a question of sorts: does the existing hegemon have the will and capacity to oppose the revisionist power? An attempt to dismiss the question or to let allies respond to it is a tacit admission by the tested great power that its interest in maintaining a strong foothold and influence in the region is in decline. Silence in response to a probe is telling. Probing, therefore, always elicits some sort of answer, and in this narrow sense it is a success. The purpose of a probe is also to attain a secondary, albeit crucial, goal of beginning to redraw the map of influence without generating counterbalancing pressures from the tested great power and its allies. The most successful probe would be one that pushes the targeted small states and other regional spectators closer to the revisionist power (or at least convinces them to distance themselves from their existing security patron, the rival great power) while at the same time convincing the rival great power that it is too costly to maintain its political influence and provide security in the region. Hence the probe needs to be evaluated on what it achieves in the three audiences: the directly targeted neighboring small state, the distant security patron, and the geopolitical onlookers (in particular other states in the region). The success or failure of a revisionist state’s probe depends on the actions by these three groups, and, arguably, it can attain partial success by achieving a revision of the status quo in one audience but not the other. For instance, a probe can succeed in extending the revisionist power’s influence over the immediate target, the ally or would- be ally of the rival, but at the same time it may generate more vigorous efforts by regional onlookers to counterbalance it through a variety of strategies, ranging from military modernization to tighter defense cooperation with the distant security patron. This seems to be the case for Russia’s takeover of Crimea. Moscow quickly conquered Crimea and destabilized Ukraine’s easternmost oblast, successfully demonstrating its ability and willingness to use force to achieve limited territorial adjustments. While Kiev maintains its political independence, it has also been shown to be weak and unable to oppose Russian pressures. The quasi– civil war in the eastern regions and Russia’s conquest of Crimea make Ukraine an unlikely candidate for a closer relationship with the EU and NATO, even if Ukrainian political elites and public opinion may continue to be in favor of it. Russia’s probe, in the form of its intervention in Crimea and eastern Ukraine, has thus been successful in neutering the westward drift of Kiev. The EU, and in particular states such as France and Germany, have now an even smaller desire to bring Ukraine closer, as it is deemed too dangerous and risky; Ukraine is not worth losing business deals with Russia, not to mention starting a war with Russia. The Ukraine War has also damaged American credibility in the region. Washington after all had given assurances (not “guarantees, ” which are reserved for NATO members) to the Ukrainian government in the Budapest Memorandum of 1994. This is undoubtedly a Russian success. But there are also other consequences of Russia’s probing, unintended and unwelcome by Moscow. Some states in the Central European region, in particular Poland and the Baltic states, have awakened from the geopolitical vacation of the past two decades. The 1990s and the 2000s were characterized by a widespread sense that threats to the territorial security of the region were minimal, and most of the strategic focus was on economic cooperation with the EU and on keeping in the good graces of the United States through participation in wars in Iraq and Afghanistan. This is over, at least in part. While strengthening the EU continues to be a priority in Central European capitals, there is simply no more interest in “out- of- area” operations, which drain resources and time from territorial defense. From this perspective, Russian probes have altered the geostrategic outlook of some Central European states. The eastern frontier is what really matters to them now, as their threat assessment has changed. Russia, in other words, has reached an upper threshold in its probes, creating a backlash among some of the states in the region, which are pursuing diplomatic counterbalancing and defense modernization. They are also calling for more visible and permanent NATO (and in particular, U.S.) security presence on their territories to shore up the extended deterrent against Russia. It appears therefore that Russia is less successful than the other revisionist power, China. Moscow is less subtle in its probes, choosing dramatic military interventions (Georgia and Crimea) that generate growing fear and opposition among some European states as well as the United States. In part Moscow’s more aggressive behavior is a result of a Russian assessment of the weakness and divisions of the West. But in part the seeming Russian rush to restore influence over its “near neighborhood” is due to internal demographic, economic, and political problems. The growing weakness of Russia, a great power more by courtesy and by nuclear weapons than by economic and political strength, gives little time to Putin to shore up his country’s position facing China’s rapid economic growth and Europe’s political appeal. It is a short- term approach of large probes, and it may be successful only by extending influence over its most immediate nearby target.43 China, on the other hand, may have a different time frame, allowing it to probe in a much more indirect and less violent way, though this could change in the months ahead. It is therefore more careful and guarded, pursuing a long- term strategy of small probes over, quite literally, small rocks in the South China Sea. The U.S. “pivot” or “rebalancing” to Asia makes American presence and resolve more pronounced, increasing the doubt of a U.S. retrenchment and thus, from China’s perspective, the need to be cautious in testing the limits of American influence and commitment. Moreover, the counterbalancing efforts of regional onlookers, from Japan to the Philippines and Vietnam, are increasing in intensity, in both the rhetoric used and the arms buildup. Similarly, unlike Russia in Crimea, Beijing has not succeeded in extending its direct control over a large piece of real estate. But in the end it may be more successful, because it is establishing a gradual change in the map of power, visible only after a decade- long period. Through its probes, China is pursuing a classic example of “salami tactics. ” As Thomas Schelling describes them, “If there is no sharp qualitative division between a minor transgression and a major affront, but a continuous gradation of activity, one can begin his intrusion on a scale too small to provoke a reaction, and increase it by imperceptible degrees, never quite presenting a sud den, dramatic challenge that would invoke the committed response. ”44 Many small probes into areas of contested influence do not individually invite a strong response, but they erode steadily the perception and in the end the reality of the opponent’s influence. Moreover, a continuing sequence of gradual probes signals the seriousness of the revisionist’s intent to alter the status quo. In the mind of the hegemon, the steady drumbeat of low- intensity and peripheral incidents creates the impression that the revisionist both has special claims for and may someday be willing to fight over a particular piece of real estate. These claims are often backed up by legal, historical, or ethnic justifications and a creeping physical presence— in Ukraine, Russian forces and equipment; in the South China Sea, artificially created reefs. Over time, this places the onus of a response on the shoulders of the hegemon and its allies in the region for why the status quo should be maintained. For a weary hegemon like the United States today, probes communicate that the act of supporting the regional status quo is no longer cost free but will require a level of exertion that was not needed in the past, inevitably leading to questions of whether such effort and resulting escalation are worthwhile. Nonetheless, it is certainly possible to see failed instances of probing, which achieve the opposite of the revisionist power’s intentions. The historic scorecard of probing states is mixed. A clear failure of probing would be if the targeted regional states and offshore security patron responded strongly, tightening their alliance and even initiating a direct war. This is an unintended consequence of a probe and can take several forms, from a tightening of alliances countering the revisionist power to increased military contingency planning and rearming. In the worst- case scenario, it results in a combination of actions that counterbalance the revisionist state more effectively and forcefully than before the probing behavior started. The revisionist state did not want nor expect this response before engaging in probing. It amounts to a disconfirmation of the initial hypothesis that the rival great power is in decline and retreat, and in the end it worsens the strategic position of the probing state. The biggest loser may thus be the probing power, which puts in motion a series of strategic interactions that undermine its own strength. This was the case of Germany in the early twentieth century. Kaiser Wilhelm’s visit to Tangier in 1905 initiated the first Moroccan crisis, manufactured by Berlin to, among other objectives, probe the strength of the brand new and untested Franco- British Entente Cordiale. 45 By challenging French interests in Morocco in a nonviolent way, Berlin wanted to pressure Paris, “the weakest link in the surrounding chain” of states opposing Germany.46 But it desired to do that in an area and in a way that were expected not to draw Great Britain into a direct confrontation, so that Germany could demonstrate to Paris that the entente was in effect useless. Morocco was important to France but not to Great Britain, and the German Foreign Office expected that London would not back Paris. Great Britain after all was also seen as retrenching after a bloody war with the Boers and unable and unwilling to project power on land to guarantee the security of its French quasi- ally. As Friedrich von Holstein put it, the French would seek a rapprochement with Germany, in effect bandwagoning, “when they have seen that English friendship . . . is not enough to gain Germany’s agreement to the French seizure of Morocco, but rather that Germany wishes to be loved on its own account. ”47 Germany, however, greatly miscalculated the British need for a continental ally and resulting commitment to France. The Moroccan crisis was resolved in a multilateral conference in Algeciras where Berlin ended in a position that was considerably worse than before the crisis: its only support was from the weak Austro- Hungarian Empire, while London was firmly and actively on the side of Paris. Instead of weakening the nascent strategic friendship between Britain and France, “German bullying” strengthened it.48 From then on, the “European Balance of Power, which had been ignored for forty years, again dominated British foreign policy; and henceforth every German move was interpreted as a bid for continental hegemony. ”49 London reoriented its attention away from the empire and toward the European continent, gradually planning to ready an expeditionary force to come to France’s defense.50 Berlin’s probe in Morocco turned into a clear failure.51 Probing is low risk, insofar as it is tailored to minimize a strong reaction of the rival, but it is not danger free for the revisionist state. Despite the fact that it arises out of a desire to clarify an allegedly new map of power, the effects of probing are difficult to interpret. All parties involved— the revisionist power and the targeted states— can miscalculate their reactions. In a case of moral hazard, the smaller states, directly targeted by the revisionist power, may respond violently to the low- intensity probe, feeling secure thanks to the alliance with a more powerful patron. Or, sensing that their distant patron is no longer capable of maintaining its influence, they may decide the exact opposite and accept the hegemony of the rival. This was the case of Athenian allies in Thrace, switching sides under General Brasidas’s pressure and persuasion. They were mistaken because their “judg ment was based more upon blind wishing than upon any sound prediction. ”52 Athens rallied and sent large forces north to restore its sway. The probing power can also be the one to miscalculate, either not seeing the success or ignoring the failure. The nature of probing is such that the effects are often not visible immediately and require time to alter the perceptions and realities of power. The episode of Spartan commander Brasidas is again telling. Sparta did not follow up on his successes, in part because Spartan kings were jealous of his military exploits, but in part because they thought the damage inflicted on Athens was sufficient to strike a deal and end the war.53 They were of course wrong, as the war continued for decades. Alternatively, despite being checked, the probing power may simply up the ante, seeking some gain. This may have been the case of Germany, which did not stop challenging France and Britain after 1905, despite its diplomatic isolation, the military conundrum of a two- front war, and a robust Franco- British entente. In brief, there is no easy single interpretation of a probe and its effects. A related risk is that a probe may lead to an unintended and untimely escalation of the strategic rivalry. As we described, the purpose of probing is to see how permissive the geopolitical order is, and to that goal a probe is limited in geographic reach and means used. It targets an issue presumed peripheral to the rival great power, seeking, for instance, a small territorial adjustment that is costly to the weaker neighboring state but not deemed worthy of a direct conflict by the distant and more powerful security patron. But the limited nature of the probe is somewhat at odds with its ultimate purpose to check the limits of an allegedly declining rival great power. A probe is a low- intensity, local pinprick with wider repercussions; limited geographically yet potentially global in outcome. The probing state has a strong interest in keeping the crisis limited and circum scribed to the narrowly defined area, but it is also poking the rival great pow er to see what the reaction may be. It is banking on the fact that the probe is on the periphery of the rival’s influence and interests, and thus that the rival will not escalate the interaction. The probing challenger, in other words, is betting that its great power rival will fear entrapment, being involved in an undesirable conflict, more than loss of prestige, reputation, or influence. The revisionist power seeks to use the fact of alliances (which it lacks itself) as a source of competitive disadvantage for the hegemon. This is based on two reinforcing perceptions— first, that the commitment involved in their maintenance is an encumbrance depriving the hegemon of strategic flexibility; and second, that the hegemon’s temptation to devalue its own alliances suggests that it feels the weight of this encumbrance. Probes therefore arise from a view that entrapment is the congenital flaw of alliances. They are the ultimate act of attempting to expose the dangers of entrapment to hegemon and ally alike. This is ultimately a gamble— an expectation, not a certainty. And the gamble can backfire, as there is always the possibility that a probe will result in a dramatic escalation since it is targeted at multiple audiences. There is thus a clear recognition that a probe has a much wider purpose than its immediate action may convey, and consequently the desire to keep it limited runs against the desire to have a much larger demonstrative effect. As a result, the interaction a probe initiates has an inherent risk of escalating into a much larger confrontation.54 The revisionist state neither desires nor expects the escalation, but its possibility and perhaps likelihood are a direct outcome of probing. A probe by definition crosses a limit, a tacit or an explicit line of influence, in the expectation that it no longer reflects the actual will and power of the rival state. The revisionist power tests limits that until then were accepted and unchallenged and takes the first step in an “escalatory ladder” of competitive behavior. For instance, Kaiser Wilhelm’s support of Boer independence in 1896 was a test of British strength in what Berlin wrongly thought was a peripher al area of the British Empire. Similarly, the Moroccan crisis in 1905 was a test of British commitment to France in a region that should have been of no importance to London. Both, however, were a “move in the European Balance of Power, ” and that, beyond the details of the individual probes, was becoming of paramount concern to Great Britain. 55 Both were met by a strong British response, intensifying the Anglo- British rivalry. Escalation here was a willful choice of the targeted power. Finally, probing can be in many cases a violent act, raising even further the likelihood of escalation and war. Probing is a political act first and foremost, only at times pursued by military means, but it does involve a careful application of violence or threat of violence. This requires strict political control, which is easier to maintain if the probe is not militarized and violent. But the more violent it becomes, the more difficult it is to keep it under political control. The logic of war may overwhelm the political rationale. Bismarck was keenly aware that the limited wars he fought, such as the Franco- Prussian one in 1870, would result in political outcomes that were different from his objectives were other great powers to become involved. But his greatest obstacle was the German military, resentful of civilian interference in what they deemed to be affairs in their exclusive purview. Political control over a limited war is paramount, because otherwise operational war objectives can overwhelm the larger political goals.56 The fact that Russia and China probe through a variety of nontraditional means, such as fishing vessels in the South China Sea and specially formed battalions (Vostok) of Chechens, makes political control more difficult. There is an incentive to use such means in a more aggressive way than would be warranted by official state forces, because in case of defeat one can always deny control over them and claim that they are simply individual citizens. Moreover, the “civilian” paramilitary forces that the probing power uses (e.g., the “Russian separatists” in eastern Ukraine) may not be easily recalled if the conflict ceases to be useful. The civilianization of conflict has its own risks. This makes probing behavior inherently destabilizing to an international order, as it sets forces in motion that, once unleashed, can be hard to control. Probing can, moreover, spiral into war, unexpected and perhaps unwanted by the revisionist power. For instance, in the third century BC, Rome started to probe Carthaginian power in Sicily. It extended protection to Messana (or, more precisely, to a band of mercenaries, the Mamertines, who controlled it), thereby asserting Roman influence in northern Sicily. The peaceful withdrawal of the Punic garrison from the area seemed to suggest that a war was avoidable and the probe successful in attaining a low- cost revision to the balance of power. But the Romans miscalculated and were emboldened by this small success. As Polybius put it, they “now cherished the hope that they could drive the Carthaginians out of Sicily altogether, and that once this goal was attained their own power would be greatly increased. ”57 Carthage sent a large force to Sicily and solidified its alliance with Syracuse against Rome and its new ally Messana. Rome then escalated and sent a large army to besiege Syracuse, starting the first Punic war, which lasted more than twenty years.58 What started as a low- cost, low- risk probe turned into a long and costly slugfest. To sum up, the risk of probing is that it may result in a slide toward a direct clash. Miscalculation and escalation by all parties involved can elevate what is a small, localized harassment into a wider, more violent war. Moreover, a pattern of probing may gradually lead all sides to accept war as necessary and perhaps inevitable, as each probe and reaction escalates the competitive interaction.

**And a unified NATO stops every existential threat.**

**Kolga 21** – founder of DisinfoWatch.org and is a senior fellow at the Macdonald-Laurier Institute’s Centre for Advancing Canada’s Interests Abroad

Marcus Kolga, "Improving NATO’s cohesion is critical to combat Russia and China’s threat: Marcus Kolga for Inside Policy," Macdonald-Laurier Institute, 10-5-2021, https://macdonaldlaurier.ca/improving-natos-cohesion-critical-combat-russia-chinas-threat/

A united NATO is critically important to projecting credible deterrence. The erosion of domestic trust and confidence in the Alliance among its member states, including Canada, represents a threat to this cohesion. A proposal to withdraw Canada from NATO was tabled at a recent policy conference for one of Canada’s three major political parties. The proposal was defeated, but it represents a fringe anti-NATO narrative within Canada’s illiberal left; if left unaddressed, such a narrative could grow.

If countries like Russia perceive NATO as an atomized collection of states with varied priorities rather than a unified front, the Alliance is exposed to a significant risk of miscalculation in which a foreign adversary might believe they can cross a red line and only face a limited response. Thus, gaps in cohesion within the alliance directly threaten to undermine political and military deterrence. The Alliance and members states must work towards improving communications strategies to foster greater basic general understanding of NATO’s purpose, its missions and its role in protecting its members against external threats.

Similarly, if we see threats as atomized or disparate, we may lack the capacity to adequately respond. Organized GRU terrorist attacks in Czechia, the Salisbury poisonings, transnational repression and censorship, cyberwarfare, disinformation, and overt military posturing all pose threats that are aimed at the same essential goal: undermining and supplanting the power of liberal democracy and advancing authoritarianism. Through this lens, challenges posed by other actors, including China, must also be considered as part of the broader range of shared threats posed to the democratic community as a whole.

If we are to succeed in tackling these shared threats, greater transatlantic cooperation is needed. It cannot remain stagnant, however; it must evolve and expand. The serious nature of the threats, their potential to become kinetic, and the possibility of adversarial coordination (whether formal or informal) means that we must expand our tools to meet these challenges.

In the case of Ukraine, on whose border the Kremlin mobilized over 100,000 troops this past summer, the Alliance should consider extending a Membership Action Plan despite the skepticism of some allies. Ukraine must also be empowered in a similar fashion to frontline NATO states like the Baltic states and Poland. After all, the eFP mission in Latvia not only provides military deterrence, but strengthens interlinkages, develops societal resilience, and provides clear and sustained solidarity.

Finally, the growing threats of foreign interference, information warfare, cyber attacks and emerging threats to Canada’s Arctic requires a coherent long-term strategy and an evolved notion of collective defence, which includes strengthening our partnerships with non-NATO allies in Europe, Asia, and around the world.

#### The US can’t do it alone --- Cooperative integration with alliances is key

Joseph S. Nye 20. Harvard University Distinguished Service Professor, Emeritus. "COVID-19’s Painful Lesson About Strategy and Power". War on the Rocks. 3-26-2020. https://warontherocks.com/2020/03/covid-19s-painful-lesson-about-strategy-and-power/

In 2017, President Donald Trump announced a new National Security Strategy that focused on great-power competition with China and Russia. While the plans also note the role of alliances and cooperation, the implementation has not. Today, COVID-19 shows that the strategy is inadequate. Competition and an “America First” approach is not enough to protect the United States. Close cooperation with both allies and adversaries is also essential for American security. Under the influence of the information revolution and globalization, world politics is changing dramatically. Even if the United States prevails in the traditional great-power competition, it cannot protect its security acting alone. COVID-19 is not the only example. Global financial stability is vital to U.S. prosperity, but Americans need the cooperation of others to ensure it. And while trade wars have set back economic globalization, there is no stopping the environmental globalization represented by pandemics and climate change. In a world where borders are becoming more porous to everything from drugs to infectious diseases to cyber terrorism, the United States must use its soft power of attraction to develop networks and institutions that address these new threats. For example, this administration proposed halving the U.S. contribution to the World Health Organization’s budget — now we need it more than ever. A successful national security strategy should start with the fact that “America First” means America has to lead efforts at cooperation. A classic problem with public goods (like clean air, which all can share and from which none can be excluded) is that if the largest consumer does not take the lead, others will free-ride and the public goods will not be produced. As the technology expert Richard Danzig summarizes the problem: Twenty-first century technologies are global not just in their distribution, but also in their consequences. Pathogens, AI systems, computer viruses, and radiation that others may accidentally release could become as much our problem as theirs. Agreed reporting systems, shared controls, common contingency plans, norms and treaties must be pursued as a means of moderating our numerous mutual risks. Tariffs and border walls cannot solve these problems. While American leadership is essential because of the country’s global influence, success will require the cooperation of others. On transnational issues like COVID-19 and climate change, power becomes a positive-sum game. It is not enough to think of American power over others. We must also think in terms of power to accomplish joint goals, which involves power with others. On many transnational issues, empowering others helps us to accomplish our own goals. The United States benefits if China improves its energy efficiency and emits less carbon dioxide, or improves its public health systems. In this world, institutional networks and connectedness are an important source of information and of national power, and the most connected states are the most powerful. Washington has some sixty treaty allies while China has few. Unfortunately, as Mira Rapp-Hooper recently argued, the United States is squandering that power resource. In the past, the openness of the United States enhanced its capacity to build networks, maintain institutions, and sustain alliances. But will that openness and willingness to engage with the rest of the world prove sustainable in the current populist mood of American domestic politics? Even if the United States possesses more hard military and economic power than any other country, it may fail to convert those resources into effective influence on the global scene. Between the two world wars, America did not and the result was disastrous.

## Adv --- OCO’s

### 2AC --- Terror A/O

#### **Evolving technologies make kinetic terrorist attacks an increasingly likely option**

Missiroli 19 – Antonio Missiroli, Dr. Antonio Missiroli is the Assistant Secretary General for Emerging Security Challenges. As well as being a professional journalist, he has also taught at Bath and Trento as well as Boston University, SAIS/Johns Hopkins, at the College of Europe (Bruges) and Sciences Po (Paris). Dr. Missiroli holds a PhD degree in Contemporary History from the Scuola Normale Superiore (Pisa) and a Master’s degree in International Public Policy from SAIS/Johns Hopkins University, 1/7/2019, “NATO and the South,” <http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/missiroli-nato-and-the-south>

Terrorists are also making an increasing use of modern technologies. While there have been no cases of ‘cyber-terrorism’ –ie, no proved terrorist act carried out through cyber means only– terrorist groups have indeed used cyberspace for recruitment and funding as well as operational purposes. This is an area where intelligence agencies are very busy and alert, although these activities are unlikely to reach the level of sophistication and disruption that only State-sponsored groups can achieve in this domain. There is, however, a growing concern about the possible use of unmanned vehicles for kinetic terrorist attacks –and not only on the battlefield (where they have already occurred) but also in civilian and especially urban environments–. What happened around Christmas 2018 at Gatwick airport in London was quite telling, especially in light of the commercial affordability and availability of such tools and their potential impact on civilian life. NATO has just launched a specific initiative to counter –on the battlefield but potentially also elsewhere– such a misuse of new technologies by terrorists.

#### US integration of OCO’s with allies is key to stop terrorism --- They don’t have the authority or capabilities to do it themselves

Pomerleau, 19 (Mark Pomerleau, Mark Pomerleau is a reporter for C4ISRNET, covering information warfare and cyberspace., 4-2-2019, accessed on 6-18-2022, C4ISRNet, "How military hacking can improve", <https://www.c4isrnet.com/international/2019/04/02/how-military-hacking-can-improve/)//Babcii>

It’s not just the United States that has unique offensive cyber capabilities. In a March 27 speech, Mike Burgess, Australia’s director general of the Australia Signals Directorate, [detailed](https://asd.gov.au/speeches/20190327-lowy-institute-offensive-cyber-operations.htm) how his government’s hackers conducted operations against ISIS in Syria to aid military ground forces as part of the global coalition to defeat the terrorist group. Burgess said this was “the first time that an offensive cyber operation had been conducted so closely synchronized with the movements of military personnel in theater.” The Australian offensive cyber operation took place in conjunction with a ground raid on an Islamic State position and degraded ISIS communications 11,000 km from the battlespace so commanders couldn’t connect to the internet or communicate with each other. The speech was [first reported by the Washington Post](https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/03/29/the-cybersecurity-202-trump-wants-a-cybersecurity-moonshot-but-cuts-research/5c9d4b301b326b0f7f38f2b1/?utm_term=.2f952ed629d8). The operation is similar to those described by U.S. officials, who have detailed operations conducted by U.S. Cyber Command as well as partner forces supporting ground operations as part of the coalition. In some cases, U.S. officials have described the importance of the partnerships and capabilities of other nations in these contexts because sometimes the United States **might not have the authority** or the **access to conduct the cyber effect itself.** “What we recognize is we have some **foreign partners** that **give us very unique access or very unique capabilities**. They operate off of different authorities that compliment our own authorities so **they are very, very important**,” Lt. Gen. Stephen Fogarty, commander of Army Cyber Command, told reporters in October. “Episodic synchronization” The nature of remote cyber operations, despite common conception, **are incredibly arduous**. They involve first gaining access to adversaries’ networks, mapping those networks to understand where things are and then figuring out how to degrade or destroy portions of the network. Complicating matters further, if an adversary changes portions of the network via a software patch — an anomaly with no physical world comparison — the **access gained could be negated**. In the Australian example, Burgess said, “While the effect was almost instantaneous, it took weeks of planning by specialist ASD and [Australian Defense Forces] personnel to make sure it **all went exactly to plan.”** Indeed, despite the success of the Australian cyber operation and other similar operations detailed by U.S. officials, others have lamented that such operations today take too long to plan and only have a limited effect.

#### Nuclear terror causes extinction

Arguello and Buis, 18 – \*Irma, Founder and Chair of the NPSGlobal Foundation (Non-proliferation for Global Security), degree in Phyisics Science from the University of Buenos Aires, Master degree in Business Administration from IDEA/Wharton School, Defense and Security studies (Master level) at the Escuela de Defensa Nacional, Argentina; \*\*Emiliano, lawyer and associate professor of public international law, international humanitarian law, international law of disarmament, and the origins of international law in antiquity (Irma Arguello & Emiliano J. Buis, **“**The global impacts of a terrorist nuclear attack: What would happen? What should we do?,” *Bulletin of the Atomic Scientists*, 2018, https://doi.org/10.1080/00963402.2018.1436812)

But the consequences would go far beyond the effects in the target country, however, and promptly propagate worldwide. Global and national security, economy and finance, international governance and its framework, national political systems, and the behavior of governments and individuals would all be put under severe trial. The severity of the effects at a national level, however, would depend on the countries’ level of development, geopolitical location, and resilience. Global security and regional/national defense schemes would be strongly affected. An increase in global distrust would spark rising tensions among countries and blocs, that could even lead to the brink of nuclear weapons use by states (if, for instance, a sponsor country is identified). The consequences of such a shocking scenario would include a decrease in states’ self-control, an escalation of present conflicts and the emergence of new ones, accompanied by an increase in military unilateralism and military expenditures. Regarding the economic and financial impacts, a severe global economic depression would rise from the attack, likely lasting for years. Its duration would be strongly dependent on the course of the crisis. The main results of such a crisis would include a 2 percent fall of growth in global Gross Domestic Product, and a 4 percent decline of international trade in the two years following the attack (cf. Figure 3). In the case of developing and less-developed countries, the economic impacts would also include a shortage of high-technology products such as medicines, as well as a fall in foreign direct investment and a severe decline of international humanitarian aid toward low-income countries. We expect an increase of unemployment and poverty in all countries. Global poverty would raise about 4 percent after the attack, which implies that at least 30 million more people would be living in extreme poverty, in addition to the current estimated 767 million. In the area of international relations, we would expect a breakdown of key doctrines involving politics, security, and relations among states. These international tensions could lead to a collapse of the nuclear order as we know it today, with a consequent setback of nuclear disarmament and nonproliferation commitments. In other words, the whole system based on the Nuclear Non- Proliferation Treaty would be put under severe trial. After the attack, there would be a reassessment of existing security doctrines, and a deep review of concepts such as nuclear deterrence, no-firstuse, proportionality, and negative security assurances. Finally, the behavior of governments and individuals would also change radically. Internal chaos fueled by the media and social networks would threaten governance at all levels, with greater impact on those countries with weak institutional frameworks. Social turbulence would emerge in most countries, with consequent attempts by governments to impose restrictions on personal freedoms to preserve order – possibly by declaring a state of siege or state of emergency – and legislation would surely become tougher on human rights. There would also be a significant increase in social fragmentation – with a deepening of antagonistic views, mistrust, and intolerance, both within countries and towards others – and a resurgence of large-scale social movements fostered by ideological interests and easily mobilized through social media.

### 2AC --- Grid Impact A/O

**Independently, Russian attacks on Eastern European critical infrastructure are intensifying---that ensures increasingly destabilizing aggression.**

**Park et al. 17** – Assistant Professor, Korea Army Academy at Yeongcheon, Ph.D., University of Washington

Donghui Park, Julia Summers, Michael Walstrom, “Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks,” University of Washington Henry M. Jackson School of International Studies, October 2017, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/#\_ftnref90

Ukraine’s crisis is ultimately a part of a **larger system of events** in the East-European region. Russia is conducting its foreign policy in the region chiefly based on its perception of the ongoing events there and their impact on Russia’s foreign and domestic interests. To achieve its goals, Russia is using various methods to influence the course of development that its neighbors choose to pursue. The methods now appear to include, among others, the combination of conducting the covert military operations on the ground and in cyberspace, spreading of pro-Russian and anti-Western disinformation domestically and internationally, as well as **attacking various elements** of **critical infrastructure** and **exerting control over** the **national economies** of the **Eastern European states**.

While the West’s economic sanctions against Russia are working, the Kremlin seems to retaliate in **increasingly aggressive ways** in **cyberspace** and on the ground against Ukraine. With the presidential elections around the corner, Russia possibly will **intensify** its **hybrid warfare operations** in the region, **especially** if Russia’s **internal affairs** follows **current unstable trajectory**.

The pattern in Ukraine could be a **foreshadowing** of the **future for all states**. The **number of cyberattacks** are **on the rise** and the **most sophisticated** among them have been attributed to **nation-state actors**.[90] Nation-states have the resources and the intelligence available to conduct multilayered and well-orchestrated attacks over long periods of time. The **evolving security threats** from cyberattacks led by nation-states range from **espionage** to **cyberattacks on critical infrastructure**. The motivation to use cyberspace as a fifth domain of conflict is driven by relatively low costs, the covert nature of cyber operations, and the strategic advantage they present, as opposed to conventional warfare. Through cyberattacks nation-states strive to achieve geopolitical and economic goals that otherwise might seem unattainable to them.[91] The Russian attacks on Ukrainian **electricity distribution companies** perfectly captures the nature of this new landscape and how embedded it is in existing geopolitical relations.

**European grid collapse cascades---cross-country dependencies mean collapse rips across countries.**

**Starn et al. 21** – Writer for Bloomberg

Jesper Starn, Brian Parkin, Irina Vilcu, “The Day Europe’s Power Grid Came Close to a Massive Blackout,” Bloomberg, January 2021, https://www.bloomberg.com/news/articles/2021-01-27/green-shift-brings-blackout-risk-to-world-s-biggest-power-grid

Germany is the biggest producer of green electricity in Europe. The nation is culling a quarter of coal and nuclear capacity next year, a gap it will need to plug. Instead of building a huge fleet of batteries, Germany plans to **rely more on more its neighbors**, **importing power** along huge cables.

The event shows that **problems in one nation** will **rapidly cascade between states** as they **become more reliant** on their **neighbors** for power, said Wolfgang Kroeger, a professor at the ETH university’s Risk Center in Zurich.

Continental Europe was separated into two areas due to “outages of several transmission network elements in a very short time,” according to Entsoe, the association of grid operators. “Further detailed investigation” is ongoing.

“**Longer**, **harder to fix disturbances** that **rip across countries** are a **real threat**,” said Kroeger.

**Now is key---the US power grid is increasingly vulnerable, Russian intrusions are increasing, and catastrophic hacks are an inevitability absent the aff.**

**Cunningham 21** – Opinion contributor for USA Today

Jim Cunningham, “Extreme weather is the culprit in the Texas power crisis, but that's not our worst problem,” USA Today, February 2021, https://www.usatoday.com/story/opinion/2021/02/19/texas-power-crisis-real-threat-cyberattacks-not-weather-column/4491652001/

Today the culprit in Texas and several other states is extreme winter weather, but the **greater threat** we face is **not weather related**. It is the **daily bombardment** of **cyberattacks** on our nation’s **critical infrastructure** — most notably on the **electric sector** that provides the power upon which the rest of that infrastructure relies to operate.

Just last December, we learned that hackers linked to Russia infiltrated numerous American companies and federal agencies, including the Department of Homeland Security and the Pentagon. Microsoft President Brad Smith told CBS News that, by its analysis, the number of engineers required to pull off the now infamous SolarWinds hack was “certainly more than 1,000.”

Danger from Russia and China

Separately, utility executives acknowledge their companies are subjected to **literally millions** of **cyberattacks per day**. And it was widely reported last summer that the National Security Agency issued a **warning** to **critical infrastructure operators** regarding **cyberattack threats** to **industrial control systems**.

This quiet but **unceasing barrage** of **sophisticated cyber intrusions** by **Russia**, China and others, similar to the more high-profile situation in Texas today, highlight the fact that upgrading the U.S. electric grid needs to be a national priority, and the cost of doing so should be shared equitably by federal and state governments, electric utility companies and consumers. Such a program could include grants, low-interest loans and other incentives to dramatically improve and modernize the grid.

**Yes access, short timeframe, and the threshold is low---Russia’s already compromised our utilities, which proves motive is all that matters---try-or-die for deterrence.**

**Vasquez 20** – E&E News reporter

Christian Vasquez, “Huge federal hack ripples across energy industry,” E&E News, December 2020, https://www.eenews.net/stories/1063720933

Electric utilities are **grappling** with the **fallout** from one of the most **significant cyber intrusions in years**, as the **far-reaching impact** of a **sophisticated hacking campaign** comes into sharper focus.

Four days after the supply chain cyberattack on IT service provider SolarWinds was revealed, details on its global victims — from federal agencies to oil and electricity companies — are still emerging (Energywire, Dec. 15).

The SolarWinds software hijacked by suspected **Russia-linked hackers** was **widely used by U.S. power providers**, experts say, leaving many companies scrambling to find out if they're affected by the breach. And sources say a simple software update or patch **won't erase** the **threat** from the "Sunburst" malware: Organizations targeted by the hackers will likely have **additional malware installed** that could be **difficult to find**.

"Any organization that says, 'Yep, we got it solved. It's all good,' in the next 90 days: I would respectfully disagree," said Jim Guinn, global managing director for cybersecurity in energy, chemicals, utilities and mining at Accenture.

The number of agencies and organizations that may have been hit by the cyber espionage campaign is unclear. Reuters first reported that the Commerce, Treasury and Homeland Security departments were among those targeted. The list of agencies has since grown to include the State Department and the Pentagon, The New York Times reported, citing anonymous sources familiar with the ongoing investigations.

In a joint statement yesterday, DHS's Cybersecurity and Infrastructure Security Agency, the FBI and the Office of the Director of National Intelligence said they have formed a "Cyber Unified Coordination Group to coordinate a whole-of-government response" to the hacking campaign.

"This is a developing situation, and while we continue to work to understand the full extent of this campaign, we know this compromise has affected networks within the federal government," the agencies said.

The scope of customers that used SolarWinds ranges from **government agencies** to **Fortune 500 manufacturers** and **power utilities**. In an SEC filing, SolarWinds estimated that 18,000 or fewer customers downloaded the malicious update containing the Sunburst malware.

According to federal records, the Federal Energy Regulatory Commission and the Bureau of Ocean Energy Management had contracts with SolarWinds in recent years. It's not clear if the Orion product was used and if those agencies downloaded the malicious update. The Department of Energy's Sandia and Oak Ridge national laboratories also used SolarWinds, according to a now-deleted webpage listing the Austin, Texas-based IT firm's customers.

DOE did not respond to requests for comment. FERC declined to comment. BOEM deferred comment to DHS, which is leading the federal response to the hack.

Utilities affected

SolarWinds' customer page also listed the **New York Power Authority** as a client. NYPA confirmed it uses SolarWinds products and said they are working in "close collaboration with our industry cybersecurity associations and government agencies" to determine the potential impact.

"Our thorough analysis has so far determined that there are no adverse impacts or exposures to our systems," an NYPA spokesperson said. "We continue to review our layered security controls to ensure that activities associated with this threat are appropriately blocked and we will take all necessary steps to secure our networks."

The **scope of the breach** has put **utilities across the country** on **high alert**. San Francisco-based Pacific Gas and Electric Co. told E&E News that even though they did not have SolarWinds products installed on their company networks, "out of an abundance of caution we conducted an assessment and found no impacts or breach of our network resulting from this attack," a PG&E spokesperson said.

The Electricity Subsector Coordinating Council, whose energy industry CEO members help coordinate the U.S. response to grid emergencies, held a "situational awareness call" Monday on cyberthreats from SolarWinds.

Some critical infrastructure operators have already been hacked, according to cybersecurity companies. Industrial cybersecurity firm Dragos Inc. said that there are "industrial entities compromised in this campaign." Dragos has customers globally, and the company did not specify where the victims were based.

**Fully rebuilding trust** in IT systems is going to be a **long haul**, cybersecurity experts say, and **rooting out** the **Sunburst malware** is **just the beginning**.

The SolarWinds campaign began as early as **March**, according to cybersecurity firm FireEye Inc. and Microsoft Corp., meaning the hackers have had **ample time** to **create additional backdoors** and **malware**.

In a statement yesterday, a FireEye spokesperson said that they have discovered a "kill switch" in the Sunburst malware that can deactivate it. FireEye also said that, alongside Microsoft and domain registrar GoDaddy Inc., it had seized control over one of the internet domains used by the hackers to send commands to compromised computers.

However, FireEye warned that the hackers "**moved quickly** to **establish additional persistent mechanisms** to **access to victim networks**" — and the kill switch **won't cut off** those other **backdoors**.

"You're talking about someone who broke into the Smithsonian and has been there for eight months looking and figuring out which are the most expensive pieces of art to steal," Accenture's Guinn said.

Guinn said the **biggest threat** from the hacking campaign is not the Sunburst malware but the other **potential backdoors** that could have been installed. Utilities need to **assume** they've been **compromised** and proactively hunt for other possible cyberthreats, Guinn said — a painstaking process that could take months.

"Every one of the **critical utilities globally** that know that they have used these software packages ... need to take this **very seriously**. I would even say to the extent it would be as if it was a **massive outage**," Guinn said.

**Grid collapse is an existential threat.**

**Gray 19** – Senior journalist at BBC Future Richard Gray, “What would happen in an apocalyptic blackout?,” BBC Future, October 2019, https://www.bbc.com/future/article/20191023-what-would-happen-in-an-apocalyptic-blackout

“So much of our lives and **almost everything we do** is **now dependent on energy**, and particularly on our electricity supplies,” says Juliet Mian, technical director of the Resilience Shift, an initiative to help organisations and individuals prepare for failures in critical infrastructure. “We used to use the phrase ‘when the lights go out’, but the lights not working are the least of our worries now.” She is right. While the term “black sky” events illustrates perhaps the most visible impact of widespread power failures, it fails to convey the scale of the impact these can have. In our modern world, **almost everything**, from our **financial systems** to our **communication networks**, are **utterly reliant upon electricity**. **Other critical infrastructure** like **water supplies** and our sewer systems rely upon electric powered pumps to keep them running. With no power, fuel pumps at petrol stations stop working, road signs, traffic lights and train systems go dead. **Transport networks** grind to a halt. Our **complex food supply chains** quickly **fall apart** without computers to coordinate where produce needs to be, or the fuel to transport it or refrigeration to preserve it. Air conditioning, gas boilers and heating systems also rely upon electricity to work. A little over 100 years ago, our cities ran on human and animal muscle power to ferry goods and waste around. **Modern infrastructure** is now **utterly reliant upon electricity**. “In today’s world, our systems are **highly interdependent** and it is very hard to find many systems that are not fundamentally reliant upon power,” says Mian. “A black sky scenario will affect everyone.” The causes of a black sky event are many. They vary from natural disasters like hurricanes or earthquakes to geomagnetic storms triggered by enormous flares from the Sun, or coronal mass ejections, that send a barrage of electrically charged particles racing across the Solar System and can overload electrical grids. One intense geomagnetic disturbance caused a nine-hour outage across large areas of Canada in 1989. The Electric Infrastructure Security Council, an international body that reviews threats to power grids, also lists a number of **human threats** that **can trigger** a **mass black out**. These include **cyberterrorism attacks** or coordinated physical assaults on energy infrastructure such as power stations, and electromagnetic pulses that can disable electricity grids. “Our national power grids are tremendous feats of engineering and operations that have supported rapid economic growth around the world,” say Melissa Lott, a research fellow at the Center on Global Energy Policy at Columbia University in New York. “But more investment is needed if electric power grids are going to keep up with rapid technology shifts and increasingly extreme weather events.” She says that while true black sky events are mercifully rare, the deep impact they have on businesses and people means more needs to not only update grid technology and management, but also improve infrastructure so it can be more resilient against physical threats like flooding. “In the summer of 2012, blackouts in India cut power to more than 600 million people over two days. In Puerto Rico, Hurricane Maria crippled infrastructure across the island, leaving people in the dark and triggering a humanitarian crisis. In 2018, an earthquake on Japan’s Hokkaido island left more than 5 million people without power. In order to keep these events from becoming more common and to minimise their impact, we need to invest in our grids.” Putting measures in place to counter all of these potential threats is difficult and expensive. Critical systems can be guarded from human attacks and they can be shielded from electromagnetic pulses with enough money being spent on them. Building new systems for protecting transformers from coronal mass ejections can also help to keep systems safe. But there are some events that cannot be planned for and the complex, interconnected nature of our electricity grids are remarkably vulnerable. Take what happened in September 2003 when a fallen tree brought down a power line in Switzerland’s Lukmanier Pass over the Alps into Italy and 24 minutes later another tree came down onto a line in the nearby Great St Bernard pass. The sudden failure of these two key lines caused other connections to Europe’s electricity network to trip, which triggered power plants across Italy to shut down. The whole of Italy was left without power because of two fallen trees starting a cascade of events. Modern electricity grids are increasingly interconnected and complicated, making failures like this difficult to predict. **Most of Europe** now runs off a **massive interconnected power grid** – probably the largest in the world – that supplies more than 400 million customers in 24 countries. The USA is made up of five different grids. But there are some that are seeking ways of anticipating potential power failures and are enlisting the help of artificial intelligence to help them grapple with this highly complex problem. When a power plant goes down, for example, it causes an **abrupt spike in load** on others on the network, which in turn slows down the generators at these plants and causes the frequency held on the grid to decrease. This **risks destabilising** the delicate balance that electricity grids are held in, and operators have to deploy countermeasures rapidly – often within milliseconds – to prevent sections of the grid being cut off. Researchers at the Fraunhofer Gesellschaft research institute in Ilmenau, Germany, recently revealed they are developing an AI system to automatically detect these disturbances and take steps to address them. The US Department of Energy is also funding $7m (£5.4m) of research into using artificial intelligence to not only predict potential outages and spot anomalies that might lead to larger problems, but also to help find ways of keeping supplies constant in the event of a problem. General Electric is using machine learning to help analyse weather forecasts past outage history and information on the ground from its response crews to predict the impact that impending storms might have on its networks. It is also using it to predict where its repair crews might need to be so that downed lines can be restored more quickly. Power grids can also help to protect themselves by increasing the amount of energy storage such as large scale batteries they have available so that supplies can be supplemented when generators do go off-line unexpectedly. But completely protecting our power networks from failures is almost impossible, says Mian. “We can’t necessarily design our systems so that failures don’t happen,” she says. “There’s so much complexity in our systems these failures can cascade and they can become much more widespread, which means the failure is quite often unavoidable. But what we can do is design our systems so that they can respond and recover quickly.” This is what the Resilience Shift is now trying to improve. It has been organising exercises in collaboration with the Electric Infrastructure Security Council (EIS) that help large organisations, universities, schools, community groups and even families prepare themselves for an event that might lead to mass power cuts for several days at a time. The Emergency All-sector Response Transnational Hazard Exercise, or Earth Ex, is an online exercise that allows people to rehearse the decisions they need to make and put in place the plans they need should the worst happen. (Try Earth Ex for yourself and see how prepared you are.) “We want people to be thinking about these things long before there is a problem,” says John Heltzel, director of resilience planning at the EIS. “It’s important because when the electricity grid fails, there is this risk of cascading impacts that can occur from what might at first seem to be a relatively minor event. This **cascade effect** is where the **real damage can be done**. As the people of Venezuela have discovered, even basic service like water can stop when the power goes out. “It’s effectively [like **going**] **back to the dark ages**,” says Heltzel. A report by scientists at University College London mapped out how the loss of power can filter through communities, from the loss of health care provision and sanitation services to citizens trapped in lifts and disruption to transport systems. Then there are the **social consequences** that percolate out. **Crime rates** often go up during blackouts as they provide opportunities for theft and fraud. The supply of cash and credit – particularly in our modern societies so reliant upon electronic and card payments – **dry up** meaning people have to rely on whatever cash they happen to have squirreled away. **Communication networks and** the ability to contact loved ones **disappear**, while vulnerable people like the elderly are often left stranded in their own homes. **Businesses** are also left largely **unable to operate**, resulting in **huge economic impacts**. In 2004, the Department of Energy estimated the annual cost of power outages in the US to be around $80bn (£62bn) annually. When two million customers in California had their supplies cut for two days in October this year, experts estimated the cost to the economy to be around $2.5bn (£1.9bn).

### 2AC --- Iran A/O

**Iran will escalate GPS attacks, causing escalation in the Persian gulf**

Micah **Halpern 2019**, former lecturer @ Yale, has also taught at Brandeis University and the Hebrew University of Jerusalem, political and foreign affairs commentator, 8 August 2019, “Iran Plays a Dangerous Hi-Tech Game,” https://www.newsmax.com/micahhalpern/strait-of-hormuz-jamming-centcom/2019/08/08/id/927875/

Iran is playing dirty tricks in and around the Strait of Hormuz.

To begin with, they are **jamming the GPS of tankers**, causing ships to wander off course —and in to their waters. They are also **spoofing andradioing the vessels**, proporting to be friendly and even **U.S. navy ships**.

Over the years the Iranian leadership has perfected the art of mixing and matching partial truths with outright lies in order to advance their agenda. They want to convince global observers that it is the Iranian leadership who are the innocent victims, innocent victims targeted by organized Western aggression.

In this case Iranians are deliberately dogging, misleading and **luring ships off course**.

Their actions have turned into **a war of jamming**.

Like most everything else they engage in, for Iran this is serious business.

Globally this is **extremely dangerous**. We are seeing signs **all over the Mideast**.

The U.S. Department of Transportation Maritime Division published a public warning to all ships and companies traveling in the region alerting them that Iran "spoofed bridge-to-bridge communications from unknown entities falsely claiming to be U.S. or coalition warships."

U.S. Central Command (CENTCOM) said in a statement, "Due to the heightened regional tensions, **the potential for miscalculation** or misidentification **could lead to aggressive actions** against vessels belonging to US, **allied** and coalition partners operating in the **Arabian Gulf**, **Strait of Hormuz**, **and Gulf of Oman** . . . **GPS interference**, bridge-to-bridge communications **spoofing**, and/or other communications jamming with little to no warning."

Bridge-to-bridge communication is when ships speak to one another.

Iran has been become **expert** at jamming.

That shouldn’t come as a big surprise given that as far back as 2012 the Iranian government has been jamming their own citizens. Back then, Iran replaced a series of short flagpoles scattered around their country with huge flagpoles – all the better to hide their jamming devices.

The newer, taller, flagpoles sprouted up almost everywhere. The Iranian regime was attempting to stop all forms of social media and messaging. Their citizens were using satellites to communicate and find out the truth about what was happening in the world and that was not what Iranian leadership wanted.

The **Russians**, too, have become **very good at GPS jamming**. Intelligence analysts report that Russia is jamming not waterways, but airspace, specifically the airspace around **Syria**. And that means that Russia is now capable of jamming communication for the **new US stealth fighter jet, the F-35**. This may be an exaggeration -I am skeptical that Russia is that sophisticated.

Even more worrisome than all of this is a report that was issued this summer by the International Federation of Airline Pilots Association. The report details that pilots, landing in Tel Aviv’s Ben Gurion Airport in Israel, have lost GPS and that it is a recurring phenomenon.

Thankfully, there are alternative tools that can be used to land and take off. Israel has said that they are dealing with the issue. But the mere presence of this issue demonstrates that we now live in a world hampered — **dangerously so**, **by a significant threat of jamming**. And this jamming can and is affecting more than ships at sea and military drones and jets in the sky, it is also targeting civilian aircraft with hundreds of civilian passengers aboard.

When it comes to tech, Iran is highly skilled.

They are developing their own tools and are using and adapting Russian and North Korean tech.

**Jamming** and **spoofing by Iran** explains quite a lot of what has been happening in the Strait of Hormuz. Iran does not play games for fun. And this time, as always, the Iranians are playing by their own rules and they are playing **to win**.

**Goes nuclear**

Kaveh L. **Afrasiabi &** Nader **Entessar 19,** Kaveh L. Afrasiabi is an Iranian-American political scientist, Nader Entessar is a professor and chair of the department of political science and criminal justice at the University of South Alabama, 2 July 2019, “A nuclear war in the Persian Gulf?” https://thebulletin.org/2019/07/a-nuclear-war-in-the-persian-gulf/

Tensions between the **U**nited **S**tates and Iran are **spiraling toward a military confrontation** that carries a **real possibility** that the **U**nited **S**tates will use **nuclear weapons**. Iran’s assortment of asymmetrical capabilities—all constructed to be effective against the **U**nited **S**tates—nearly assures such a confrontation. The current US nuclear posture leaves the Trump administration at least open to the use of **tactical nuclear weapons** in **conventional theaters**. Some in the current administration may well think it to be in the best interest of the United States to seek a quick and decisive victory in the oil hub of the Persian Gulf—and to do so by **using its nuclear arsenal**.

We believe there is a heightened possibility of a US-Iran war triggering a US nuclear strike for the following reasons:

The sanction regime set against the Iranian economy is so brutal that it is likely to force Iran to take an action that will require a US military response. Unless the United States backs down from its present self-declared “economic warfare” against Iran, this will likely escalate to an open warfare between the two countries.

In response to a White House request to draw up an Iran war plan, the Pentagon proposed sending 120,000 soldiers to the Persian Gulf. This force would augment the several thousands of troops already stationed in Iran’s vicinity. President Trump has also hinted that if need be, he will be sending “a lot more” troops. Defeating Iran through conventional military means would likely require a half million US forces and US preparedness for many casualties. The US nuclear posture review is worded in such a way that the use of tactical nuclear weapons in conventional theaters is envisaged, foreshadowing the concern that in a showdown with a menacing foe like Iran, the nuclear option is on the table. The United States could once again justify using nuclear force for the sake of a decisive victory and casualty-prevention, the logic used in Hiroshima and Nagasaki.

Trump’s **cavalier attitude toward nuclear weapons**, **trigger-happy penchant**, and **utter disdain for Iran**, show that he would likely have no moral qualm about issuing an order to **launch a limited nuclear strike**, **especially in a US-Iran showdown**, one in which the oil transit from the Gulf would be imperiled, impacting the global economy and necessitating a speedy end to such a war.

### 2AC --- UQ --- Russian Attacks

**Russian cyberattacks are increasing now because of an uncoordinated US response strategy and perceived lack of consequences for cyber-aggression---that ensures catastrophic Russian cyberattacks on critical infrastructure and kinetic retaliation.**

**Rondeaux 20** – Senior fellow and professor of practice at the Center on the Future of War, a joint initiative of New America and Arizona State University

Candace Rondeaux, “Why Is the U.S. Still So Vulnerable to Russian Cyberattacks?,” World Politics Review, December 2020, https://www.worldpoliticsreview.com/articles/29298/why-is-the-u-s-still-so-vulnerable-to-a-russian-cyber-attack

To call the revelations about Russia’s devastating cyberattack on U.S. government agencies and thousands of American businesses chilling would be a gross understatement. What is even scarier, though, is that despite **wave after wave** of **Russian-sponsored cyberattacks** on the United States and its allies for more than a decade now, Washington still apparently **lacks** the **political will** to **defend against** this **Russian aggression**.

It is possible and even probable that this latest attack will provoke a strong response from the U.S. and its allies, as some have suggested. As well it should. After all, the breach of the network monitoring software made by Texas-based SolarWinds, which has been widely attributed to Russia’s SVR intelligence agency, targeted the digital information architecture of several federal agencies, including the National Security Agency and the departments of Homeland Security, Treasury, Commerce and State. It also affected an estimated 18,000 companies with SolarWinds accounts, including several on the Fortune 500 list.

Over the coming weeks and months, the scope and scale of the cyberattack will become clear. It has already produced fallout for SolarWinds longtime CEO Kevin Thompson, who announced his resignation last week. And if news reports are any guide, the Russian hack could trigger a federal investigation into suspected insider trading, since some SolarWinds shareholders apparently cashed in right before news of the breach became public. But it is easy to imagine much worse scenarios. Second- and third-order effects of the cyberattack might include, for instance, leaks of sensitive information—or worse, sabotage of America’s critical infrastructure, such as electrical grids or banking systems.

Yet given the U.S. government’s **poor** and **well-documented track record** to date on **developing** and **implementing** a **comprehensive strategy** for **cyberspace**, it is also equally possible and far more **likely** that whatever immediate response the outgoing Trump administration and the incoming Biden administration come up with, it will **fall well short** of what is required to **mitigate** the **risks** of **more attacks**. That is because what is really needed is not just a response from the White House, but legislative action from Congress, an institution that has failed time and again to develop a sound cyber strategy or build proper cyber defenses. Instead Congress has allowed the politics of the petty, personal and partisan to paralyze this country in its time of greatest crisis.

While the latest move in Russia’s global cyber offensive exposed a fatal flaw in the way Washington formulates its national security priorities, it also reflects a major Kremlin miscalculation. There is a lot of noise around the signal Moscow keeps trying to send with these attacks. But what still **comes through clearly** is a **misplaced belief** among **Russian leadership** that there will be **no more costs** or **consequences** for its **continued provocations**. What President Vladimir Putin apparently **fails to see** is that the **further up the escalation ladder** Russia’s security agencies climb with their cyberattacks, the **more likely** it is that Russia’s sovereign wealth will **wind up in America’s crosshairs**, through retaliatory sanctions and other financial restrictions.

More ominously, the options in terms of non-military responses narrow considerably after that. No one on either side wants to go there, and everyone in the middle—the European Union especially—is rightfully afraid of such an outcome. But it is not hard to imagine that the **release of sensitive data** acquired from the SolarWinds breaches, or a **second wave attack**, could trigger such a scenario. Even if the outcomes were more subtle—say, a **series** of **slow-burning** and **targeted attacks** against American citizens and institutions, or against allied states that Moscow deems particularly troublesome, or, perhaps, leveraging stolen data to foment discord among NATO members—**more cyberattacks** attributed to Russia will only **harden the position** of **hawks** who might **advocate for military escalation**.

Putin is correct to surmise that any U.S. calculations about retaliating against these cyberattacks will always factor in other challenges, like the multitrack diplomacy required on everything from nuclear weapons to space to climate change, for which the U.S. still needs Russian cooperation. It is **folly**, however, to assume that the divide and conquer tactics Russia has fomented through its global disinformation campaign will lead to **permanent American paralysis**. With **systemic attacks** on **supply chains** or **critical infrastructure**, it only **takes one misstep** to **produce catastrophic collateral damage** or real human casualties. In fact, the hollowed-out state of American diplomacy after four years of Donald Trump should scare Putin more than it does, because ever since 9/11, the Pentagon hammer has rarely seen a nail it doesn’t want to pound.

Americans should be even more scared, especially Wall Street. In fact, a brief review of how we got here might be useful. The internet has been up and running since 1969, when it was first developed by the Pentagon’s Defense Advanced Research Projects Agency, or DARPA. When Tim Berners-Lee invented the World Wide Web in 1989, he transformed what was a rather clunky, albeit advanced, telecommunications system into a world-shattering, paradigm-shifting technological juggernaut. Since then, there have been hundreds, if not thousands of state-sponsored cyberattacks, according to the Council on Foreign Relations’ handy cyber operations tracker. At the same time, the digital revolution and birth of the online marketplace have generated billions for Wall Street, and trillions for the American economy. That doesn’t mean it will remain that way forever.

The data would seem to indicate that China, Russia, the U.S. and Iran stand out as the biggest players on the pitch when it comes to cyber operations. Yet to date, not one of these countries has stepped forward to say that it’s time to hold a global summit on the future of cyberspace. All that has been done is a lot of tinkering and dickering with policy nonstarters at the United Nations. There has been zero bold thinking—just a lot of authoritarians genuflecting in front of the false god of “cyber sovereignty” and chaotic clutch plays from more democratically inclined states. This state of affairs is likely to continue for the foreseeable future, despite all its risks

Only time will tell whether the **perilous state** of **America’s cyber defenses** and the pitiable lack of a national strategy to safeguard its supply chains from asymmetric attacks **further accelerates** America’s **decline** as a **major world power**. At least some part of the problem can be **attributed** to the **appalling ignorance** at the **federal**, state and local level of the technological innovations that drive the American economy and what it takes to protect them. No doubt, the power-hungry habits of a tech industry that has repeatedly resisted calls to work in earnest with government to build comprehensive solutions to managing cyber risks are also partly to blame. At bottom, however, the torpid U.S. government response to state-sponsored cyberattacks **screams out** for a **wholesale rethink** of what constitutes American vital interests.

There are plenty of good ideas out there for shoring up America’s cyber defenses. This latest attack will surely only serve as a **rallying cry** in support of the **consensus view** that the **most urgent work** is needed at the **federal level**. One of the best ideas to surface in the last couple days comes from the head of the Stanford Internet Observatory, Alex Stamos. He has urged the U.S. government to form “the cyberspace equivalent of the National Transportation Safety Board” that, instead of looking into the causes of plane crashes and train wrecks, “would track attacks, conduct investigations into the root causes of vulnerabilities and issue recommendations on how to prevent them in the future.”

**The invasion of Ukraine proves uniqueness---NATO must increase trans-Atlantic cooperation to ensure cyber-threats don’t escalate**

**Maigre 22** – senior cybersecurity expert at e-Governance Academy in Estonia

Merle Maigre, "NATO’s Role in Global Cyber Security," German Marshall Fund of the United States, 4-6-2022, https://www.gmfus.org/news/natos-role-global-cyber-security

Malicious cyber activity has increased substantially over the past years, ranging from ransomware and espionage to politically motivated cyberattacks and sophisticated malware used in the war in Ukraine. NATO allies must remain on high alert.

The changed nature of military conflict changes the defensive mission of NATO, which faces capable opponents in cyberspace and raises the question of how to create accountability when a hostile state fails to observe globally agreed norms.

The set of action for NATO for the next five years evolves around how to impose costs and how to deny benefits against malicious actors in cyberspace.

Introduction

What the war in Ukraine says about cyber power is yet not entirely cleared from the fog of war. Many aspects remain uncertain, but given the unpredictability of the Putin regime, the risk of an escalation in hostile cyber exchanges between Russia and NATO states remains high. What is clear is that, as of February 24, 2022, we live in a different world in which the European and global security orders have been shattered.

This brief first explores the challenge that cyber threats pose to NATO allies and how the rapidly evolving cyber-threat landscape can alter the international security environment. Secondly, it looks at developments in cyber defense policy within NATO. Finally, the brief analyzes how NATO needs to adapt to address cyber challenges, studying how allies align their sovereign interests, capabilities, and cyber doctrines with NATO operational requirements and strategic ambitions. NATO is set to issue strategic documents in 2022 that will guide the next decade of its military planning. This will certainly require more transatlantic consultation on political-military matters with an emphasis on cyber security and cyber defense.

Cyber Challenge to World and NATO Allies

Malicious cyber activity has increased substantially over the past years while the world has kept turning amid the omnipresent pandemic and now war in Ukraine. States, non-state actors, and criminal groups compete and are increasingly weaponizing sensitive information and infiltrating other countries’ networks to steal data, seed misinformation, or disrupt critical infrastructure.

The coronavirus pandemic further complicated the cyber-threat landscape. In March 2020, attempts to mitigate the spread of the coronavirus led to social distancing measures, travel restrictions, and remote work. In a short span of time, IT security professionals had to respond to the challenges of working from home, such as enterprise data movements when employees accessed cloud-based apps via their home internet, corporate software, videoconferencing, and file sharing.1 Even if hardware and software solutions were in place to secure the organization’s data, there were often no established policies to help employees wade through the jungle of threats and vulnerabilities they faced when moving their workplace out of the traditional office environment.2

According to the FireEye Mandiant Special Report: M-Trends 2021, the top five most targeted industries in 2020 were business and professional services, retail and hospitality, finance, healthcare, and high technology. The main methods used were extortion, ransom demands, payment card theft, and illicit transfers. Direct financial gain was the likely motive for 36% of intrusions, and an additional 2% of intrusions were likely perpetrated to resell access. In 2021, data theft remained an important mission objective for threat actors; in 32% of intrusions, adversaries stole data.3

Currently, highly organized, technically proficient criminal syndicates comprise the most significant cyber threat to allies. These groups try to steal data or extort money through ransomware. In 2021, prominent ransomware attacks struck Colonial Pipeline, the operator of the largest fuel pipeline on the East Coast of the United States; JBS, the largest meat processing company in North America; and Coop, a major supermarket chain in Sweden. Healthcare was also targeted—in May of the same year, the entire health service system of Ireland was disrupted for weeks, and over the spring and summer, dozens of hospitals in Europe and the United States were locked out of life-critical systems by ransomware attacks.4

Another set of threats comes in the form of belligerent state actors that seek to steal sensitive data for espionage. In December 2020, Russian intelligence services infiltrated the digital systems run by US tech firm SolarWinds and inserted malware into its code. During the company’s next software update, the virus was inadvertently spread to about 18,000 clients, including large corporations, the Pentagon, the State Department, Homeland Security, the Treasury, and other US government agencies. The hack went undetected for months before the victims discovered vast amounts of their data had been stolen.5

There are also politically motivated cyberattacks mandated by states that interfere in democratic processes and political discourse. In September 2020, the internal email system of Norway’s parliament was hacked.6 Ine Eriksen Søreide, the Minister of Foreign Affairs of Norway, underlined the significance of the attack by calling it an important cyber incident that affected the “most important democratic institution” of the country.7 Norwegian authorities later identified Russia as the actor responsible for the attack, marking the first time that Norwegian authorities had made a political attribution to such an attack.

Since the beginning of this year, Ukraine’s government has been hit by a series of cyberattacks that defaced government websites and wiped out the data on some government computers. In mid-January, hackers defaced about 70 Ukrainian websites, including the Ministries of Foreign Affairs, Defense, Energy, Education, and Science, as well as the State Emergency Service and the Ministry of Digital Transformation, whose e-governance portal gives the Ukrainian public digital access to dozens of government services. The hackers replaced the home pages of about a dozen sites with a threatening message: “be afraid and expect worse.” After a couple of days, however, most of the sites were restored.8 The international hacktivist collective Anonymous has declared “cyberwar” against Russia’s government, claiming credit for several cyber incidents including distributed denial of service attacks that took down Russian government websites and Russia Today, the state-backed news service.9

The most worrying type of cyberattack is sophisticated malware designed by states or state-backed actors that act as “time bombs” in the critical cyber networks of target countries, such as the energy, telecom, and transportation sectors. Around the globe, aging critical infrastructure has long been vulnerable to attack. In 2020, the UK’s National Cyber Security Centre issued a warning of Russian attacks on millions of routers, firewalls, and devices used by infrastructure operators and government agencies.10

On the day of the Russian invasion, ViaSat, a provider of high-speed satellite broadband services, was hacked along with one of its satellites Ka-Sat, whose users included Ukraine’s armed forces, police, and intelligence service. Destructive wiper malware attacks by Russia against Ukraine included WhisperGate, discovered in January by Microsoft, in Ukraine’s networks that “provide critical executive branch or emergency response functions”;11 HermeticWizard and IsaacWiper,12 targeting multiple Ukrainian organizations just hours before the Russian invasion began; and CaddyWiper, spotted by researchers at the Slovak internet security company ESET in mid-March.13 All of them were designed to wipe or overwrite critical files on infected systems and leave computer hard drives corrupted and unrecoverable. These incidents demonstrate that, in the words of cyber expert and Silverado Policy Accelerator think tank chairman Dmitri Alperovich, “Cyberattacks have become a theater for great-power conflict in which governments and militaries fight in the hybrid ‘gray zone,’ where the boundaries between peace and war are blurred.”14 The actors navigate a complex web of ambiguous and deeply interconnected challenges, where cyberattacks are not a separate front, but rather an extension of the conflict.

### 2AC --- S --- NATO Key

#### NATO OCOs are key to deter Russian gray-zone aggression, but coordination is key.

Alexander Vershbow, 1-25-2021, [Alexander Vershbow is the Wolk Distinguished Visiting Fellow at the University of Pennsylvania’s Perry World House and a distinguished fellow at the Atlantic Council’s Scowcroft Center for Strategy and Security. During his diplomatic career, he served as NATO deputy secretary general, assistant secretary of defense for International Security Affairs, ambassador to NATO, Russia, and the Republic of Korea, special assistant to the president for European Affairs at the National Security Council, and State Department director of Soviet Union Affairs., "REFLECTIONS ON NATO DETERRENCE IN THE 21ST CENTURY," Texas National Security Review, https://repositories.lib.utexas.edu/bitstream/handle/2152/90610/TNSRVol4Issue4Vershbow.pdf?sequence=2]

NATO thinking on deterrence today, even more than in the Cold War, should go beyond conventional and nuclear weapons to encompass cyber and other gray-zone threats. Offensive cyber capabilities offer the means to inflict strategic effects without the direct use of military force — such as by disabling nuclear missiles in their launchers or by destroying or disrupting reconnaissance and command-and-control systems. Cyber capabilities complement the more traditional basket of tools used by Russia to destabilize its adversaries below the level of armed conflict (such as political subversion, economic sabotage, disinformation, and fomenting separatism). Russia uses these so-called hybrid means to undermine states and alliances, damage infrastructure, and erode social cohesion, all while concealing the identity of the attacker.26 NATO has sought to deter cyber aggression, first of all, by declaring that even though the Washington Treaty refers to “armed attack” as the basis for

NATO action under Article 5, a cyber attack could inflict sufficient damage to be considered the functional equivalent of an armed attack, triggering Article 5.27 Beyond this, deterrence in the gray zone may depend on developing the capability to inflict equal or greater damage in response to large-scale cyber aggression and to make clear that NATO reserves the right to react symmetrically (i.e., cyber versus cyber) or asymmetrically, to include kinetic and non-kinetic options such as sanctions. In this regard, the adapted NATO Command Structure includes a new 24/7 cyber operations center at its main headquarters and allies have agreed that NATO’s Supreme Allied Commander for Europe can turn to nations with offensive cyber capabilities if needed in a conflict.28

Deterring gray-zone threats poses a more difficult challenge. Efforts to define a “red line” of conflict that must not be passed by nature encourage adversaries to take action perceived as below the red line. On the deterrence side, ambiguity and flexibility can help, but more important will be to strengthen allied nations’ own resilience — to harden critical infrastructure, reduce societies’ vulnerability to subversion and disinformation, expose and shut down the movement of dark money and other sources of corruption, and improve internal security and intelligence sharing within governments and across the NATO alliance. Allies also need to be more effective in pushing back against Russian disinformation and propaganda.29 NATO-E.U. cooperation on combating disinformation and establishing centers of excellence, such as the European Center of Excellence for Countering Hybrid Threats (Finland), the NATO Strategic Communications center of excellence (Latvia), and the NATO Energy Security center of excellence (Lithuania) are all important steps in this regard.

#### Alliance wide cyber information sharing is critical for operational strength

Canbolat and Sezgin, 16 (Mustafa Canbolat and Emrah Sezgin, 1st Lieutenant, Turkish ArmyB.S., Turkish Military Academy, 2008 , 1st Lieutenant, Turkish Air ForceB.S., Turkish Air Force Academy, 2009, December 2016, accessed on 6-16-2022, DTIC, "Is NATO Ready for a Cyberwar", <https://apps.dtic.mil/sti/citations/AD1030734>)//Babcii

b. Recommendations As Matthijs Veenendaal, Kadri Kaska, and Pascal Brangetto (2016) note, cyber capabilities are still regarded as **strategic assets by most states**. Because of the secrecy of these capabilities, states are reluctant to delegate the authority to use them, particularly in offensive operations. For instance, **in the United States**, “only the President can approve a cyber-attack likely to result in ‘significant consequences.’ However, this does not mean that these capabilities are irrelevant to **NATO** and NATO-led **operations**” (Veenendaal et al., 2016). NATO must plan for the “contingency of nations wanting to deploy them during a NATO-led military operation” (Veenendaal et al., 2016). However, without information sharing and knowing the level of possible contribution of an allied member, it will be **very difficult** to **plan** for possible **cyber scenarios** and **react swiftly** to cyber-attacks against NATO and its members. Handling “the need for secrecy or political sensitivity concerning specific military operations is not new for the Alliance” (Veenendaal et al., 2016). To enhance a full-fledged cyber doctrine, it would be beneficial to check the NATO Allied Joint Doctrine for Special Operations. It states in its introduction that special operations may be described as military activities conducted by specially designated, organized, trained, and equipped forces using operational tactics, techniques, and modes of employment not standard to conventional forces. Politico-military considerations may require low prominence, covert or discreet techniques, and the acceptance of a degree of physical and political risk not associated with conventional operations. (Veenendaal et al., 2016) The approach for s**pecial operations** is applicable for NATO to develop **information sharing** among members for cyber operations. NATO has the **capacity** to develop a **sound doctrine**, which deals with unconventional small sized units depending on secret information and conducting clandestine operations. Countries hesitate to **share information** because of their **vulnerabilities** in the cyber domain; however, if NATO becomes a more powerful cyber actor, **willingness to share information among members will increase**, and the **bonds of NATO members** will strengthen.

### 2AC --- S --- US Key

#### NATO has cyber capabilities, but coordinating with the US is key to a credible deterrent

Laura Oolup, 2019, [MA candidate at the University of Tartu in the Johan Skytte Institute of Political Studies, "CYBER AS A DETERRENT: UTILIZING OFFENSIVE CYBER CAPABILITIES IN NATO’S DETERRENCE POSTURE," University of Tartu, https://core.ac.uk/download/pdf/223009731.pdf]

The US has been widely acknowledged as the global cyber power which is at the forefront with the offensive cyber capabilities. Therefore, the US is extremely important asset for NATO to have credibility and capability imposing retaliatory threat in cyberspace. The US has not been clear in words either which capabilities exactly it possesses, but the actions give a taste of it. The SCADA-attack against the Iranian nuclear facility in Natanz that caused kinetic effects is a significant reflection of it (Zetter 2014). What can be noted here is that the offensive cyber capabilities have been presented through their deployment.

Additionally, the existence of and participation in exercises like the Crossed Swords organized primarily by the Cooperative Cyber Defence Centre of Excellence accredited by NATO, enables Allies to improve their offensive cyber capabilities and mirrors to the enemy which capabilities are being obtained. During this year’s exercise, the participants from cyber commands and special operation forces tested their offensive skills on attacking industrial control systems and also unmanned ground vehicles (CCDCOE 2019).

So far, we can see that in general NATO should have the potential for utilizing offensive cyber capabilities as a deterrent, because the necessary capability seems to exist. This is driven from Allies acquiring offensive cyber capabilities which have been also presented through previously conducted cyber campaigns, certain Allies have offered their sovereign cyber capabilities for the use of NATO, the skills for creating offensive cyber capabilities are being developed, NATO is working towards incorporating cyber component into force structures. However, when it comes to the credibility of the cyber threat from the viewpoint of the enemy, there are some problems.

First two issues have already been touched upon above as well which entail lack of knowledge regarding which kind of offensive cyber capabilities are exactly possessed or being developed by the Allies and secondly, ambiguous message by NATO’s Secretary General about in which cases and to what extent NATO would use the offered offensive cyber capabilities. Considering the conceptualized classical deterrence theory, the deterrer needs to be clear on its means, how they will be used and which effects they could cause (see i.e. Knopf 2009:41). Certain ambiguity could be acceptable in regards of the red lines, as otherwise, the enemy can play too easily around the boundaries. But the deterrent message should have more substance than just saying one is acquiring capabilities to carry out counterattacks in case of a necessity and that there have been few instances where those capabilities have been utilized. This does not seem enough to influence the decision-making equation of the enemy because it does not mirror what could be the costs in case of the aggression. It may especially turn out to be so if the adversary should happen to be risk-acceptant.

Third issue shadowing credibility of the potential cyber threat is stemmed from the previous two and this is that different ‘languages’ in the broader sense are being used by the member states offering their capabilities for NATO’s use. This does undermine the credibility of the deterrent threat, because in case of an Alliance, common language must be used by the members of it to ensure that there is no room for uncertainty and misperceptions. Talking about offensive cyber capabilities as a retaliatory measure, unified message by all the member states reflects the willingness to retaliate and gives the enemy the impression that the Alliance together stands by its words.

#### US coop is key – it has the most advanced cyber capabilities within NATO – examples prove.

Laura Oolup, 2019, [MA candidate at the University of Tartu in the Johan Skytte Institute of Political Studies, "CYBER AS A DETERRENT: UTILIZING OFFENSIVE CYBER CAPABILITIES IN NATO’S DETERRENCE POSTURE," University of Tartu, https://core.ac.uk/download/pdf/223009731.pdf]

The US has been considered the cyber power who “has the most advanced cyber capabilities within NATO” (Arts 2018:2). Therefore, it is not surprising that when the Defence Secretary Mattis at the time pointed out during the announcement of the US offering its cyber capabilities for the use of NATO is already willing to do so today (Mattis 2018). The US new cyber strategy allows military to carry out cyber operations to protect its systems, networks and national critical networks in general (Nakashima 2018). Furthermore, it seems that the utilization of the offensive cyber capabilities is not considered limited to deterring only cyberattacks as it is said, the intention is also to “ensure the US military’s ability to fight and win wars in any domain, including cyberspace” (Department of Defense 2018:1-2).

The offensive cyber capabilities the US is developing, have the purpose to counter cyberattacks, but at the same time be considered as any other means during war time. The offensive cyber capabilities should be flexible. This means, the US should have in its use various offensive cyber capabilities that can cause different types of effects depending on the situation and necessity (Department of Defense 2018:3). They are aimed to use as retaliatory measures in kind to cyberattacks but also as means to enhance the US military advantage in any way. Therefore, in the strategy it is mentioned that “during wartime, US cyber forces will be prepared to operate alongside our air, land, sea, and space forces to target adversary weaknesses, offset adversary strengths, and amplify the effectiveness of other elements of the Joint Force” (Department of Defence 2018:1).

However, there is not that much information out there what exactly are the capabilities the US obtains. Although, certain public announcements give some ideas in this regard. For instance, it has been announced that the US is procuring a Unified Platform that should support as a mission capability the US cyber command in its defensive and offensive cyber operations (Pomerlau 2019; Northrop Grumman 2018). Moreover, to develop the offensive cyber capabilities and to in general improve the work and operability of the US Cyber Command, it has allocated $75 million – which is 70% more compared to previous year - in the fiscal year of 2019 to do that (Pomerlau 2019).

The US has examples of conducting offensive cyber operations that reflect both the capabilities and willingness to create logical and kinetic effect. The most recent example concerning logical effect is related to the US cybercommand’s actions in regards of the Russian Internet Research Agency. The US assault on Russian Internet Research Agency (IRA) located in St. Petersburg was a pre-emptive approach to prevent Russia’s troll factory to conduct information operations and thereby meddle with the US midterm elections in 2018. The strike entailed cutting the IRA out of internet. This was a notable operation, because it was the first kind of the US to launch that kind of offense against Russia (Nakashima 2019).

The Stuxnet case that has been brought up in this paper for several times now is the example of the US being able to conduct an offense that relays kinetic effects. This was the US-Israel operation against Iran by using the worm called Stuxnet that was configured to target only certain computers targeting Iranian uranium enrichment centrifuges to halt the Iranian nuclear bomb development program. It was successful in the sense it caused physical destruction, was first of its kind, and set the Iranian nuclear program behind by two years (Zetter 2014).

### 2AC --- S --- Coop Key

#### Only the Alliance provides a forum for collaboration

Vivo and Fertasi 16 – Diana De Vivo joined the IES in October 2017 as part-time Doctoral Researcher on counter-terrorism, radicalisation and gender. She holds a Master's Degree (cum laude) in International Relations and Politics and a Bacherlor's Degree (cum laude) in Political Sciences from the University of Naples "L'Orientale", Italy. She currently works full time at NATO and has worked previously at the European External Action Service (EEAS)and the Calabria Region Delegation to the EU, the Italian Delegation to NATO, the Joint Force Command NATO in Naples, in a Private International Law Firm and at "L'Orientale" University in Naples (Italy). Nadja El Fertasi was a Senior executive at the NATO Communications and Information Agency. She worked with NATO for 20 years. 8-1-2016, "Cyber resilience: protecting NATO’s nervous system," NATO Review, https://www.nato.int/docu/review/articles/2016/08/12/cyber-resilience-protecting-natos-nervous-system/index.html

D. NATO’S CYBER PARTNERSHIPS 46. A strong network of partners is essential in an increasinsgly interconnected world, and this applies in particular to cyber security and defence. NATO therefore engages with a wide range of partners, including industry, academia, partner nations, and other international organisations. 47. Industry plays a central role in providing technical solutions and innovations, but they also own or operate a substantial share of Allied information systems. In the NATO Industry Cyber Partnership (NICP), the Alliance therefore provides a forum for NATO entities and national experts to engage with industry representatives (and academia) from member states. The NICP aims at facilitating information sharing on cyber threats and at improving the ability of Allies to detect, prevent, and respond to cyber incidents. The Partnership covers 12 priority areas, notably supply-chain management; best practices; awareness raising; education, training, and exercises; and innovation. 48. Cyber security and defence cooperation is very often a key component of NATO collaboration with partner nations. NATO has particularly deep partnerships with Georgia and Ukraine, which includes extensive cyber cooperation initiatives. Through the Substantial NATO-Georgia Package, the Alliance supports Georgia’s cyber capabilities, interoperability, and cooperation with individual Allies. NATO also established a Trust Fund on Cyber Defence in conjunction with Ukraine in 2014. The Trust Fund aims at developing strictly defensive capabilities in the area of cyber security incident response, including through setting up two Incident Management Centres. Ukraine also receives NATO training in employing the Trust Fund’s related technologies and equipment. Other notable recent cyber cooperation initiatives with partner nations include agreements with Finland, the Republic of Moldova, Jordan, and Iraq.

### 2AC --- S --- Coop Key: Attribution

**Info sharing with NATO is critical to effectively attribute responsibility for cyberattacks**

**Maigre 22** – senior cybersecurity expert at e-Governance Academy in Estonia

Merle Maigre, "NATO’s Role in Global Cyber Security," German Marshall Fund of the United States, 4-6-2022, https://www.gmfus.org/news/natos-role-global-cyber-security

When should states publicly attribute cyberattacks? Effective public attribution requires a clear understanding of the attributed cyber operation and the cyber-threat actor, but also the broader geopolitical environment, allied positions and activities, and the legal context. The public attribution framework put forward by Max Smeets and Florian Egloff in March 202127 distinguishes four factors that act as enablers or constraints in public attribution. These factors are intelligence, incident severity, geopolitical context, and post-attribution actions. The combination of these four components enables consistent decision-making about whether to publicly disseminate information about an adversary’s actions, privately tell the adversary, or restrict knowledge of the intrusion to the government and potentially other partners.

Collecting and processing intelligence—information about foreign countries and their agents—provides a technical basis for attribution. How could allies improve intelligence sharing to conduct more rapid attribution and enable a response to adversary cyber activity? During the Nordic-Baltic foreign ministers meeting in Tallinn in September 2020, a 90-minute tabletop exercise was organized28 to test the ministers’ ability to respond to and attribute an escalating cyberattack. They answered multiple-choice questions on communication of and possible diplomatic countermeasures to the attack. The ministers learned through first-hand experience that a timely exchange of technical intelligence can be key in attributing any cyberattack. “The shared view [of the countries involved]—especially when it comes to complicated issues—is crucial,” said Urmas Reinsalu, Foreign Minister of Estonia.29

Attribution is only as good as the information that allies are willing to share. NATO’s value can be in becoming the preferred platform for sharing cyber information. General Paul Nakasone, who heads US Cyber Command, told the House Armed Services subcommittee on intelligence that “in 35 years” he has never seen a better sharing of accurate, timely, and actionable intelligence than what has transpired with Ukraine.30 Sharing information and intelligence with allies “builds coalitions” and can “shine a light on disinformation” campaigns, like the one Russia used to lay the groundwork for their invasion of Ukraine.

### 1AR --- S --- Coop Key: Attribution

#### Intelligence-sharing is key to proactive deterrence and attribution.

Dominick Namias and Jacob Chace, 3-24-2022, [Dominick Namias is a Legislative Fellow at the United States House of Representatives and has a BS in politics and government from Liberty University. Jacob Chace is a government and journalism student at Liberty University, "U.S. WARFARE WITHIN THE FIFTH DOMAIN: DETERRING RUSSIAN CYBER AGGRESSION," Liberty University, https://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=1267&context=hsgconference]

The 2021-2022 Russo-Ukrainian crisis is revealing of Russia’s ultimate strategy in two ways. Firstly, it is now clear that a cyberattack will more than likely precede a kinetic attack, especially when there is little resistance to that aggression. Secondly, there will be more aggressive action coming out of the Russian Federation and NATO and the U.S. are not properly prepared on the cyber-defense front. The evidence for the latter point has been addressed earlier with the examples of successful cyberattacks against the United States such as the Colonial Pipeline and JBS infrastructure attacks as well as the Notpetya attack.

NATO has been primarily concerned with building up cybersecurity in member states. The next step, led by the United States, is to go on the offensive and accurately identify the sources of these cyber aggressions. On several occasions, Russia has been able to hide behind the idea that the cyber-attackers are not state-affiliated and fiend responsibility of aggressions from within the Federation:

Three successive U.S. administrations have failed to develop any form of doctrine to adequately address increasingly problematic cyberattacks from unattributable sources that plague U.S. businesses and can even endanger lives. Instead, the private sector has been left to deal with ever more destructive and dangerous ransomware attacks unassisted, and Russia continues to do nothing about cyberattacks originating from Russian territory.29

This is an epidemic that can be cured by shifting from a conservative policy regarding the cyberworld and towards a more proactive position. If the United States were able to identify actors with precision, further measures could be taken to prevent attacks on the U.S. infrastructure and on the private sector. In addition, being able to identify these actors would allow the United States and its allies to expose the perpetrators worldwide through media with solid evidence, damaging the perpetrator state’s reputation with the international community. Once the United States can present solid evidence against cyber criminals, the United States and NATO allies can voluntarily take conjoint actions against the perpetrator state/entity. This can be done through intelligence sharing, public statements of support for actions taken following an attack, and participation in the charges taken against the perpetrator state/entity. This strategy is reliant upon the ability of the United States and its allies to accurately identify perpetrators with a proactive joint campaign.

**That’s key to draw redlines and preserve cyber-deterrence**

**Maigre 22** – senior cybersecurity expert at e-Governance Academy in Estonia

Merle Maigre, "NATO’s Role in Global Cyber Security," German Marshall Fund of the United States, 4-6-2022, https://www.gmfus.org/news/natos-role-global-cyber-security

Action Plan for the Next Five Years

To make NATO future-proof, it must be cyber-secure and operational. But is it doing enough to address the complex and evolving challenges of cyberspace? NATO’s strategic challenge is to blend its successful conventional deterrence functions with a new strategy for cyber action. NATO’s ability to send a collective message of resistance and to establish a credible threat response is its most valuable asset on the cyber-security front.

Four sets of actions for NATO are proposed. First, denying covertness by attribution: NATO should persuade opponents that they cannot be clandestine in their cyber actions. NATO and its members need to demonstrate that it is difficult or impossible to act covertly and be clear about attributing responsibility for cyberattacks.

Until recently, governments did not publicly release details on cyber incidents. But since 2018, public disclosures of cyberattacks by several Western powers indicate a new multinational policy of state transparency. The growing relevance of attribution is partially due to states becoming better at attributing cyber operations. Greater public knowledge of cyberattacks heightens awareness of cyber conflicts and leads to greater public acceptance of cyber countermeasures.

Ultimately, what matters is that states engaging in unlawful actions using cyber means will face consequences. With attribution, policymakers show that they know what is happening in these networks and can investigate incidents. It also clearly spells out unacceptable behavior and can help create state practice. The best way to implement the international norms is by calling out behavior and having consequences when these norms are breached. Attribution will make clear to the malicious actor that their actions will be seen and addressed. It is the basis, under international law, for countermeasures and self-defense.

### 2AC --- Cyber Impact

#### Cyber-attacks triggers state and economic collapse---defense doesn’t assume the evolving nature of cybernetic weapons

Ghavam 16 – Z’hra M. Ghavam, Master of Arts in Security Studies Europe and Eurasia. National Security Affairs at the Naval Postgraduate School, September 2016, “NATO’S PREPAREDNESS FOR CYBERWAR,” https://archive.org/details/natospreparednes1094550552

\*edited for ableist language, which we do not endorse

Cyberspace is a physical and virtual domain that is comprised of computer hardware, information infrastructure, and electronic systems, which make digital interactions and communications possible.2 The cyber dimension has emerged as one of the most indispensable and yet vulnerable domains. Cyber attackers have increased digital attacks against both private industry and state actors to fulfill various political, informational, military, and financial agendas.3 Cyber attacks against critical infrastructure—that is, systems, networks, organizational structures, and resources vital to a nation’s security and well-being—have the power to destabilize organizations, industries, and nations.4 For most NATO members, the vulnerability of critical infrastructure and information systems within the energy, financial, telecommunications, and health sectors represents the leading concern.5 An act of cyber aggression on a nation’s financial industry could trigger a regional economic crisis. A cyber attack that releases sensitive information on a presidential candidate could influence the results of a ballot decision, corrupt the institutional integrity of nationally held elections, and even prompt regime change. Moreover, a cyber attack that disabled a country’s power grid or contaminated its water supply could create social havoc and ~~paralyze~~ national activity. The Center for Strategic and International Studies has shown the ubiquity of cyber threats by publishing reports on major cyber incidents involving espionage and attacks committed by state and non-state agents. Some of the organizations and industries that have incurred significant cyber intrusions and attacks include the U.S. Democratic National Committee (2016), the U.S. Joint Chiefs of Staff (2015), the White House (2014, 2015), the U.S. State Department (2006, 2014), Sony Pictures Entertainment (2014), the U.S. Office of Personnel Management (2014), the U.S. Department of Energy (2014), the European Aeronautic Defense and Space Company (2013), 23 U.S. gas pipelines (2011-2012), Google (2010, 2011), NASA (2011), the International Monetary Fund (2011), the European Commission (2011), the European Union (2011), and NASDAQ (2010).6 While these examples provide a glimpse of the power of cybernetic weapons, they also show that cyberspace represents much more than just another military conduit of modern warfare.

### 1AR --- Cyber Impact

#### Even small attacks could cause an escalatory spiral---that’s uniquely likely under times of crisis

Davis 19 – Member of the NATO parliamentary assembly and also a repetatur for the science and technology committee.

Susan Davis, October 13 2019, “NATO in the Cyber Age: Strengthening Security and Defence, Stabilizing Deterrence,” NATO Parliamentary Assembly, Science and Technology Committee, 148 STC 19 E rev. 1 fin. fc

66. As argued, states most likely do not see a cyber attack as a viable option for a pre-emptive, disarming first strike. However, in a crisis or pre-war situation, states could perceive a significant “cost of going second” (Davis, 2014). In such situations, one side “may well be frightened of what would happen if the other side attacks and may be convinced that going first will be advantageous” (Davis, 2014). This could lead to high escalatory risks. 67. In short and intense conflicts, pressures to use cyber attacks on military targets are high, as they are just another tool in the box, and the probability of attacks on critical infrastructure is still low, since they would not degrade the defender’s capabilities quickly enough to make a crucial difference (Lewis, 2018). If the war is expected to last longer, the latter type of attacks could appear more tempting, however. 68. Another key problem is the difficulty of determining the intent of a cyber intrusion (Lindsay, 2015). When a defender detects a breach, he may not know whether the intruder wants to spy on him, pursue active defence measures, gain a foothold for future defensive measures, or prepare for an imminent or future cyber attack (Slayton, 2017). It is extremely difficult to gauge intent in cyber space, and, in such cases, states tend to assume the worst (Hennessey, 2017). As a result, this can lead to misperception and an escalatory spiral (Slayton, 2017).

**It will trigger NATO Article 5 commitments and risk kinetic warfare.**

**Imeson 19** – Writer for the Financial Times

Michael Imeson, “Russia cyber aggression fuels tensions with west,” Financial Times, October 2019, https://www.ft.com/content/0aa7a6e0-ca52-11e9-af46-b09e8bfe60c0

Russian government-backed **cyber aggression** is **heightening concerns** from the west following a **spate** of **high-profile incidents**, **prompting threats of countermeasures** from the likes of NATO, the EU and UK.

“**Cyber threats** to the security of our alliance are **becoming more frequent**, **more complex** and **more destructive**,” Jens Stoltenberg, NATO’s secretary-general, wrote this month, warning that such threats emanated “from state and non-state actors, from close to home and the other side of the world”. The sole “state actor” named by Mr Stoltenberg was Russia.

**Concerns** over **online aggression** were fuelled in July when investigative journalists and other experts probing Russian intelligence activities had their **email accounts attacked**. Although ultimately unsuccessful, the attempted hack of Swiss-based ProtonMail accounts — used to share sensitive information related to probes of Moscow’s GRU military intelligence directorate — **refocused global attention** on **Russian cyber aggression**.

“We face a **determined**, **aggressive Russia**, **seeking traditional political advantage** by new, high-tech means,” Ciaran Martin, chief executive of the UK’s National Cyber Security Centre (NCSC), said last month. Mr Martin added that cyber threats from China, Iran and North Korea “have been a constant over the past few years”.

UK authorities last year exposed “a campaign by the GRU . . . of indiscriminate and reckless cyber attacks targeting political institutions, businesses, media and sport”, affecting a large number of countries, including Russia, according to the Foreign Office and the NCSC.

Mike Beck, global head of threat analysis at cyber group Darktrace, says Russia’s cyber policy has **switched**, from information gathering to **offensives** and **disrupting important industries**.

“When the International Olympic Committee looked at evidence of Russian doping, the Russian state response was to hack the World Anti-Doping Agency and release information on other countries’ athletes,” says Mr Beck.

To counter the heightened cyber threats, the UK’s ministry of defence in August announced the creation of a new army unit to focus on “intelligence, counter-intelligence, information operations, electronic warfare, cyber and unconventional warfare”.

The EU said in June that it would conduct war-games to prepare for any cyber attacks, signalling the bloc’s determination to increase co-operation against Russian and Chinese meddling. This would involve finance and home affairs ministries simulating everything from fake news to data theft to hacking into the operational technology of critical national infrastructure.

NATO’s Mr Stoltenberg noted that a **serious cyber incident** from a **hostile state** could **prompt swift retaliatory action** under the alliance’s **Article 5 collective defence commitment**, where an attack against one ally is treated as an attack against all members. The article has been invoked only once, after the terrorist attacks on the US in 2001 which led to NATO supporting the invasion of Afghanistan.

Other moves to counter aggression include the EU’s cyber sanctions regime — signed off in May — which issues penalties including travel bans and asset freezes against individuals found to have been involved in cyber incidents.

Russia, however, seems unperturbed by such developments and possible penalties, denying involvement.

Russia’s ministry of foreign affairs dismissed the UK’s creation of a new army cyber unit, noting that the threats were “imaginary” and said the move demonstrated “the UK’s anti-Russian policy”.

Andrei Krutskikh, international cyber security adviser to Russian president Vladimir Putin, in June told the UN’s Open-ended Working Group on Cyber Security: “The greatest danger is that incidents online can lead to a full-scale war offline. The doctrine of so-called **preventive cyber strikes** promoted by a number of countries poses a **real threat** to **international peace** and **security**.”

### 2AC --- Russia Impact

#### Multiple pathways to escalation

Gady 15 – Research Fellow at the International Institute for Strategic Studies.

Franz-Stefan Gady, “Could Cyber Attacks Lead to Nuclear War,” *The Diplomat*, 4 May 2015, https://thediplomat.com/2015/05/could-cyber-attacks-lead-to-nuclear-war/

Short fuses on U.S. and Russian strategic forces have particularly increased the risk of accidental nuclear war, according to Cartwright, while “the sophistication of the cyberthreat [to nuclear weapons] has increased exponentially.”

“One-half of their [U.S. and Russian] strategic arsenals are continuously maintained on high alert. Hundreds of missiles carrying nearly 1,800 warheads are ready to fly at a moment’s notice,” a policy report compiled by a study group chaired by the retired U.S. general summarized.

“At the brink of conflict, nuclear command and warning networks around the world may be besieged by electronic intruders whose onslaught degrades the coherence and rationality of nuclear decision-making,” the report further points out.

The War Games-like scenario could unfold in one of the following three ways:

First, sophisticated attackers from cyberspace could spoof U.S. or Russian early warning networks into reporting that nuclear missiles have been launched, which would demand immediate retaliatory strikes according to both nations’ nuclear warfare doctrines. Second, online hackers could manipulate communication systems into issuing unauthorized launch orders to missile crews. Third and last, attackers could directly hack into missile command and control systems launching the weapon or dismantling it on site ( a highly unlikely scenario).

### 1AR --- Russia Impact

#### Russian hybrid war escalates and causes World War III.

Peter Apps, 3-2-2018, [Peter Apps is a Reuters global affairs columnist and formerly a Future of War fellow at New America, "Commentary: Putin’s nuclear-tipped hybrid war on the West", U.S., https://www.reuters.com/article/us-apps-russia-commentary/commentary-putins-nuclear-tipped-hybrid-war-on-the-west-idUKKCN1GD6H2 //Weese]

This month marks the fourth anniversary of Russia’s March 2014 annexation of Crimea, an event that shocked the world and shook European faith in the post-Cold War security order. In retrospect, it has become clear that, for Putin, annexing the peninsula was not so much an end goal as a declaration of future intent, an early escalation in a broader and more ambitious effort that Ukrainian President Petro Poroshenko recently termed, with little obvious exaggeration, Russia’s “World Hybrid War” on Western democracy itself. In an unusually bellicose speech on Thursday, Russian President Vladimir Putin put Moscow’s remilitarization and its confrontation with the West at the heart of his pitch for re-election. His approach to this confrontation, which many now term “hybrid warfare,” mixes nuclear posturing and cutting-edge technology with covert action, and was deliberately designed so as to make it very difficult for the West to respond. President Vladimir Putin’s Russia did not, it must be said, invent hybrid warfare. Combatants have always looked for innovative ways around the rules and conventions of conflict, and Israel, Iran and the Gulf states have employed common hybrid tactics – including cyber attacks, and the use of armed proxy groups – for years. China’s leaders, too, have found increasingly unorthodox ways to push back against the United States and its allies in their immediate neighborhood; it recently emerged that, while Western nations were distracted by North Korea’s nuclear program, China artificially expanded islands in the South China Sea in support of its territorial ambitions. What Moscow has successfully done, however, is to refine a variety of old and new techniques to a higher level, and to employ them in a wider range of ways. As with China and Iran, Russia’s aim in developing and perfecting its hybrid warfare capabilities is to weaken and undermine the United States and its allies without sparking all-out war. It’s a dynamic that brings with it some very real dangers, not least of accidental conflict. The American air strikes that killed dozens, if not hundreds, of Russian mercenaries in Syria last month marked the bloodiest confrontation between the two nations in decades. U.S. prosecutor Robert Mueller’s decision to charge 13 Russians and several Russian companies with interfering in the 2016 election also amounts to a significant escalation. Exactly what prompted Russia’s interest in reheating Cold War-era animosities remains a subject of much debate among Western security analysts. Many, however, see its roots in the anti-government protests that rocked Russia in 2011 and 2012, the most serious such unrest since the breakup of the Soviet Union. Putin was widely believed to be furious that American diplomats had wooed pro-democracy and anticorruption activists, and to have concluded that Washington hoped to subvert his power. When Russia invaded Crimea early in 2014, and when a wider conflict erupted in Russian-speaking Ukrainian regions later that year, it acted with ruthless efficiency. By using troops wearing uniforms without insignia or identification – who became known universally as “little green men” – Russia achieved surprise and dominance on the ground before authorities in Kiev, let alone Washington, really knew what was happening. It would be hard to overstate how much this took U.S. President Barack Obama’s administration by surprise. The Pentagon’s Quadrennial Defense Review, published only days before the Crimea annexation, barely mentioned Russia and prioritized the risk of war with China as well as ongoing action against Islamist militant groups in the Middle East and beyond. Russia’s seizure of the strategically important Crimean peninsula, and its apparent role in shooting down a Malaysian Airlines flight over eastern Ukraine in July 2014, forced the United States and its European allies to urgently reconsider their beliefs about Russia’s intentions. Since then, NATO has deployed battle groups to Eastern Europe and the Baltic States (in case Moscow is tempted to try out the techniques it used in Ukraine against NATO members). In some ways, this resembles the Cold War, but it is in many respects a much more dynamic confrontation. Russia is now far more closely intertwined with the West, through investments and business deals, and this gives it new vulnerabilities – to sanctions, for example. Mueller’s prosecution of former Trump campaign manager Paul Manafort – who has a long history of business interests to the former Soviet Union – has drawn attention to just how convoluted some of these dealings have become. Russian money has been essential to the success of many Western businesses, possibly including those of President Donald Trump. But many powerful Russians are similarly beholden to the West – which is one reason so many of them have been frantically lobbying Congress to ensure their names aren’t included on upcoming sanctions lists. NATO members concerned about Russian political interference have recruited armies of bloggers and social media activists to push back against Russian messaging, and established new monitoring bodies to track Russian disinformation efforts. But, in hindsight, they may have interpreted that threat too narrowly. Rather than simply concentrate its efforts on spreading subversion on Europe’s vulnerable periphery, Moscow appears to have concentrated on destabilizing the West’s most powerful countries. The most recent Mueller indictments allege that, by mid-2014, Russia’s preparations for its interference in the 2016 U.S. presidential elections were well underway, and that it had already made significant progress with plans to boost its political influence in Europe. (These plans, the indictment suggests, included paying off the so-called “Habsburg group” of well-connected former European politicians.) Meanwhile, the ongoing fighting in Ukraine – as well as Russia’s post-2015 military intervention in Syria – has prompted a major Western reappraisal of Russia’s military capabilities. In addition to its newer hybrid warfare tactics, Russia has proved increasingly adept at combining the use of drones, electronic warfare and more conventional heavy artillery to lethal effect against Ukrainian forces using more traditional Western equipment and tactics. The seizure of Crimea prompted NATO to deploy a significant, and permanent, ground force to the Baltic countries and Poland. New fronts continue to erupt, and Western analysts increasingly worry over Russian activity in the Western Balkans. Putin’s explicit nuclear threats this week will likely cause the United States and its European allies to reconsider their own nuclear postures. It seems far from impossible that the United States would decide to increase its nuclear footprint in Eastern Europe. Just over a century ago, a similar welter of international anxiety and confusion formed the base of dry tinder that World War One would set alight. Russia and its rivals must take great care not to allow history to repeat itself.

### 2AC --- Hybrid War Impact

#### Russian hybrid war escalates globally

Trenin, 18 (Dmitri Trenin, director of the Carnegie Moscow Center, chairs the research council and the Foreign and Security Policy Program, 1-25-2018, accessed on 8-11-2021, Carnegie Moscow Center, "Avoiding U.S.-Russia Military Escalation During the Hybrid War", http://carnegie.ru/2018/01/25/avoiding-u.s.-russia-military-escalation-during-hybrid-war-pub-75277)//Babcii

. The war is being fought simultaneously in a number of spheres, on different levels, and in the never-ending, twenty-four-hour news cycle. This aspect of warfare is particularly true of the field of information, which is of prime importance in the Information Age that emerged with the end of the Cold War. From cyber conflicts and the use of artificial intelligence to the predominance of propaganda and fake news, the main battles of the Hybrid War are taking place outside of the purely physical realm and in the domain of new information technologies. Just as important to the Hybrid War is economics, which has been the key driver of globalization that paralleled the rise of these innovative information technologies. The prominence of the U.S. media and the United States’ immense financial power give it a huge advantage in both fields. As a result, the weapons of choice in the Hybrid War are those that use information and economic power to discredit and sanction one’s adversaries.3 Politically, the Hybrid War includes the outside stimulation of political changes in other countries through street activism and the promotion of specific values, parties, or popular movements. It has been characterized by interference in elections, political transitions, and other political processes, including various efforts to hack sensitive information, spread compromising or damaging materials and fake news, encourage character assassinations, and impose personal and other noneconomic sanctions (for example, restrictions on travel, seizure of assets, imprisonment, or deportation) on opponents. The existence of a common information space makes waging political warfare on foreign territory much easier and more attractive than ever before. Cross-border promotion of democracy and support for the color revolutions that dominated the 2000s (for example, the 2003 Rose Revolution in Georgia and the 2004 Orange Revolution in Ukraine) have now found counterparts in emerging solidarity among those who espouse more conservative and traditionalist values, such as political systems based on authoritarian models and strict national sovereignty.4 Military power is not out of the picture—though its use is different than in the Cold War. The static standoff of million-strong armies in Europe and the long shadow of the nuclear arms race have drawn down or faded. Nuclear deterrence between Russia and the West remains in place but at lower and more stable levels than during the Cold War. Today’s risks of miscalculation derive from potential incidents involving conventional forces. A token military standoff has reemerged along Russia’s border with NATO countries, but, to date, this standoff bears no resemblance in either scale or scope to the forces that faced each other during the Cold War. The main focus is on developing new military technologies and novel means and ways of prosecuting warfare—from outer space to cyberspace—that blur or eliminate the distinction between wartime and peacetime. Like its predecessor, the Hybrid War is a war in the time of peace. Even more than in the past, however, the onus is on national leaderships to minimize the number of casualties, ideally to zero. Russian military strategists had developed the concept of hybrid warfare even before the actual conflict broke out in earnest between the United States and Russia in early 2014. Analyzing the experience of the post-Soviet color revolutions and the 2011 Arab Spring, Chief of the General Staff Valery Gerasimov wrote in February 2013 that the “consequences of new conflicts are comparable to those of a real war”; in many cases, nonmilitary methods “are substantially more effective than the power of arms,” and greater emphasis is placed on “political, economic, information, humanitarian, and other nonmilitary means” and “covert military measures,” including “information warfare and actions by special forces.” In this environment, “overt use of military force, often in the form of peacekeeping or crisis management, takes place only at a certain stage, mainly to achieve final success in a conflict.” With regard to the U.S.-Russia confrontation, another key feature has surfaced: asymmetry between the sides’ capabilities. POWER ASYMMETRIES AND ASYMMETRIC ACTIONS Although Gerasimov was referring to a hybrid war when discussing new means and methods of warfare, this analysis uses the newly fashionable term to describe the current U.S.-Russia confrontation. Unlike its Cold War predecessor, this conflict is asymmetrical. At least since the 1970s, the Soviet Union was the United States’ equal in terms of both nuclear and conventional military power. Even beyond its own vast land mass and immediate sphere of influence in Eastern Europe, it wielded considerable ideological power in many Western countries and in the Third World and presided over a system of alliances in Africa, Asia, Europe, Latin America, and the Middle East. The Russian Federation, by contrast, has few formal allies, no satellite states, and a handful of protectorates, if one includes the self-proclaimed states of Abkhazia, Donbass, South Ossetia, and Transnistria. It has no ideology to compare with the comprehensive dogma of Marxism-Leninism, and although it is still a nuclear superpower, it lags far behind the United States in non-nuclear military capabilities. Economically, Russia—with its estimated 1.5 percent of the global gross domestic product—is a dwarf. Neither the balance nor the correlation of forces, however, will determine the outcome of this confrontation. Despite the glaring asymmetries in the national power of the two sides of the conflict, the course of events is not predetermined. As a nonlinear, highly asymmetrical conflict, the outcome likely will result from domestic developments in Russia or the United States or both. Both countries are facing serious problems that could prove decisive in the final calculations of the Hybrid War. The United States is going through a triple crisis of its political system, exemplified but not caused by the arrival of President Donald Trump and the virulent domestic opposition to him and his policies. A crisis of social values lies beneath this political crisis and points to a widening gap between the more liberal and the largely conservative parts of the country. At the same time, the United States faces a crisis within its own foreign policy as it struggles to reconcile the conflict between the more inward-looking U.S. national interest and the international liberal order of the U.S.-led global system. Russia, though outwardly stable, is approaching its own major crisis as the political regime created by Putin faces an uncertain future after the eventual departure of its figurehead. Putin’s Kremlin is already working on a political transition that would rejuvenate the elite and improve its competence and performance, but, at the same time, Russian society is also changing and Putin’s heirs cannot take its support for granted. Gross inequality, sluggish economic growth, low vertical mobility, and high-level corruption will present a range of serious challenges to the future Russian leadership. The eventual outcome of the Hybrid War could be reminiscent of the downfall of the Soviet Union, which was far less the result of the U.S.-Soviet Cold War than of a misguided effort to reform the Soviet Union itself. Russia might break down and break up again, or it might decide on a foreign policy more geared toward its economic needs than to a certain concept of world order. As for the United States, it might decide to limit its global commitments and redesign its international role as the world’s preeminent but no longer dominant state. Yet, in doing so, it will need to accept that its change in status will come with a certain price and that it will not be able to take advantage of the benefits of the position it once enjoyed. Asymmetries in power lead to asymmetric actions, which as Gerasimov suggested are intended to “neutralize the enemy’s superiority in warfare” or “identify and exploit the enemy’s vulnerabilities.”5 By an order of magnitude—or more—Russia is outgunned, outmanned, and outspent by the combined forces of the United States and its allies. To stay in the fight, it must rely on its few comparative advantages and seek to use them to maximum effect. These advantages include the geographical proximity of some of the main theaters of operation, such as Crimea and eastern Ukraine, where Russia has escalation dominance; the Russian political system, which allows for secretive, swift, and decisive action; and Moscow’s willingness to take much higher risks in view of the disproportionally higher stakes involved for the Russian leadership and a national culture that historically has tolerated higher losses in defense or protection of the Motherland. Through swift decisions and actions, made without prior warning, Russia is capable of surprising its adversaries and keeping them off-balance. This situation promises an uncertain, hard-to-predict, and risky environment, where miscalculation can lead to incidents or collisions that, in turn, lead to escalation. Granted, these incidents would be of a different kind than the tank standoff at Berlin’s Checkpoint Charlie in late October 1961 or the Cuban Missile Crisis barely a year later. Escalation resulting from miscalculation would not be automatic, but the wider damage it could cause needs to be taken seriously. AVOIDING MISTAKES LEADING TO ESCALATION The Hybrid War is highly dynamic and, so far, has no agreed-upon rules. In this sense, it resembles the Cold War of the early 1950s rather than that of the 1970s. However, it is possible, up to a point, to avoid military escalation during the Hybrid War. U.S.-Russian antagonism does not mean that the two countries’ interests are in total opposition. Unlike in the second half of the twentieth century, neither party envisions a real shooting war against its adversary and neither wants to allow the situation to become uncontrollable. The most obvious ways to manage the confrontation are incident prevention, confidence building, and arms control. Incident prevention, on the face of it, should be easy. Since the early 1970s, Moscow and Washington have had agreements in place to avoid incidents, which in the Cold War days carried the risk of escalation to nuclear levels. Effective prevention requires a degree of professionalism, adequate safety measures, and reliable channels of communications. However, during a Hybrid War, these preconditions cannot be taken for granted. Acting from a position of relative weakness, Russia is likely to compensate for its inferior overall strength by raising the stakes of confrontation.

### 2AC --- Meltdowns Impact

#### Meltdowns make Earth unlivable.

Slocum 15 — Christopher Slocum, Researcher at Arizona Oil & Gas, J.D. from University of Missouri-Kansas City School of Law, 2015 (“A Theory for Human Extinction: Mass Coronal Ejection and Hemispherical Nuclear Meltdown,” *The Hidden Costs of Alternative Energy Series The Hidden Costs of Alternative Energy Series*, July 21st, Available Online at <http://azoilgas.com/wp-content/uploads/2018/03/Theory-for-Human-Extinction-Slocum-20151003.pdf>)

With our intelligence we have littered the planet with massive spent nuclear fuel pools, emitting lethal radiation in over-crowded conditions, with circulation requirements of electricity, water-supply, and neutron absorbent chemicals. The failure of any of these conditions for any calculable or incalculable reason, will release all of a pool’s cesium into the atmosphere, causing 188 square miles to be contaminated, 28,000 cancer deaths and $59 billion in damage. As of 2003, 49,000 tons of SNF was stored at 131 sites with an additional 2,000-2,400 metric tons produced annually. The NRC has issued permits, and the nuclear industry has amassed unfathomable waste on the premise that a deep geological storage facility would be available to remediate the waste. The current chances for a deep geological storage facility look grim. The NAS has required geologic stability for 1,000,000 years. It is impossible to calculate any certainty 1,000,000 years into the future. Humanity could not even predict the mechanical failures at Three Mile Island or Chernobyl, nor could it predict the size of the tsunami that triggered three criticality events at Fukushima Daiichi. These irremediable crises span just over 70 years of human history.

How can the continued production and maintenance of SNF in pools be anything but a precedent to an unprecedented human cataclysm? The Department of Energy’s outreach website explains nuclear fission for power production, providing a timeline of the industry. The timeline ends, as does most of the world’s reactor construction projects in the 1990s, with the removal of the FCMs from Three Mile Island. One would think the timeline would press into the current decade, however the timeline terminates with the question, “How can we minimize the risk? What do we do with the waste?” (The History of Nuclear Energy 12). Nearly fifteen years into the future, these questions are no closer to an answer. The reactors at Fukushima Daiichi are still emitting radioisotopes into the atmosphere, and their condition is unstable. TEPCO has estimated it could take forty years to recover all of the fuel material, and there are doubts as to whether the decontamination effort can withstand that much time (Schneider 72). A detailed analysis of Chernobyl has demonstrated that nuclear fall-out, whether from thermonuclear explosions, spent fuel pool fires, or reactor core criticality events are deleterious to the food-chain. Cesium and strontium are taken into the roots of plants and food crops, causing direct human and animal contamination from ingestion, causing cancer, teratogenicity, mutagenesis and death. Vegetation suffers mutagenesis, reproductive loss, and death. Radioactive fields and forest floors decimate invertebrate and rodent variability and number necessary to supply nature’s food-chain and life cycles. The flesh and bones of freshwater and oceanic biota contribute significantly to the total radiation dose in the food-chain. Fresh water lakes, rivers and streams become radioactive. Potable aquafers directly underlying SNFs and FCMs are penetrated by downward migration of radioisotopes. Humans must eat to live. Humans must have water. No human can survive 5 Sv of exposure to ionizing radiation, many cannot survive exposure to 1 Sv.

Realizing the irremediable devastation caused by one thermonuclear warhead, by one Chernobyl, by one Fukushima Daiichi, it remains to be said that the earth can handle as many simultaneous loss of coolant failures as nature can create. Humanity cannot. It is not good enough to lead by relegating probable human wide extinction phenomena to an appeal to lack of evidence. Policy cannot indefinitely ignore responsibility by requiring further study. Nor can leadership idle into cataclysm by relying on the largest known natural phenomena of the last 200 years. Permitting construction and continued operation of malefic machinery, based on 200 years of cataclysmic experience is a protocol for calamity. Of coronal mass ejections, Hapgood warns, that we need to prepare for a once-in-1000-year event, not just simulate infrastructure safeties by the measure of what we have seen in the past. The same is true for all natural phenomena. The future of humanity is too precious to operate with such insouciance. The engineering is not good enough. It never will be. Nature is too unpredictable, and nuclear power is too dangerous.

### 2AC --- AT --- OCO’s Bad

#### An offensive strategy solves---effectively deters adversaries by imposing credible costs.

Borghard 20 – Assistant professor at the Army Cyber Institute at the United States Military Academy at West Point and a Council on Foreign Relations International Affairs Fellow

Erica D. Borghard, “Operationalizing Defend Forward: How the Concept Works to Change Adversary Behavior,” Lawfare, March 2020, https://www.lawfareblog.com/operationalizing-defend-forward-how-concept-works-change-adversary-behavior

Here, I want to focus on the first end state: the theory of victory for how defend forward can change adversary behavior below the level of armed attack. Defend forward hypothesizes the U.S. can change adversary behavior through making attacks less effective and, cumulatively, by altering the adversary’s decision calculus regarding the perceived benefits, costs and risks of conducting malicious campaigns against the United States.

There are two specific pathways that link defend forward with the desired outcome. The first is driven by a logic of cost imposition. Specifically, adversary behavior will change when adversaries experience (or perceive) an increase in the direct and indirect costs of conducting malicious activities. This includes U.S. efforts to counter adversaries’ offensive cyber capabilities and infrastructure, the organizations that support their cyber operations and campaigns, and the locus of their decision-making. In addition to making it more difficult for adversaries to conduct malicious operations and campaigns, this will force them to divert resources from other lines of effort and shift to secondary and tertiary plans, and it will also increase their uncertainty about the likelihood of success. The second pathway stems from a bargaining logic—to reduce the information asymmetries between the U.S. and its adversaries. The idea is to improve intelligence about adversary capabilities, provide early warning of impending attacks, and enable rapid counter-cyber responses and information-sharing with targeted owners and operators, while simultaneously reducing their access to U.S. information.

Together, increasing costs to adversaries and improving U.S. situational awareness about adversary behavior and capabilities can reduce information asymmetries and help the U.S. get “left of boom,” with the potential to yield cascading positive effects. Additionally, disrupting adversary capabilities and infrastructure, in some instances, may have an aggregate effect of disrupting infrastructure, organization and capabilities that could have supported multiple operations by adversaries. Moreover, affecting the adversary’s decision-making cycle can increase the domestic costs for the adversary’s regime if defend forward creates costs for stakeholders that support the government.

Defend forward has a number of detractors, some with important concerns. The commission strove to address these, including by providing recommendations for how the U.S. can improve engagement with international allies and partners; detailing an enhanced signaling strategy to mitigate potential risks of inadvertent escalation; and proposing investments in resilience to shore up the private sector’s ability to withstand and rapidly recover from adverse events. However, if we agree that the current status quo in cyberspace is not acceptable, this raises the question: What is a viable alternative to defend forward to change adversary behavior? Defend forward seeks to create costs for adversary military organizations and capabilities and improve U.S. situational awareness—as well as the situational awareness of U.S. allies and partners—in support of defensive strategic objectives. Unlike in the realm of nuclear deterrence, in cyberspace we cannot expect a binary outcome—the use of a capability versus nonuse, for example—but the U.S. can and should take steps to reduce the frequency and magnitude of malicious adversary behavior.

#### Preempting and degrading adversarial capabilities is key to solve.

Sulmeyer 18 – Director of the Cyber Security Project at the Harvard Kennedy School's Belfer Center

Michael Sulmeyer, “How the U.S. Can Play Cyber-Offense: Deterrence Isn't Enough,” Foreign Affairs, March 2018, https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense

Today’s fight in cyberspace occurs in the gray zone between war and peace. If the United States hopes to win, it should spend less time trying to persuade its competitors that it is not worth hacking and more time preempting them and degrading their ability to do so. It is time to target capabilities, not calculations.

HACK THE HACKER

How could the United States begin degrading its opponents’ ability to hack? Washington’s actions need not always be aggressive or destructive. In countries where technology companies are willing to cooperate with the U.S. government (or with requests from their own government), a phone call to the right cloud provider or Internet service provider (ISP) could result in getting bad actors kicked off the Internet. This is not a permanent solution, but it will force adversaries to rebuild, which often prompts unforced errors, making them more vulnerable to U.S. surveillance and disruption.

If subtle measures prove insufficient, the United States should be ready to take more offensive action. In situations where the defense of the nation is on the line, U.S. hackers could pursue a campaign of erasing computers at scale, disabling accounts and credentials used by hackers to attack, and cutting off access to services so it is harder to compromise innocent systems to conduct their attacks. Such a campaign would aim to make every aspect of hacking much harder: because hackers often reuse computers, accounts, and infrastructure, targeting these would sabotage their capabilities or render them otherwise useless.

Such actions need not send a message that hacking the United States doesn’t pay. Instead, they should support a more limited but more achievable objective: stop adversaries from hacking the United States. Whether or not foreign leaders perceive that cyberattacks on the United States are worth conducting, Washington can prevent them from doing so in the first place.

Offensive cyber-operations should not be undertaken lightly—the United States must bear in mind its commitments under international law and its relationships with its allies. But excessive caution cannot prevent Washington from defending itself: with the United States’ enemies already attacking it online, the country will need to be more proactive than it has been thus far.

### 1AR --- AT --- OCO’s Bad

#### Credible offensive capabilities are key to deterrence.

Mazanec & Thayer 15 – Director in GAO’s Defense Capabilities and Management team; Professor, Faculty of Political Science, University of Iceland

Brian M. Mazanec, Bradley A. Thayer, “Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace,” Palgrave McMillan, 2015, <https://link.springer.com/book/10.1057/9781137476180>

Deterrence-in-kind: developing offensive cyber capabilities

In addition to a declaratory policy, developing credible options for deterrence-in-kind, for example, offensive cyber capabilities, will be key to bolstering credibility of such a policy as some actors will not believe the United States would respond to a cyber attack with anything but cyber weapons. Peter Singer and Allan Friedman identified this deterrence-in-kind as well as the prospect of mixed ‘cyber- and real-world retaliatory force’ as one avenue to pursue to bolster the deterrence of cyber attacks.13 US Cyber Command’s ambitious plan to field over 100 cyber teams by late 2015 is a positive step in this direction.14 Evidence leaked in August 2013 that the United States conducted 231 offensive cyber operations in 2011 also helps demonstrate advanced cyber capability.15 These developments could help ensure any clear US threat of retaliatory cyber attack in response to a major cyber attack was credible, in spite of the challenges of weapon and target unpredictability. Some analysts, such as Franz-Stefan Gady, have pointed out that a ‘systematic public display of nation states’ cyber-war capabilities ... . can have a greater deterrence effect’ on some actors because they will better understand adversary capabilities and signaling through behaviors and actions.16

#### Offensive capabilities are a key component of an effective deterrence strategy.

Limnéll 13 – Professor of Cybersecurity, Aalto University, Finland

Jarno Limnéll, “Offensive Cyber Capabilities are Needed Because of Deterrence,” The Fog of Cyber Defence, National Defence University, Department of Leadership and Military Pedagogy, Publication Series 2, Article Collection no. 10, 2013, https://cyberwar.nl/d/20130200\_Offensive-Cyber-Capabilities-are-Needed-Because-of-Deterrence\_Jarno-Limnell.pdf

Offensive Weaponry is Required for Credibility and Deterrence

First, if one wishes to be a credible actor both in the military battlefield and in world politics, one must have offensive capabilities – as one must have defensive capabilities and the ability to be resilient. One simply cannot have a credible cyber defence without offensive abilities.

Second, in order to achieve and raise her deterrence, one must possess offensive capabilities. The ability to act offensively includes a strong preventive message to the others – provided that they understand it and believe it. Offensive capabilities represent the key component of deterrence.

Third, offensive thinking and building offensive weaponry are vital in order to create a strong and credible defence. With just “defence thinking” one will not succeed. One has to have an understanding of how the attacker acts, and one should try to find all possible vulnerabilities in her own defence. It is also a matter of developing one’s defensive potentials, testing the current defence and training one’s forces. All this becomes much more efficient if one can test it with her own capabilities. Without the ability to act as an attacker, no country can build an effective and credible cyber defence.

Fourth, agility and the concept of operations for smart defence are reality in contemporary warfare for most countries. One will never achieve her objectives by just being defensive – regardless of how defensive her grand doctrine is. In some cases, as it has been in the past, attack is the best defence. One cannot stay in bunkers. Instead, one has to be an active defender and snatch the initiative when it is needed. Passive defence alone will not work. In short, when the lights go off how does one defend with kinetic weaponry against a nonkinetic adversary?

### 2AC --- AT --- A5 Thumps

#### A5 vagueness is intentional---leaves NATO flexibility room in deterring attacks

Ghavam 16 – Z’hra M. Ghavam, Master of Arts in Security Studies Europe and Eurasia. National Security Affairs at the Naval Postgraduate School.

September 2016, “NATO’S PREPAREDNESS FOR CYBERWAR,” https://archive.org/details/natospreparednes1094550552

3. Clarity NATO’s publicly declared policy on cyber threats is consciously and purposefully vague.207 Why? Strategic ambiguity has its benefits. According to the Atlantic Council panel, there is no “redline” or “determined threshold” that would automatically define a cyber act as an act of war.208 Leaving the rules undefined affords NATO ample room in which to operate. For a 28-member multinational organization that operates on the principle of consensus, time and latitude for solidifying strategic-level decisions are critical. If NATO publicized a cyber redline, it would box the Alliance into a corner. This kind of policy could embolden cyber offenders and provoke massive intrusions that target NATO’s networks at just below this threshold. Having a defined redline could also invite nefarious cyber actors to cross it to test NATO’s resolve, damage its reputation as a leader in Euro-Atlantic security, and undermine the credibility of its Article 5 commitments. Following the Wales Summit in 2014, NATO affirmed its stance on law and cyberspace while refusing to address cyber redlines: Our policy also recognizes that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm, therefore, that cyber defense is part of NATO’s core task of collective defense. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.209

## Adv --- Cohesion

### 2AC --- Democracy A/O

**NATO key to democracy---checks war**

**Menon and Ruger 5/20 –**Rajan Menon holds the Anne and Bernard Spitzer Chair in Political Science at the City College of New York/City University of New York and is a Senior Research Scholar at the Saltzman Institute of War and Peace Studies, Columbia University and a Global Ethics Fellow at the Carnegie Council on Ethics in International Affairs,Ph.D. University of Illinois at Urbana-Champaign, William Ruger is a research fellow in foreign policy studies at Cato Institute. He earned his Ph.D. in Politics from Brandeis University and an A.B. from the College of William and Mary. NATO enlargement and US grand strategy: a net assessment. Int Polit 57, 371–400 (2020). https://doi.org/10.1057/s41311-020-00235-7

Those who championed NATO expansion also believed that it was essential to the **promotion and consolidation of democracy** in post-Cold War Europe. US leaders in the executive branch, the legislature, and the foreign policy community more generally (i.e., specialists in universities, the media, and think tanks), general agree that **a NATO with strong US leadership was essential for democracy**’s success in the alliance’s newest states and that emergence of authoritarian regimes in the states east of NATO’s old perimeter would **lead to turmoil there or even war,** a denouement that would ill serve US interests. The proponents of NATO enlargement also considered it essential for promoting economic reform and bringing militaries under civilian control in countries that had been part of the Soviet bloc for decades (e.g., US Information Agency 1996; Holbrooke 1995, 41–42; Talbott 1997; Albright 1997a). They disagreed with critics who warned that NATO’s eastward expansion would eventually provoke resistance from a resurgent Russia and force the USA to bear the burden involved in protecting several militarily weak states near or adjacent to the Russian border. Beyond that, advocates of reconfguring NATO after 1991 insisted that it should move out of area to help control confict, consolidate stability, and advance human rights in countries outside Europe. Included in this new agenda were humanitarian interventions (to stop mass atrocities) and stability operations in countries emerging from civil war.

**NATO is key to curb pre-World War II authoritarianism**

**Marten 17 –** Kimberly Marten, International security expert and Russia watcher; Professor at Barnard College, Columbia University; Ph.D. in Political Science at Stanford University, March 2017, “Reducing Tensions Between Russia and NATO,” Council on Foreign Relations: Center for Preventative Action, <https://www.cfr.org/report/reducing-tensions-between-russia-and-nato>

Although some NATO members have failed to live up to the alliance’s democratic ideals, their integration into the NATO community and continuing desire for the security benefits it provides may serve as a brake on what otherwise could be **untrammeled authoritarianism**. At a time of growing ethnic nationalism in Europe, NATO’s integration of European military command structures and the continued European reliance on U.S. intelligence and force projection capabilities through NATO is especially important. One of NATO’s early purposes was not merely to deter the Soviet threat but to bring postwar German military forces into the alliance structure and calm French fears of a third world war. NATO was a crucial enabler of peace not only after World War II but also after the Cold War because some Europeans feared that German reunification in 1990 could create a new military juggernaut. **NATO’s military integration now means that even if right-wing nationalists were to rule a European state, they could not threaten their neighbors** without a drastic and expensive overhaul of force capabilities, deployments, infrastructure, and policy, providing a long warning time for any possible aggression. NATO continues to provide protection not merely from Russia but within Europe itself.

#### Democracy solves global nuke war – extinction

Yulis 17 (Max, Penn Political Review, “In Defense of Liberal Internationalism”, 4/8, pennpoliticalreview.org/2017/04/in-defense-of-liberal-internationalism/)

Over the past decade, international headlines have been bombarded with stories about the unraveling of the post-Cold War world order, the creation of revolutionary smart devices and military technologies, the rise of militant jihadist organizations, and nuclear proliferation. Indeed, **times are paradoxically promising and alarming**. In relation to treating the world’s ills, fortunately, **there is a capable hegemon**– one that has the ability to **revive the world order** and traditionally hallmarked **human rights, peace, and democracy**. The United States, with all of its shortcomings, had crafted an international agenda that significantly impacted the post-WWII landscape. **Countries invested their ambitions into security communities, international institutions,** and international law in an effort **to mitigate** the **chances of** a nuclear catastrophe or another World War. The horrors and atrocities of the two Great Wars had traumatized the global community, which spurred calls for peace and the creation of a universalist agenda. Today, the world’s fickle and declining hegemon still has the **ability, but not the will**, to uphold the world order that it had so carefully and eagerly helped construct. Now, the stakes are too high, and **there must be a mighty and willing global leader to lead the effort of diffusing democratic ideals** and reinforcing stability through both military and diplomatic means. To do this, the United States must abandon its insurgent wave of isolationism and protectionism, and come to grips with the newly transnational nature of problems ranging from climate change to international terrorism. First, the increase in intra-state conflict should warrant concern as many countries, namely in Africa and the Middle East, are seeing the total **collapse of civil society and government.** **These power vacuums are being filled with** increasingly ideological and dangerous tribal and non-state actors, such as Boko Haram, ISIS, and Al-Shabaab. Other bloody civil wars in Rwanda, Sudan, and the Congo have contributed to the deaths of millions in the past two decades. As the West has seen, however, military intervention has not been all that successful in building and empowering democratic institutions in the Far East. **A civil crusade**, along with the strengthening of international institutions, may in fact be the answer to undoing tribal, religious, and sectarian divisions, thereby mitigating the prospects of civil conflict. During the Wilsonian era, missionaries did their part to internationalize the concept of higher education, which has contributed to the growth of universities in formerly underdeveloped countries such as China and South Korea.[1] In addition, the teachings of missionaries emphasized the universality of humanity and the oneness of man, which was antithetical to the justifications for imperialism and the rampant sectarianism that plagued much of the Middle East and Africa.[2] Seeing that an increase in the magnitude of human casualty is becoming more of a reality due to advancements in military technology and the increasing outbreaks of civil war, **international cooperation and the diffusion of norms that highlight the importance of** stable governance, democracy, and human rights **is the only recourse to address the rise in sectarian divides and civil conflicts**. So long as the trend of the West’s desire to **look inward** continues, it is likely that nation states mired in conflict will devolve into ethnic or tribal enclaves bent on **relying on war to maintain their legitimacy** and power. Aside from growing sectarianism and the increasing prevalence of failed states, an even more daunting threat come from weapons that transcend the costs of conventional warfare. The problem of nuclear proliferation has been around for decades, and on the eve of President Trump’s inauguration, it appeared that Obama’s lofty goal of advocating for nonproliferation would no longer be a priority of American foreign policy.[3] In addition, now that the American president is threatening to undo much of the United States’ extensive network of alliances, formerly non-nuclear states may be forced to rearm themselves. **Disarmament is central to liberal internationalism**, as was apparent by the Washington Naval Treaty advocated by Wilson, and by the modern CTBT treaty. The reverse is, however, being seen in the modern era, with cries coming from Japan and South Korea to remobilize and begin their own nuclear weapon programs.[4] A world with more nuclear actors is a formula for chaos, especially if nuclear weapons become mass-produced. Non-state actors will increasingly eye these nuclear sites as was the case near a Belgian nuclear power plant just over a year ago.[5] If any government commits a serious misstep, **access to nuclear weapons on the behalf of terrorist and insurgent groups will become a reality,** especially if a civil war occurs. States with nuclear weapons require domestic stability and strong security, which is why states such as Israel, North Korea, and Pakistan could be in serious trouble in the event of a domestic uprising or military coup. The disarmament of all states is essential for human survival, and if it is not achieved, then **a world full of nuclear weapons and** an international system guided by realpolitik could give rise to nuclear warfare. In today’s world, nuclear weapons leave all states virtually defenseless. But, **for nuclear deproliferation to become a cornerstone of the global agenda,** a pacifying and democratic power must **rise to the limelight to advocate the virtues of peace, stability, and human rights**. Those who equivocate democratic interventionism as an idealistic crusade cannot be further from the truth.Some, however, see it as an effective foreign policy that has a grand scheme for peace in mind.[6] The latter contention, despite being widely disputed, **holds the premise for the democratic peace theory**. Throughout the history of all democracies, not one modern-day democracy has fought against another democracy.[7] Whether that’s because of ideational symmetry, similar objectives and morals, or generally pacific foreign policies, **such a phenomenon must be given attention by policymakers.** According to liberal internationalists, democracies make better partners, tend to move towards increased political and moral agreement, oppose illiberal regimes, and support disarmament policies. This supposition is heavily supported by the smooth post-WWII transitions that the German, Japanese, and Italian governments underwent. All of the governments were formerly fascistic and authoritarian, but with intensive military and economic support from the West, they became some of the most shining exemplars of democratic societies. Even today, Germany is the backbone of the European Union and repeatedly champions democratic norms, such as human rights, economic freedom, and individual liberty.[8] Equipping other countries with the necessary foundations for democracy is no easy feat, but **the fight for peace far outweighs the costs of inhabiting a world rife with nuclear-armed authoritarian and belligerent states**. In conclusion, liberal internationalism can have a lasting legacy on the prospects for peace if it is executed properly. **Putting democracy, humanism, and liberty on a pedestal is what states ought to do if they seek to** save humanity **from itself**. Although the rise of transnational issues pertaining to climate change, nuclear weapons, and civil wars should make international cooperation an increasingly desired aim, states seem to be thinking just the opposite. Only time will tell whether this is a short-lived trend, or a more ominous warning for the world at large.

### 2AC --- NATO Cohesion Impact

#### NATO is key to avert all existential threats

Nicholas Burns 18. Barbara Goodman Family Professor of the Practice of Diplomacy and International Relations, Harvard Kennedy School; Director, American Secretaries of State Project. “Assessing the Value of the NATO Alliance.” Harvard’s Belfer Center. 9/5/2018. https://www.belfercenter.org/publication/assessing-value-nato-alliance

Mr. Chairman and Mr. Menendez, you have asked for an assessment of NATO’s value to the United States. In my judgment, NATO continues to be of vital importance to American security interests in five principal ways. First, NATO is at the core of one of the most significant foreign policy accomplishments in American history—the creation of a long-term peace in Europe following the close of the Second World War. Because of NATO and the emergence of the European Union, Europe is united after centuries of division and war. NATO’s military strength has been a major reason for the absence of war with the Soviet Union and Russia since 1949. A recent Atlantic Council study reminds that America spent 14.1 percent of its GDP on defense during the First World War, 37.5 percent during the Second World War and 13.2 percent during the Korean Conflict. We spend nothing close to those levels now in large part due to the great power peace we have enjoyed for over seventy years. NATO has been a major factor in that peace. And due to the expansion of NATO and the European Union eastward after the fall of the Soviet Union, millions of East Europeans now live in free, democratic societies—a significant success for U.S. diplomacy. Second, NATO delivers additional benefits to U.S. military objectives and operations beyond our shores. NATO is at the heart of our defense of North America and Europe from nuclear and conventional threats. British and French nuclear weapons join ours in deterring aggression in the North Atlantic area. Since the late 1940s, every Administration has believed that the best way to defend our country is through American forces forward deployed in Europe with the NATO allies. This strategy remains right for today given Russia’s invasion of Georgia in 2008, of Crimea and Eastern Ukraine in 2014 and its current pressure on Estonia, Latvia, Lithuania and Poland. NATO remains our primary vehicle for deterring Putin in Eastern Europe. The NATO allies host a great number of critical bases for U.S. forces—Ramstein in Germany, Aviano in Italy, Rota in Spain, Souda Bay in Greece and Incirlik in Turkey—that serve as a platform for our presence in Europe, as well as for U.S. force projection against terrorist groups in North Africa and the Middle East and for our continued military operations in Afghanistan. Europe is a critical link in the development of our Ballistic Missile Defense network focused on the Middle East with Turkey, Romania, Poland, Germany, Spain, the Netherlands, Denmark, the UK and other allies all hosting elements of this system. NATO allies continue to participate in the U.S.-led coalition against the Islamic State in the Middle East. Many of the allies play lead roles in other counter terror operations such as French forces in Mali supported by the U.S. In Afghanistan, the NATO allies remain with us in combat operations and in training the Afghan military. Over 1000 soldiers from European and other partner nations have died there during the last seventeen years. NATO continues to maintain the hard-earned peace in Kosovo with European troops bearing the large share of the burden. An EU-led force has taken on all of the peacekeeping responsibility in Bosnia, freeing up the U.S. for other activities. Third, the NATO allies are among our closest and most supportive global partners as we confront the great transnational challenges that define this century—the fight against terrorism, the entire complex of cyber threats, climate change, the risk of pandemics, mass migration and others. The NATO allies and our partners in the European Union act together with us on these and other issues. This is of incalculable benefit to the U.S. Neither Russia nor China have treaty allies. NATO is a significant advantage for the United States when it acts as a force multiplier for American interests.

### 1AR --- NATO Cohesion Impact

**An integrated NATO is key to numerous existential threats**

Goldgeier 10 – James M. Goldgeier, James Goldgeier is a Professor of International Relations and Robert Bosch Senior Visiting Fellow at the Center on the United States and Europe at the Brookings Institution. He was a Visiting Senior Fellow at the Council on Foreign Relations from 2017-19 and in 2018-19, he held the inaugural Library of Congress Chair in U.S.-Russia Relations at the John W. Kluge Center. Ph.D., Political Science, University of California, Berkeley; M.A., Political Science, University of California, Berkeley; A.B., Government, Harvard University, Febuary 2010,“The Future of NATO,” Council on Foreign Relations Press, <https://www.cfr.org/report/future-nato>

If the North Atlantic Treaty Organization (NATO) did not exist today, the United States would not seek to create it. In 1949, it made sense in the face of a potential Soviet invasion to forge a bond in the North Atlantic area among the United States, Canada, and the west European states. Today, if the United States were starting from scratch in a world of transnational threats, the debate would be over whether to follow liberal and neoconservative calls for an alliance of democracies without regard to geography or to develop a great power concert envisioned by the realists to uphold the current order. The United States is not, however, starting from scratch, and **NATO should not disappear.** While the bonds across the Atlantic may be frayed, they are stronger than those tying the United States to other parts of the world. Common history and values matter, as do the resources (both financial and military) that Europe possesses. The NATO allies share a common interest in preventing disruptions to the **global economy**, including **attacks on freedom of navigation**. As a community of democracies, the member states are threatened by forces such as Islamic extremism and the **rise of authoritarian states**. For the United States, the alliance is a source of legitimacy for actions in places like Afghanistan. For Europe, **NATO is a vehicle for projecting hard power**. While NATO alone cannot defend against the range of threats facing the member states, it can serve as the hub for American and European leaders to develop the ties with other institutions and non-European countries necessary to provide for the common defense. For all its faults, NATO enables the United States to partner with **close democratic allies** in ways that would be difficult without a formal institution that provides a headquarters and ready venue for decision-making, as well as **legitimacy and support for action that ad hoc U.S.-led coalitions do not.** As has been true since the fall of the Berlin Wall two decades ago, the United States (and Europe) should want **NATO** to succeed. After the Cold War, the alliance dramatically redefined itself. In the 1990s, it fostered stability across **Europe** by beginning its process of enlargement to the formerly communist east and by intervening to stop genocide in the Balkans. In the 2000s, it broadened its scope through the mission in Afghanistan as well as a **counterterrorist operation** in the Mediterranean and counterpiracy efforts in the Gulf of Aden and off the Horn of Africa (in addition to continuing the enlargement process). But as NATO has broadened its scope, some members have grown concerned that the alliance is shifting its attention away from Europe. These members seek to return NATO to a more traditional understanding of its role defending against threats on the continent, particularly as an increasingly authoritarian and assertive Russian government has sought to reclaim a sphere of influence lost in the Soviet collapse. In November 2010, NATO will release a new “strategic concept” to guide the alliance going forward. That document must state clearly that providing for collective defense in the twenty-first century goes well beyond defending against the “armed attack” of Article V. To remain relevant, NATO must expand its traditional understanding of collective defense to confront the twenty-first-century threats of **terrorism**, **proliferation of weapons of mass destruction** (WMD) to both states and nonstate actors, and **cyberwarfare.** By necessity, the United States has turned its attention away from Europe in order to **counter these modern threats**, which largely emanate from Africa, the broader Middle East, and Asia. **If NATO fails** to accept a growing global role, then the United States will lose interest in investing in the alliance’s future. But Europe faces these threats too and must recognize that a more robust NATO offers it **the chance to counter them.** Given the varied nature and source of threats today, NATO can be successful only if the Europeans agree to stronger NATO-European Union (EU) cooperation and to closer ties with major non-European democracies, particularly those in the AsiaPacific region.

### 2AC --- Alliance Impact

#### Unraveling of the global alliance system triggers every impact—And solves nothing, because history proves that the war will come to us

Mira Rapp-Hooper, Stephen A. Schwarzman Senior Fellow for Asia Studies at the Council on Foreign Relations and a Senior Fellow at Yale Law School’s Paul Tsai China Center, 2020, Saving America’s Alliances: The United States Still Needs the System That Put It on Top, Foreign Affairs

The stakes of failing to reform the alliance system could scarcely be higher. If Washington does not act, it will miss the opportunity to protect its dearest interests on relatively favorable terms, before China’s growing power and Russia’s revanchism undermine the system’s proven guarantees. The reform agenda recommended here is vast, but it is far less burdensome than a U.S. foreign policy that cannot rely on allies. The United States can no more go it alone now than it could in the immediate postwar years. Whether the United States has alliances or not, American security and prosperity will still require an open and independent Asia and Europe. Even if Washington pulled back from both theaters, the United States would still face cyberattacks, financial and infrastructural disruptions, and assaults on its democratic institutions. And by retrenching, Washington would lose whatever readiness for conflict it currently has. If the country later joined a war abroad, it would have to do so only after significant time delays and without the allied cooperation that might have allowed it to prevail. Put simply, the United States might fall into a conflict that it could have instead deterred—one now waged with hypersonic speed and destruction.

### 2AC --- AT --- NATO Ineffective

#### NATO is effective — neg authors are overly critical.

Skaluba 22 — Christopher Skaluba, Director of the Scowcroft Center for Strategy and Security, former Adjunct Professor at Syracuse University, 2022 (“No consensus? No problem. Why NATO is still effective,” *Atlantic Council,* January 18th, Available Online at https://www.atlanticcouncil.org/blogs/new-atlanticist/no-consensus-no-problem-why-nato-is-still-effective/)

Critics of the alliance (and even some supporters) have interpreted NATO’s unwillingness to militarily support Ukraine—especially during the most significant challenge to the European security order since the Cold War—as an indicator of its declining relevance, timidity, or its divisions. But that overstates the importance of political consensus to NATO’s value and understates its role as an effective and flexible defensive alliance. This is a role with potentially critical benefits for Ukraine.

First, it sets too high a bar for an alliance of thirty members with aligned, but distinct, priorities. Unanimity on every issue is impossible, let alone one as complex as military support to Ukraine.. In reality, it’s Debate and disagreement, as it should be for any democratic institution, are built-in features of NATO—not bugs astounding how often NATO does reach consensus about issues big and small, creating an unrealistic expectation that it always will. The opposite of consensus is not failure. Suggesting otherwise turns any debate that doesn’t end harmoniously into an indictment of NATO, playing straight into Russian propaganda.

Second, a belief that NATO’s value is tied primarily to achieving consensus on every issue misses the more mundane (and important) ways it supports its allies and partners. Its affinity for process—particularly its ability to build a common situational understanding among its members—is an invaluable tool. Habits of consultation and information sharing, buttressed by deep cooperation on operations, intelligence sharing, defense planning, and interoperability, create the foundation upon which any consensus is to be built. Even in the absence of that agreement, the ability to collectively define threats and jointly train to confront them is immensely valuable in its own right.

Third, these habits of cooperation give NATO members the flexibility to act outside of the Alliance’s frameworks. While NATO does much by consensus—such as its missions in the Baltic states—the skills it helps members develop is central to enabling them to form separate coalitions for action. This happened recently with ample success in taking on the Islamic State. Such flexibility should be a point in NATO’s favor, not evidence of its ineptitude.

In the case of military support for Ukraine, policymakers will find more attractive alternatives for dealing with Moscow’s aggression outside of the auspices of the Alliance. Up to and including its recent dialogue with Russia, it has taken a host of consensus actions to support Ukraine—from condemning Kremlin aggression and standing up for Kyiv politically to reaffirming its open-door policy with an expectation that Ukraine will eventually become a member. It might even share intelligence and develop training and advisory programs for the Ukrainian military.

And while it won’t find a consensus to fight, it could provide the foundation for certain allies to support Ukrainian forces in ways consistent with their national priorities outside of NATO. In that case, NATO’s enabling value to its members in complicating Putin’s cost-benefit assessment should be applauded.

Last week’s NATO-Russia Council meeting showcased an Alliance working in lockstep and finding political consensus in responding to preposterous Russian demands. NATO should always strive for this degree of consensus. But if and when this crisis intensifies, and Putin advances further into Ukraine, expectations for NATO assistance will be raised, decisions about how to respond will become more difficult, and consensus will be more elusive.

### 1AR --- AT --- NATO Ineffective

#### Empirical evidence flows aff.

Hamilton 22 — Lee Hamilton, Senior Adviser for the Indiana University Center on Representative Government, Distinguished Scholar at the IU Hamilton Lugar School of Global and International Studies, Professor of Practice at the IU O’Neill School of Public and Environmental Affairs, 2022 (“Commentary: NATO still relevant, still facing challenges,” *The Daily News,* February 4th, Available Online at https://www.newburyportnews.com/opinion/commentary-nato-still-relevant-still-facing-challenges/article\_b7d2cbe6-845a-11ec-824f-e7dc02262f0f.html)

The North Atlantic Treaty Organization is the largest peacetime alliance in the world and has been arguably the most successful such alliance in history.

It has had remarkable success in achieving its basic goals: containing Soviet expansion, checking the rise of nationalism and helping integrate Europe.

It provides a model for multinational cooperation, something we desperately need in today’s complex and dangerous world. and it has shown an admirable ability to adapt to changing needs and circumstances.

Three decades ago, with the collapse of the Soviet Union, it was possible to think NATO had outlived its basic mandate. But it found new and important responsibilities in combating ethnic violence and civil war, as in the former Yugoslavia, and countering terrorism.

It maintains an array of peacekeeping and training activities in Europe, the Mediterranean, the Middle East and Africa.

Today, the crisis over a possible Russian invasion of Ukraine presents new challenges to the alliance while reinforcing the fact that NATO is as relevant as ever. It is essential to the security of our allies in Europe; and because their security is closely tied to our own, it is essential to the United States.

In a sense, NATO rose from the ashes of World War II. Europe had been devastated. An estimated 36.5 million Europeans had been killed, more than half of them civilians.

Millions of people were displaced. America, throwing off its history of isolationism, created the Marshall Plan to rebuild Europe’s economy. But Western leaders worried about the region’s military security. Would the Soviet Union seek to extend its dominance into Western Europe? Would nationalist militarism bubble up and lead Europe back toward war?

To address those threats, a dozen nations, including the United States, signed the North Atlantic Treaty in April 1949. In the treaty’s best-known section, Article 5, the members declared that “an armed attack against one of them … shall be considered an armed attack against all of them.” It was a pledge for mutual self-defense.

Within months, the Soviet Union exploded an atomic bomb, putting an exclamation point on the need for deterrence. The Korean War and the Soviet invasions of Hungary in 1956 and Czechoslovakia in 1968 tested NATO, but the alliance held.

It was a measure of the treaty’s success that NATO forces were able to avoid military actions throughout the Cold War.

Over the decades, NATO expanded. Today it includes 30 member nations, three of them former Soviet republics: Estonia, Latvia and Lithuania. It also claims partner relationships with nearly 20 European countries. NATO calls its partnership with Ukraine one of its “most substantial” and says cooperation has increased since 2014, when Russia invaded Ukraine and seized Crimea.

Ukraine has expressed interest in joining NATO. Russian leader Vladimir Putin, who views Ukraine as part of “historical Russia,” portrays that prospect as an existential threat. With an estimated 100,000 troops massed near the Ukrainian border, Russia is demanding a guarantee that NATO won’t let Ukraine join.

The threat of a Russian invasion of Ukraine poses a real problem for NATO. President Joe Biden said last week that “there are differences” among alliance members about how forcefully to respond, depending on what Russia does. Putin is likely to try to exploit those differences. The best way to resolve this crisis, of course, is through tough, clear-eyed diplomacy, with a clear message that Russia will face consequences if it invades. But it’s harder to negotiate from a position of strength when all your allies may not be on the same page.

NATO has achieved remarkable success in maintaining peace and security throughout its 72-year history. It has demonstrated, probably better than any other organization, the importance of multinational cooperation. But as the Ukraine crisis shows, its challenges are far from over.

### 2AC --- AT --- Trust Turn

#### Unwillingness to share new cyber technology undermines cohesion

Bazin, 17 (Aaron Bazin, Lt. Col. PsyD, U.S. Army, 9-27-2017, accessed on 6-19-2022, Army University Press, "An Alliance Divided? Five Factors That Could Fracture NATO", <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2018/An-Alliance-Divided-Five-Factors-That-Could-Fracture-NATO/)//Babcii>

Organizational structures and processes. This project’s focus groups concluded that NATO’s rigid organizational processes that hold onto the past could result in an Alliance “unable to evolve with member states’ national interests.” Bureaucratic politics within the Alliance structures could cause NATO’s **slow adaptation to contemporary needs and values**. For instance, the participants listed the top-down defense planning process of determining capability requirements as a case where the Alliance and evolving national interests do not align. Furthermore, civil-military frictions on both NATO and national levels could negatively affect readiness of the forces. Long decision-making processes and underdeveloped institutional procedures in national headquarters could prevent the Alliance from developing a legal framework for a common course of action under the NATO flag; for instance, in addressing new adversaries that use unconventional means such as cyber. Put simply, **NATO cannot be faster than the individual countries** that make it up. Lastly, size matters; cohesion is more difficult to forge and maintain in an ever-enlarging alliance, especially when increasingly divergent national interests tend to change the modus operandi of the Alliance. More rather than less often, NATO’s international staff will need to find compromise during its decision-making processes between a political and formal equality hoped to enhance Alliance cohesion on the one hand and the desirable Alliance effectiveness on the other hand. Technology advances. The participants agreed that **technology advances are important for NATO’s continued cohesion**. Technology will constitute a significant intervening factor in how NATO nations maintain their cohesion in the future for three reasons. First, ever-evolving communication technology can facilitate the spread of risks coming from outside of the Alliance and exacerbate their negative effect. The examples that resonated the most during focus group sessions are information warfare and targeted propaganda against NATO nations. Internet communications technology creates infinite room for alternative media that distort reality, contribute to the emergence of populist and radical movements, and increase the danger of miscommunication among nations. Second, NATO risks losing the innovation game to the commercial defense industrial sector. In the future, private companies will continue to stay ahead of NATO in designing specifications and setting standards for platforms. This can have a major impact on readiness and interoperability among NATO nations if their innovation efforts (e.g., the U.S. Third Offset Strategy) do not materialize.31 Third, some nations may become reluctant to share their latest technology acquisitions, especially if they put private gains above the collective endeavor. **This would pose a challenge** “for anyone to share information they own without gaining any profit for themselves.” The political unwillingness may feed distrust, which can result in a deepening interoperability gap between allies on the battlefield, and ultimately, a less cohesive Alliance.

#### Network intrusions are the largest internal link --- They destroy confidence in the alliance --- Sustained cooperation and integration is essential

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>

Steady divergence Yet when it comes to the direction of allies’ cyber policy, growing **differences are apparent** – especially in the development and deployment **offensive cyber capabilities**. First, even though most states now have – or are in the process of – establishing a cyber command, operational capabilities vastly differ across states. Whereas some governments are increasingly allocating significant resources to conduct cyber operations – and are now starting to benefit from these investments – the majority of allies still run their cyber commands on a budget of a few million a year –an amount that is insufficient for effective operations in the cyber domain. Secondly, until a few years ago, NATO members’ strategic visions were largely aligned. National cyber strategies shared a common threat focus on operations that could potentially cause major societal havoc, such as taking down the power grid. Allies’ national strategies were also largely unified in their vision to address this threat, discussing the need for deterrence, resilience, and norms. However, this changed with the publication of the US Department of Defense’s strategy on **Defend Forward** and US Cyber Command’s vision on **Persistent Engagement**.[[8]](https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/#_ftn8) The United States emphasizes the need to **cause friction** “wherever the adversary maneuvers,” operating “globally, continuously and seamlessly” (potentially) below the threshold of armed attack. “We must…maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries,” in the words of NSA director and Cyber Command head Gen. Paul Nakasone.[[9]](https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/#_ftn9) Whereas deterrence is about changing your adversary’s cost-benefit calculus, Persistent Engagement is about taking the opportunity away from the adversary to act.[[10]](https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/#_ftn10) Third, NATO member positions on how international law applies – particularly the obligations of states vis-a-vis sovereignty – **are now more divergent than a decade ago.** Whereas countries like the Netherlands and France are located on the side of the “**sovereignty as a rule” camp**, the United Kingdom has taken the position that a remote cyber operation by one state into another’s cyber systems or network does not violate the latter’s sovereignty. Where to go from here? The **divergence** in cyber policy across NATO member states **is problematic**. Allies disagree on both the goals of cyber policy and the ways and means to achieve them. **This can cause tension between allies**, especially when it comes to the necessity and legitimacy of operating on each other’s national systems and networks. Some may argue that these differences result from differences in maturity. Some states simply have not caught up with the latest developments, goes the argument. This assumes a single path to cyber maturity or that the dynamics of cyberspace pull all states in the same direction. It suggests that – even without major policy coordination – allies’ cyber policies will converge over time. But a more persuasive understanding of the current trend is that even though states can learn from each other’s institutional progress, differences do not merely stem from states “lagging behind.” **These states are on a different policy path**. This means it requires dedicated and sustained policy attention to, at a minimum, **coordinating the different policies of states** – and potentially bring them closer together.

## Extra

### Extra --- Random Cards

#### US expertise and resources necessary for quick and flexible NATO cyber response

Albon et al., 22 (Lillian Albon, [Anika Binnendijk](https://www.rand.org/pubs/authors/b/binnendijk_anika.html), [Quentin E. Hodgson](https://www.rand.org/about/people/h/hodgson_quentin_e.html), [Bilyana Lilly](https://www.rand.org/pubs/authors/l/lilly_bilyana.html), [Sasha Romanosky](https://www.rand.org/about/people/r/romanosky_sasha.html), [David Senty](https://www.rand.org/pubs/authors/s/senty_david.html), [Julia A. Thompson](https://www.rand.org/pubs/authors/t/thompson_julia_a.html)Lillian Ablon is an information scientist at the RAND Corporation and a professor at the Pardee RAND Graduate School., 6-1-2022, accessed on 6-16-2022, Rand, "Cyberspace as a Military Domain: Lessons for NATO", <https://www.rand.org/pubs/perspectives/PE329.html>)//Babcii

The integration of cyber effects into military operations to operationalize the domain fully is an **ongoing process** at the national level, just as it is an area of development for NATO. The **United States**, for example, has **experimented with multiple approaches** to develop planning processes and personnel to integrate with operational staffs—including liaison officers from its Cyber Command to the geographic and other functional combatant commands and creating Joint Cyber Centers across the headquarters staffs to combine intelligence, operations, planning, and communications—but these approaches are still **evolving**. In addition, the authorities to execute cyber operations, while often focused on offensive action, are also an ongoing discussion in defensive operations. This is where **a series of high-level strategy and operational tabletop exercises** can **inform** NATO how best to **identify the key issues**, **experiment with alternative constructs**, and **evaluate the most useful approach** that works for the alliance. Workforce NATO will need staff officers, civilian personnel, and other augmentees who not only are steeped in the technical aspects of cyberspace but also understand how cyberspace operations can contribute to the overall success of NATO NATO concluded an agreement with the Estonian government in 2014 to leverage its national cyber range for NATO use.52 Determining whether this range architecture is sufficient for all of NATO’s needs will first depend on conducting a needs assessment and capability gap analysis. It is reasonable to conclude that NATO’s exercise and training regimen for cyberspace will **grow** in the coming years, which would indicate a **need for more capacity** and **certainly** a need for **greater range capability** to adapt to changing technology.

#### Enhanced US cooperation is essential to establish solidified defense

Holcomb, 20 (Franklin Holcomb, Franklin Holcomb is a Title VIII Fellow in the Transatlantic Leadership program at CEPA with a focus on Russian and Eastern European security and political analysis. graduated from Texas A&M University with a double major in Russian Language and International Studies: Politics and Diplomacy. He is finishing his master’s degree in Democracy and Governance at the University of Tartu , 12-4-2020, accessed on 6-16-2022, CEPA, "Countering Russian and Chinese Cyber-Aggression | CEPA", https://cepa.org/countering-russia-and-chinese-cyber-aggression/)//Babcii

SECTION 3: THE UNITED STATES AND EUROPE

The United States must expand cooperation with its central and eastern European partners not only to help bolster their defense capacity but also to help the United States better understand hostile cyber actors’ activities and how to counter them. Central and eastern European governments and societies are committed to improving regional cybersecurity and have had to think creatively about becoming more resilient. The United States has partners across central and eastern Europe eager to share their frontline experience in defending against hostile hacking and information attacks on their cyberspace.

That experience dealing directly with hostile cyber actors, combined with U.S. resources and expertise, could vastly improve the security of both the United States and Europe. “If you want to be more secure, you need to do practical work with those who face a real threat from the East,” Kerza said. “If you sit at home thinking that a cyberattack will never reach you, you’ll be wrong.”[22](https://cepa.org/countering-russia-and-chinese-cyber-aggression/#footnote_21_6693) Meanwhile, Iti Press, the counselor for cyber issues and economic affairs at the Estonian Embassy in Washington, said many Estonian cybersecurity experts have struggled to get access to their U.S. counterparts and emphasized the importance of improving participation in joint cyber exercises taking place **in the United States**.[34](https://cepa.org/countering-russia-and-chinese-cyber-aggression/#footnote_33_6693) Sven Sakkov, the former director of ICDS, described U.S. involvement in the **NATO** CCDCOE in Tallinn, where only one member of the 30 senior staff is an American, as **“underwhelming”** and urged greater U.S. participation.[35](https://cepa.org/countering-russia-and-chinese-cyber-aggression/#footnote_34_6693) Likewise, the Latvian defense counselor in Washington, Rolands Heniņš, said, “We are there on the front line facing malign influence for over 30 years, and we have learned our lessons. Use our smart people and knowledge.”[36](https://cepa.org/countering-russia-and-chinese-cyber-aggression/#footnote_35_6693) Joanna Świątkowska, the former European Cybersecurity Forum official, said the United States and Europe should expand the sharing of threat indicators and early warning information to help harden European and American cyber defenses and present a united front to hostile actors.[3](https://cepa.org/countering-russia-and-chinese-cyber-aggression/#footnote_2_6693) And Solvita Denisa-Liepniece of the Baltic Center for Media Excellence said the United States could learn from eastern European journalists how hostile states conduct disinformation campaigns and media manipulation.[31](https://cepa.org/countering-russia-and-chinese-cyber-aggression/#footnote_30_6693)

**American**-European cooperation in cyberspace will be vital to ensuring the security of the transatlantic community in the face of shared threats from Russia and China. It is highly unlikely that these foes will ever be deterred from launching cyberattacks, but by working together American and European countries can be prepared to manage these attacks as they come and exact a high price on those conducting them. In the coming years, the United States should focus on **engaging** more with its European partners.

U.S. Cyber Command should conduct more bilateral and multilateral cyber defense exercises across Europe, with a focus on engaging central and eastern European states and expert communities. U.S. Cyber Command should improve existing information-sharing frameworks with its counterparts in central and eastern Europe. The U.S. government broadly should bring eastern European cybersecurity and disinformation experts to the United States, where they can engage with, learn from, and teach their American counterparts. The U.S. government should also send U.S. experts to work directly with their counterparts in Europe. The U.S. government should coordinate strong joint responses with European countries against particularly dangerous or reckless cyber actors such as Russia. The U.S. policy community should engage with eastern European officials and experts to learn about the effectiveness of various methods of improving cyber resilience employed in central and eastern Europe. The U.S. State Department and Congress should increase dialogue with European governments and the European community to improve and expand ways to name, shame, and sanction hostile cyber actors. The U.S. government should increase financial assistance for central and eastern European cyber defense and research programs through initiatives such as the Countering Russian Influence Fund.

#### The US can’t do it alone --- Whole of system is key

Talihärm, 13 (Anna-Maria Talihärm, Anna-Maria Talihärm is Senior Analyst of the Legal and Policy Branch, NATO Cooperative Cyber Defence Centre of Excellence , August 2013, accessed on 6-16-2022, United Nations, "Towards Cyberpeace: Managing Cyberwar Through International Cooperation | United Nations", <https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation)//Babcii>

Despite the lack of consensus on exactly what constitutes cyberwarfare or cyberterrorism, governments need to ensure that their infrastructure is well protected against different types of cyberthreats and that their legal and policy frameworks would allow to effectively prevent, deter, defend and mitigate possible cyberattacks. Not being able to agree on common **definitions of central terms** such as “cyberattack” and “cyberwar” should not prevent states from expressing the urgency of preparing their nations for possible cyberincidents.

INTERNATIONAL **COOPERATION**

The logic of international cooperation and collaboration lies on why, when, and how to collaborate, and generally takes place in order to follow one’s interests or to manage common aversions.1 In the context of cybersecurity, the need for international cooperation between states, international and regional organizations and other entities **is emphasized by the borderless and increasingly sophisticated nature of cyberthreats.** Principally, any actor, whether it is a country or a non-governmental organization, following its objectives in cybersecurity requires cooperation from a wide range of international partners. In fact, much of the international collaboration will occur outside specific national frameworks, emphasizing the Whole of System approach that **stresses the need to take into account all relevant stakeholders**.2

## T

### 2AC --- CI --- Security Cooperation

#### Security coop is any action by the DOD including information sharing

**Joint Chiefs of Staff, 17** (Joint Chiefs of Staff, The Joint Chiefs of Staff is the body of the most senior uniformed leaders within the United States Department of Defense, May-23-2017, accessed on 6-16-2022, Jcs, "Security Cooperation", https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\_20\_20172305.pdf)//Babcii

Security cooperation (SC) encompasses all Department of Defense (DOD) interactions, programs, and activities with foreign security forces (FSF) and their institutions to build relationships that help promote US interests; enable partner nations (PNs) to provide the US access to territory, infrastructure, information, and resources; and/or to build and apply their capacity and capabilities consistent with US defense objectives. **It includes**, but is not limited to, military engagements with foreign defense and security establishments (including those governmental organizations that primarily perform disaster or emergency response functions), DOD-administered security assistance (SA) programs, combined exercises, international armaments cooperation, and **information sharing and collaboration**.

## Security K

### 2AC --- No Link

#### OCOs are a unique danger --- they’re not securitized.

Gomez 16 – Senior Researcher at the Center for Security Studies at ETH Zurich, Assistant Lecturer at De La Salle University, M.A. in International Security from the Institut Barcelona d’Estudis Internacionals

Miguel Alberto N. Gomez, “Arming Cyberspace: The Militarization of a Virtual Domain,” Global Security and Intelligence Studies, Spring, https://www.ibei.org/arming-cyberspace-the-militarization-of-a-virtual-domain\_54871.pdf

Conclusions and Future Direction

The growing number of OCOs being attributed to state or state-sponsored actors demands a better understanding of the underlying factors that result in the militarization of cyberspace. While the existing literature posits two seemingly incompatible arguments centered on either fear-based rhetoric or rational choice, the study has demonstrated that both these factors account for the varying levels to which cyberspace has been militarized across states.

On the one hand, while increasing societal use of information communication technologies have led to greater risks associated with these technologies, the capabilities developed that are necessary to mitigate such could similarly lead to the transform the domain of cyberspace for use in warfare. Aside from the re-tasking of defense technologies, there is now the appearance of technologies once associated with the criminal elements of cyberspace in OCOs attributed to state or state-sponsored actors. The malleability of this technology supports the argument that increasing use alone does not account for the militarization of this domain, but rather the ability to maximize the functionality provides those with this skillset to expand beyond the traditional domains of air, land, and sea.

Equally important—and thus linking the two existent theories—is the continued relevance of conventional military capabilities vis-à-vis the use of cyberspace. While there is no doubt as to the advantages offered by this virtual domain, namely its asymmetric characteristics, low cost of entry, and challenges of attribution; these exist in conjunction with the stated policy goals of a state. The ability to employ this domain is dependent on conventional military capabilities to consolidate whatever gains were obtained in the process. Although it would be theoretically possible to utilize OCOs to disrupt a state’s critical infrastructure in times of war, the impermanence of the damage caused requires additional resources to be brought to bear in order to force a change in policy or behavior of a given adversary.

Viewed as the causal explanations for the militarization of cyberspace, the risk faced by a state may be understood as the catalyst that encourages the militarization of this domain. However, without conventional military capabilities that could be used to apply constant pressure on one’s adversaries, viewing OCOs as a revolution in military affairs is of limited value.

With this in mind, what role do the other aspects (e.g., regime type, rivalry, and elite influence) identified by the literature have on militarization? Although the study has not demonstrated that these to have a direct causal influence on militarization, this does not suggest that no relationship exists. As previously mentioned, the nature of the quantitative techniques applied could lead to differing results if the number of observations is increased. Regime type, for instance, could influence the type of risk faced by states and, in turn, influence the technologies developed to meet these risk. Hare’s model captures this and is seen clearly in cases of states such as that of the United States and the People’s Republic of China (PRC). The former perceives threats to its critical infrastructure and other services in cyberspace. Consequently, this prompts the development of technologies to ensure resilience and pro-active prevention of disruptive events. The latter, in contrast, is concerned with dissent and political activism in cyberspace. Consequently, this results in the emergence of censorship technologies that do not translate directly to offensive capabilities in cyberspace— though espionage-related capabilities would benefit from these (Giles and Hagestad 2013; Hare 2010).

Similarly, perceived risk originating from internal threats could account for the decision to engage (or not) in OCOs against other rival states. However, cases such as that of the PRC do not follow this line of reasoning as the most prominent of their activities in this domain have been directed against their military, political, and economic rivals.

Lastly, the influence of elites in the militarization of this domain could, in the view of authors such as Nissenbaum, be constrained by a lack of understanding of its nature and the continued lack of synergy between experts in technology and national policy (Hansen and Nissenbaum 2009). This would lead to a situation wherein political elites could, and do, vocalize the dangers posed by cyberspace but lack the proper understanding of how to apply these technologies as a tool to support national policies and goals.

The manner in which states conceptualize cyberspace at this point in time finds parallels with that of the mid-twentieth century and the advent of nuclear war. While the technology of the time offered to revolutionize warfare, few understood the implications of such and the extent with which these would alter the relationship between states and their respective military strategies.

### 1AR --- No Link

#### Overarching theories don’t apply.

Gomez 16 – Senior Researcher at the Center for Security Studies at ETH Zurich, Assistant Lecturer at De La Salle University, M.A. in International Security from the Institut Barcelona d’Estudis Internacionals

Miguel Alberto N. Gomez, “Arming Cyberspace: The Militarization of a Virtual Domain,” Global Security and Intelligence Studies, Spring, https://www.ibei.org/arming-cyberspace-the-militarization-of-a-virtual-domain\_54871.pdf

The increasing frequency of offensive cyberspace operations (OCOs) directed toward states, particularly the disclosure of Stuxnet in 2010 that appears to have been aimed at disrupting Iran’s nuclear development program, has prompted a reassessment of state behavior in cyberspace. In the years since, states have gradually militarized cyberspace through the establishments of various programs that have framed this as a new domain of warfare. Yet despite the pace of these transformations, a unified theoretical understanding of this phenomenon continues to remain conspicuously absent. To date, scholars have attempted to explain such by highlighting the advantages offered by cyberspace while others have cited the growing fear-based rhetoric grounded by the increasing societal dependence on technology. Neither of these, however, can adequately explain why certain states have militarized while others have not despite predictions of such taking place. Consequently, this study, encompassing the period from 2011 to 2014, proposes that depolarizing these respective arguments may close the existing theoretical gap. In doing so, the study employs a quantitative analytical approach that examines how cyberspace had been militarized across states as a function of both strategic considerations and resource requirements which are both driven by rational choice and societal perceptions regarding this domain.

## PTX DA

### 2AC --- No Link

#### Increased support AND coop with NATO is inevitable BUT popular

CRS, 21 (CRS, Congressional Research Service, June-3-2021, accessed on 6-19-2022, Sgp.fas, "NATO: Key Issues for the 117th Congress", https://sgp.fas.org/crs/row/R46066.pdf)//Babcii

President Biden has signaled support for Stoltenberg’s proposals and, more broadly, has pledged renewed U.S. support for NATO and increased cooperation and consultation with NATO allies. Although these statements have been welcomed across NATO, analysts caution that disagreements between the United States and its allies could persist, including on how best to confront China and Russia and on long-standing concerns about defense spending and burden-sharing. U.S. allies also may continue to question U.S. credibility given policy reversals experienced during the Trump Administration and concerns about longer-term U.S. foreign policy trends, such as a potential embrace of isolationism or a return to “America First” policies by a future Administration. Although many Members of Congress have criticized specific developments within NATO—regarding burden-sharing, for example—**Congress as a whole has demonstrated consistent support for NATO.** During the Trump Administration, congressional support at times was viewed by some as an effort to reassure allies troubled by President Trump’s criticisms of the alliance. Over the past several years, both chambers of Congress have passed legislation reaffirming U.S. support for NATO (e.g., H.Res. 397, H.R. 676, H.R. 5515/P.L. 115-232, and H.Res. 256 in the 115th Congress; S. 1790/P.L. 116-92 and H.R. 6395/P.L. 116-283 in the 116th Congress) and in some cases sought to limit the President’s ability to withdraw from NATO unilaterally (H.R. 676 in the 115th; S. 1790/P.L. 116-92 in the 116th Congress). At the same time, Congress continues to assess NATO’s utility and value to the United States, and some Members are concerned about key challenges facing NATO, including burden-sharing, managing relations with Russia and China, and divergent threat perceptions within the alliance. Contents Introduction ..................................................................................................................................... 1 Key Defense and Security Challenges ............................................................................................ 2 Deterring Russia........................................................................................................................ 3 Transition in Afghanistan .......................................................................................................... 4 Expanding NATO Engagement in Iraq and Addressing Broader Instability in the Middle East and North Africa ................................................................................................ 4 Assessing China’s Impact on NATO and Transatlantic Security .............................................. 5 Enhancing Resilience ................................................................................................................ 6 Defense Spending and Burden-Sharing........................................................................................... 7 Enhancing Political Cohesion.......................................................................................................... 9 Concerns Regarding the U.S. Commitment to NATO ............................................................ 10 Tensions with Turkey .............................................................................................................. 12 Commitment to Democratic Values ........................................................................................ 14 Issues for Congress........................................................................................................................ 15 Figures Figure 1. NATO Members and Dates of Accession......................................................................... 2 Figure 2. Defense Spending by NATO Members, 2013-2020......................................................... 8 Contacts Author Information........................................................................................................................ 16 Introduction The United States was the driving proponent of the North Atlantic Treaty Organization’s (NATO) creation in 1949 and has been the unrivaled leader of the alliance as it has evolved from a collective defense organization of 12 members focused on deterring the Soviet Union to a globally engaged security organization of 30 members (see Figure 1). Historically, U.S. Administrations have viewed U.S. leadership of NATO as a cornerstone of U.S. national security policy that brings benefits ranging from peace and stability in Europe to the political and military support of important allies, including many of the world’s most advanced militaries. During his term in office, former President Donald Trump openly challenged long-standing U.S. support for NATO, however, arguing, among other things, that NATO was a “bad deal” for the United States.1 Although past U.S. presidents criticized burden-sharing dynamics within NATO, none did so as stridently and publicly as Trump. Trump’s criticisms contributed to heightened political tensions between the United States and Europe, prompting some allies to question his Administration’s commitment to NATO and to criticize its perceived unilateral approach to foreign policy issues. Trump Administration officials maintained that the United States remained committed to NATO, highlighting the Administration’s requests in 2017 and 2018 to increase funding for the U.S. force presence in Europe and its efforts to secure defense-spending increases across the alliance in recent years. Many allies have welcomed President Joe Biden’s pledge to renew U.S. support for NATO and to prioritize consultation and cooperation with allies. NATO Secretary General Jens Stoltenberg has said the currentne U.S. Administration presents “a unique opportunity to open a new chapter in relations between Europe and North America.” 2 Allied heads of state and government are to meet at NATO headquarters in Brussels, Belgium, on June 14, 2021, to set NATO’s agenda for the coming year. Key allied priorities include the following:

### 1AR --- No Link

#### Slew of cyber policies are inevitable BUT are wildly popular and build PC

Patel, 22 (Pooja Patel, Senior Manager of Advocacy Signal Ground, 4-21-2022, accessed on 6-19-2022, Signal Group, "Cyber policy isn’t going away anytime soon", https://signaldc.com/cyber-policy-isnt-going-away-anytime-soon/)//Babcii

Throughout the 117th Congress, there continues to be strong bipartisan, bicameral momentum to coalesce around key cybersecurity initiatives. This has been all the more enhanced by the Biden Administration’s prioritization of this issue. Especially in an increasingly tense and partisan atmosphere, where policymakers will continue to diverge from bipartisan agreements with an election on the horizon, cybersecurity issues will continue to be a strong opportunity for lawmakers to facilitate real impact through **efforts that cross party lines.** Thus far in the 117th Congress, cybersecurity policies and funding have garnered attention in nearly every major funding package. This includes large funding infusions within the 2021 American Rescue Plan, the 2021 Infrastructure Investment and Jobs Act, and the FY 2022 omnibus package. Beyond inclusion in these broader packages, there has also been significant traction to move smaller, less controversial **bills** that can **quickly move through the legislative process**, which has been supplemented by strong advocacy efforts from influential cybersecurity leaders on both sides of the aisle. Over the next few months when very little policy will get done due to the upcoming elections, cybersecurity policy remains one of the few areas where policy changes could occur – ranging from large funding opportunities to policy implications concerning jurisdiction of federal cybersecurity programs, and more. Cybersecurity remains well-positioned to receive strong attention over the next several months, and policymakers from both sides of the aisle will continue to act on opportunities to **secure wins** in this policy space.

#### NATO is bi-part

NATO, 22 (NATO, 5-20-2022, accessed on 6-19-2022, NATO, "NATO Secretary General welcomes US Congress Delegation to NATO headquarters", https://www.nato.int/cps/en/natohq/news\_195748.htm)//Babcii

NATO Secretary General Jens Stoltenberg welcomed a US Congressional Delegation to NATO headquarters on Friday (20 May 2022), thanking the **lawmakers** for the strong and bipartisan commitment of the United States to NATO, as **demonstrated** by **both chambers of Congress**. The delegation included Senate and House committee chairs Senator Patrick Leahy, Senator Bob Menendez and Congressman Richard Neal, along with 13 other distinguished Democratic and Republican senators and representatives.

Mr Stoltenberg updated the delegation on work to reinforce NATO's deterrence and defence and on Allies' efforts to provide and sustain support to Ukraine, **including security assistance**. They also discussed the historic application by Finland and Sweden to join NATO. Mr Stoltenberg said he welcomed the strong US bipartisan support for admitting Finland and Sweden into the Alliance.  He also noted the importance of addressing the security concerns of all Allies.

The bipartisan delegation and the Secretary General also discussed next month’s NATO Summit, including strengthening the Alliance’s deterrence and defence and strengthening support for partners. They also addressed burden sharing within the Alliance, and the importance of continued defence investments.

## China DA

### 2AC --- Turn

**The problem is capability NOT intent --- The plans integration of cyber strategy into NATO effectively solves Chinese hybrid war**

Lauren **Speranza 20**, director for trans-Atlantic defense and security at the Center for European Policy Analysis, 7/8/20, “China Is NATO’s New Problem,” https://foreignpolicy.com/2020/07/08/china-nato-hybrid-threats-europe-cyber/

But **NATO**, long worried about Russia, has largely been silent on China. **Now**, that is changing. NATO Secretary-General Jens Stoltenberg recently called on the alliance to stand up to Beijing’s “bullying and coercion,” underscoring how China’s rise is fundamentally shifting the global balance of power. It’s apparent that NATO can **no longer ignore the threat**. If the alliance hopes to **remain competitive**, it will need to develop a **new strategy** for dealing with Beijing. First, NATO needs a **common assessment of China’s hybrid threats**—a mix of diplomatic, economic, security, information, and technological actions designed to quietly undermine democratic states and institutions to Beijing’s benefit while avoiding a traditional conflict. While China’s conventional military threat in the Indo-Pacific is far from NATO’s borders, its hybrid activities are happening in the alliance’s own backyard. **Cyber-espionage**, **i**ntellectual **p**roperty **theft**, **infiltration of critical infrastructure**, **debt manipulation**, and **disinformation** are prime examples. While these threats may **seem** to fall outside of NATO’s purview, they pose serious security risks for the alliance. For instance, China’s desire to invest in Lithuania’s Klaipeda Port may not look like a problem for NATO on its surface. But its investments have worrying strings attached that give China operating control over the infrastructure. That control could decrease allies’ willingness to move military forces—including sensitive technologies—through the port and its surrounding networks. This could lead to disrupted planning and fewer military exercises, decreasing NATO’s ability to defend the Baltic States during a crisis with Russia. This could also open the door for pragmatic collaboration between China and Russia to undermine trans-Atlantic security. Allies need to forge a **shared understanding of these risks through information-sharing and dialogue**—no small feat for countries that do not see eye to eye on China. Some are even willing to ignore such vulnerabilities, due to economic benefits or disenchantment with trans-Atlantic institutions. The **U**nited **S**tates has a **critical role** to play in getting allies **on the same page** and **setting common goals** for countering China’s hybrid activities. Second, NATO needs to focus on public diplomacy. **NATO** has an important role to play in the battle against the CCP’s global narratives, which Beijing promulgates through **hybrid activities**. To defend the trans-Atlantic values on which the alliance is built—freedom, **democracy**, **rule of law**, and **human rights**—NATO should clearly communicate China’s violations of these principles and its propaganda efforts to cover them up. (These include, among others, human rights abuses against ethnic Uighurs in Xinjiang and violations of the U.N. Convention on the Law of the Sea in the South China Sea.) NATO should also enhance its outreach to key partners in the Indo-Pacific, such as Australia, Japan, New Zealand, and South Korea, which can serve as important counterweights to Chinese influence in the region. Effective public messaging also means getting serious about attributing the blame for attacks, as the European Commission recently did over Chinese disinformation around COVID-19, to raise the pressure on Chinese officials. Trans-Atlantic countries have struggled to shape China’s behavior because they cannot prove malign intent or agree to call out Beijing for its subversive efforts. Allies should develop **clearer guidelines**—**what needs to be proved**, **by whom**, **and to what degree**—to enable **collective attribution**. NATO is strongest when it speaks with one voice. It should use that voice to demand transparency and change from China. Third, the alliance should step up its counteroffensive. China’s hybrid actions intentionally blur the lines between what is legally permissible, politically inappropriate, and downright escalatory. This makes it difficult for leaders to determine appropriate responses, producing a reactionary approach thus far. But an intensifying geostrategic competition has already begun. To compete in this environment, the trans-Atlantic community needs a more proactive approach. Rather than waiting for China to invest in the next major European port, allies should coordinate legislation to prevent the riskiest Chinese acquisitions. And rather than waiting for more Chinese cyberintrusions, allies should collaborate on responsible, targeted offensive cyberactions. Over time, this would help dissuade China from manipulating investments in critical infrastructure, conducting cyber-espionage, and other hybrid activities. While adopting a more offensive posture remains controversial among certain allies, it is gaining traction across Europe and is strongly supported in Washington. Although NATO, as a defensive alliance, should not implement such a counteroffensive, policymakers should leverage it as the primary forum to coordinate actions among willing nations. Fourth, NATO needs to deepen its cooperation with other key players, such as the European Union and the private sector. Where NATO lacks the mandate and means, the EU and multinational businesses play critical roles in developing, implementing, and enforcing the legislation and financial incentives necessary to counter Chinese hybrid threats. Complementary to that, NATO and its allies can focus on providing intelligence, defending cyberspace, developing capability targets for new technologies, conducting exercises and **contingency planning**, informing resilience requirements for secure infrastructure, and **bolstering deterrence**. Despite the political obstacles that impede more formal NATO-EU cooperation, allies should look to the European Centre of Excellence for Countering Hybrid Threats in Helsinki to bring together NATO and EU staff, national officials, and industry voices in one place to align their counter-hybrid policies for China. The Chinese government’s manipulative efforts around the coronavirus have thrust China’s hybrid activities to the center of trans-Atlantic debates. Policymakers need to seize the moment and respond by “using NATO more politically,” in Stoltenberg’s words. NATO is first and foremost about its nations. In the fight against China’s hybrid threats, these nations bring much more to the table than military power alone. They have access to a broad range of tools—military, political, economic, technological, and information—which the alliance can use to its collective geopolitical advantage in the competition with China. What NATO needs now is a strategy to leverage those tools in a coordinated manner. That will go a long way in solving NATO’s China problem.

### 1AR --- Turn

#### Closer integration with Europe is key to prevent EU-Chinese coop that allows them to win the race

Schuman 2-16-2021, MA, international affairs, correspondent for TIME. (Michael, "Europe can’t stay neutral in US-China stand-off", *POLITICO*, https://www.politico.eu/article/europe-cant-stay-neutral-in-us-china-stand-off/)

China also represents a long-term economic threat to Europe — not merely because it is an advancing competitor in a global market economy, but because Beijing’s policies are designed to use and abuse that open world economy to eventually dominate it. Beijing’s leadership makes no secret of its goal to foster high-tech industries and national champions to overtake its established Western rivals, fueled by untold billions of state aid. By one estimate, the Chinese government has lavished more than $100 billion on its electric vehicle sector, in the form of subsidies for buyers, research and development support and other aid. Another $49 billion has been committed to create a Chinese competitor to Airbus. Partnerships with European companies are vital to the success of China’s agenda. Beijing sees joint ventures and other corporate cooperation with foreign companies as a way to extract the advanced technology and know-how required for China to catch up to, and then leapfrog over, the Western world. An October report from the Foundation for Defense of Democracies argues that the Chinese are targeting key sectors of the German economy — including industrial equipment and electronics — with the aim of pillaging them. China’s economic relations with Germany are “a template for the CCP strategy to dominate the 21st-century economy and set the rules for the modern world,” the report contends. In other words, by continuing to engage with China, Germany is gaining today, but paving the way to its doom tomorrow. There’s little chance European politicians can talk China into a better relationship. After seven years of negotiations, the EU’s recent investment agreement with China “amounts to so little,” lamented Brussels-based think tank Bruegel in a January analysis. Littered with vague pledges and lacking methods of enforcement, Bruegel noted that even on market access, the agreement’s primary focus, “only a few concessions have been made bilaterally and all of them are limited.” Simply hoping the Chinese will play fair is naïve. While Beijing threatens and blusters that Europeans must keep their markets open to 5G gear from Huawei, the Chinese are sidelining European telecom firms in the China market. Ultimately, China is simply not a true partner for Europe. The longer Europeans fail to grasp this, the weaker their position will become. China will continue to exploit the divisions between democracies to advance its interests. European politicians will strain relations with the U.S. by cynically reaping economic benefits from China while Washington does all the fighting. By the time Europe realizes it needs America’s help, it could discover Washington has found other, more reliable friends. Ultimately, the choice between the U.S. and China should be determined by what Europeans want their role in the world to be. They could defend the liberal order they helped create and continue to participate in global leadership. Or they could sit back and watch authoritarian China knock away the pillars of the current order, and the sources of European influence with them. Is the choice really that hard?

#### The US will be destroyed by Chinese cyber now --- Integrating better capabilities is key

Lewis, 22 (James Lewis, James Lewis writes on technology and public policy at the Center for Strategic and International Studies (CSIS), where he is a senior vice president and directs the Strategic Technologies Program. Before joining CSIS, he was a diplomat and a member of the Senior Executive Service with extensive negotiating, politico-military, and regulatory experience., 2-25-2022, accessed on 6-19-2022, The National Interest, "The West Is Already Fighting in a Cyber Conflict", https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/west-already-fighting-cyber-conflict)//Babcii

The **West’s** historic weakness in cyber defense **encourages opportunism**. Russia began computer network espionage in the 1980s, going after defense research and technology. China began cyber espionage in earnest in the early 2000s, when it connected to high-speed global networks. China is omnivorous when it comes to stealing intellectual property (IP) for commercial purposes. While U.S. cyber defenses are now stronger, **they are not strong enough** to stop these advanced opponents.

Russia has natural advantages. Its cyber efforts build on a decades-long legacy of signals intelligence, espionage, and influence operations. Russia’s universities crank out skilled mathematicians and programmers. Close ties between the Kremlin and the “Vory” (Russian criminal groups that became powerful after the collapse of the Soviet Union) create a culture where crime is deeply interwoven with government. This is blended with (as we have seen in Ukraine) a powerful urge for revanchism and a general disdain for Western democracies that the Biden administration has only just begun to reverse.

China shares Russia’s disdain for democracies. It started out less capable than Russia, but the Chinese government’s massive and continuous cyberespionage efforts have steadily improved its capabilities. Before Xi Jinping took office, Chinese companies routinely hacked each other as well as Western competitors and the PLA freelanced for commercial gain, hacking to steal IP and resell it to Chinese companies. China also has a strong hacker culture connected to its growing technology sector. Xi has sought with considerable success to bring hacking under Chinese Communist Party control and focus it on his strategic goals. Private hackers were told to cooperate or else, People’s Liberation Army hacking was refocused to support national intelligence goals, and China’s foreign intelligence agency, the Ministry of State Security, was allegedly given a larger role in cyber espionage. **There has been a marked uptick in cyber espionage since Xi’s arrival.**

# 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 Treaty301, 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 impending 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 based 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 Islamic State 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 weapons of mass destruction— 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 objective, 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, 2018, 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 European 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 World Trade Organization, 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 International Monetary Fund, 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 United States 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 European 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.