# Case Neg—Wave 1 Complied

# Politics

### 1NC

Search: Do republicans like NATO being an offensive organization?

#### The GOP despises NATO---empirics, Kremlin sympathy, and isolationism all prove

Saletan 22 – Saletan, William: “Putin Wants to Break NATO. Republicans Want to Help Him.” The Bulwark, 12 Apr. 2022, www.thebulwark.com/putin-wants-to-break-nato-republicans-want-to-help-him/. Accessed 24 June 2022.

Vladimir Putin’s central objective in Europe isn’t to capture Kyiv, the Donbas, or any other part of Ukraine. It’s to weaken the North Atlantic Treaty Organization, which protects most of the continent against him. And in that longstanding campaign, Putin scored two significant victories this week.

One was in France, where Marine Le Pen, a [Putin sympathizer](https://www.nytimes.com/2017/03/24/world/europe/marine-le-pen-of-france-meets-with-putin-in-moscow.html), finished a close second to Emmanuel Macron in Sunday’s French presidential election. Le Pen is running [almost even](https://www.reuters.com/world/europe/macron-faces-tough-fight-france-votes-sunday-2022-04-10/) with Macron in polls for the April 24 runoff. She has said that if she wins, she’ll [withdraw France](https://www.france24.com/en/france/20220304-ukraine-war-puts-france-s-nato-sceptic-presidential-candidates-in-a-tight-spot) from NATO’s command structure.

The other victory was in the United States, where 63 House Republicans, nearly a third of the GOP conference, voted [against a resolution of support](https://clerk.house.gov/evs/2022/roll115.xml) for NATO.

The House vote, taken on April 5, is a warning sign. Putin may be losing ground in Ukraine, but he’s gaining ground in the U.S. Congress. Three years ago, [22 House Republicans](https://clerk.house.gov/Votes/201944) voted against pro-NATO legislation. That number has nearly tripled.

The “Putin wing” of the House GOP—useful idiots such as Madison Cawthorn and Marjorie Taylor Greene, who [openly spout](https://www.wral.com/us-rep-madison-cawthorn-calls-zelensky-thug/20180199/) Russian [propaganda](https://twitter.com/RepMTG/status/1512126723164409867)—is only a tiny fraction of the Kremlin’s target audience in Congress. They’re joined by a larger crowd of Ukraine bashers, hardcore isolationists, and right-wingers who say we shouldn’t worry about anyone else’s borders until we “secure” our own. Together, that coalition adds up to [more than 20 lawmakers](https://www.thebulwark.com/whos-soft-on-russia-meet-the-republican-anti-ukraine-caucus/).

That’s a problem. But when you combine them with the NATO skeptics who voted against last week’s resolution—another 40 or so House Republicans who don’t trust alliances and who view Europeans as America’s rivals or adversaries—the problem gets a lot bigger.

The GOP’s turn against NATO is particularly worrisome because Congress has been warned, explicitly and repeatedly, about Putin’s goal of dissolving the alliance. In March 2017, after a U.S. intelligence report [confirmed](https://www.dni.gov/files/documents/ICA_2017_01.pdf) that Russia had interfered in the 2016 U.S. presidential election, the House Committee on Foreign Affairs—which was then, like the rest of Congress, under Republican control—held a hearing on this subject. The hearing was titled, “[Undermining Democratic Institutions and Splintering NATO: Russian Disinformation Aims](https://docs.house.gov/meetings/FA/FA00/20170309/105674/HHRG-115-FA00-Transcript-20170309.pdf).” Analysts and former officials explained to the committee how Russia had, in the words of one witness, persistently funded propaganda in the West to “fracture allied security, stoke public distrust against democratic institutions, and discredit the alliance structures that defend Europe.”

Over the next two years, other reports documented the same problem. The European Council on Foreign Relations noted Russia’s efforts to undermine support for NATO in [Finland, the Czech Republic, and other countries](https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe/). Foreign policy journals and articles in the American press noted [rising alarm](https://academic.oup.com/ia/article/93/2/251/2996077) in Europe at President Donald Trump’s threats to withdraw U.S. troops from the continent or to abandon the American commitment to defend NATO allies.

On January 14, 2019, the New York Times reported that “several times” in 2018, Trump had “[privately said he wanted to withdraw](https://www.nytimes.com/2019/01/14/us/politics/nato-president-trump.html)” from the alliance. The article said Trump had “told his top national security officials that he did not see the point of the military alliance, which he presented as a drain on the United States.”

A few days after the Times report, House Democrats filed and brought to the floor the [NATO Support Act](https://www.congress.gov/bill/116th-congress/house-bill/676), which [reaffirmed](https://www.congress.gov/bill/116th-congress/house-bill/676/text) that the U.S. was “solemnly committed to the North Atlantic Treaty Organization’s principle of collective defense as enumerated in Article 5.” The bill couldn’t completely bind Trump, but it expressed the sense of Congress that “the President shall not withdraw the United States from NATO” and that American policy was “to reject any efforts to withdraw the United States from NATO.” It also prohibited the use of federal funds “to take any action to withdraw the United States” from the alliance.

Every Democrat voted for the bill; 22 Republicans [voted against it](https://clerk.house.gov/Votes/201944).

One of the 22 Republicans, Rep. Scott Perry, explained why he and other self-styled hawks had voted no. In a [statement to constituents](https://www.facebook.com/permalink.php?story_fbid=2184564228306520&id=376801102416184), he complained that “the bill prevented the U.S. from ever leaving NATO . . . unless Congress first voted to repeal this would-be new law.” Perry wanted Trump to be free to pull America out of NATO, on his own.

Perry also argued that Trump should be free “to negotiate better terms for the United States in NATO,” as though the alliance were a trade deal. And he warned that “an ally of ours today may not be an ally tomorrow.”

That’s how Perry and [many](https://twitter.com/chiproytx/status/1088080295608365057) of his [colleagues](https://www.nwfdailynews.com/story/special/special-sections/2019/01/23/gaetz-explains-vote-on-nato-resolution/6218256007/) viewed the world. They saw alliances as entanglements and burdens. They worried that even friendly countries couldn’t be trusted. They believed that America should hedge its commitments because our allies might screw us.

And that was all Putin needed. He didn’t need American lawmakers to love him the way Trump did. He just needed them to constrain or withhold support from NATO.

Perry’s defection was a particularly good sign for Putin. The congressman wasn’t just an Iraq war veteran. He had also chaired part of the 2017 hearing on Russia’s strategy to undermine NATO. So he must have known he was doing what Putin wanted.

But he did it anyway, because he thought he was protecting America from Europe.

In the three years since that vote, Congress has seen even more evidence of Russia’s operations to sabotage NATO.

In April 2019, the Justice Department released the [Mueller report](https://www.justice.gov/archives/sco/file/1373816/download). It detailed how Russia had lobbied Trump campaign officials against NATO; how the Trump campaign, according to one of its own former co-chairs, had shifted away from “the NATO framework”; and how the Trump team had blocked Republican platform language that would have endorsed “providing lethal defensive weapons” to Ukraine.

In October 2019, the Senate Intelligence Committee released an analysis of [Russian propaganda techniques](https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf). The report showed how the Kremlin had sought to “drive wedges in the Western community alliances of all sorts, particularly NATO.” One of Russia’s tricks, the report noted, was “discouraging United States support” for accepting eastern European countries into NATO by portraying those countries as “free riders.”

In August 2020, the Senate committee issued a report that showed how Kremlin sympathizers had [lobbied the Trump campaign against NATO](https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf). The report found that in April 2016, then-New Jersey Gov. Chris Christie had advised Trump to affirm in a speech that “our commitment to our NATO allies in Eastern Europe is absolute” and that “we need to stand up to Russian aggression together.” The Trump campaign had rejected this language.

In September 2020, New York Times journalist Michael Schmidt reported that during Trump’s presidency, his then-chief of staff, John Kelly, had [struggled to stop Trump from pulling out](https://www.nytimes.com/2020/09/03/us/politics/trump-nato-withdraw.html) of NATO. In July 2021, Washington Post reporters Carol Leonnig and Philip Rucker revealed that Trump had told advisers he would [abandon the alliance in his second term](https://www.washingtonpost.com/politics/2021/07/13/book-excerpt-i-alone-can-fix-it/). And last month, Trump’s former national security adviser, John Bolton, told the Post that “[Putin was waiting](https://www.washingtonpost.com/politics/2022/03/04/bolton-says-trump-might-have-pulled-us-out-nato-if-he-had-been-reelected/)” for Trump to do just that.

After all these warnings, and after Putin’s latest invasion of Ukraine, one might have expected the congressional caucus of NATO critics to shrink.

Instead, it multiplied.

Why did so many Republicans vote against the latest pro-NATO resolution?

Some openly reject the alliance. “[NATO is a relic of the Cold War](https://twitter.com/RepThomasMassie/status/1511515988843499523),” said Rep. Thomas Massie. “Why should Americans pay for Europe’s defense?”

Others said the U.S. should be wary of overcommitment. “[We shouldn’t say that our support for NATO is unconditional](https://americasvoice.news/video/cQko2gFlWCIB3aZ/),” said Rep. Warren Davidson.

But others, including Perry, complained that the resolution threatened American sovereignty. In a video statement, Perry told his constituents that the resolution “politicizes NATO” by saying “[if you’re not supporting socialism, then we’re going to use NATO against you](https://www.facebook.com/repscottperry/videos/429791295614916).”

This is a bizarre misrepresentation. The resolution [affirmed](https://www.congress.gov/bill/117th-congress/house-resolution/831/text) that NATO was “founded on the principles of democracy, individual liberty, and the rule of law.” Those words are literally in [the alliance’s founding treaty](https://www.nato.int/cps/en/natolive/official_texts_17120.htm). The resolution also called for “unwavering support to the people of Ukraine.” And it endorsed a project, [jointly proposed](https://turner.house.gov/press-releases?ID=04A29990-6F5C-4465-BE92-6C6C7CF0E8C6) by [Democratic and Republican lawmakers](https://connolly.house.gov/news/documentsingle.aspx?DocumentID=4509), to build “NATO’s capacity to strengthen democratic institutions within NATO member, partner, and aspirant countries.”

To make sure nobody misconstrued that language as an attack on sovereignty, the resolution stipulated that any NATO monitoring of “challenges to democracy” within member states would be undertaken only “when requested.”

Perry ignored that stipulation and caricatured the resolution. So did several of his colleagues. Representative Chip Roy described the resolution as “[empowering international organizations to target the internal activities of sovereign nations](https://www.texastribune.org/2022/04/06/congress-nato-support-texas-representatives/).” Davidson described it as “[using NATO to try to undermine America’s sovereignty](https://americasvoice.news/video/cQko2gFlWCIB3aZ/).”

Some members who opposed the measure also expressed hostility toward Europe. Davidson said “global commitments” to accords on climate, banking, and other issues were forcing the U.S. to adopt the “inferior system” of “the Europeans.”

Roy fretted that NATO, empowered by the House resolution, would subject Americans to “[the leftist orthodoxy that now unfortunately permeates most of Western Europe](https://www.texastribune.org/2022/04/06/congress-nato-support-texas-representatives/).”

These lawmakers think they’re patriots. They think that by voting to limit NATO and America’s commitment to it, they’re protecting us. And that’s what makes their subversion of the alliance, from Putin’s point of view, so delicious.

It’s so much easier to serve evil when you think you’re doing good.

# OCOs Turn

### OCOs Bad

#### Trying to use OCOs for signaling causes miscalculation and nuke war

Erica **Longergan** **and** Keren **Yarhi-Milo** **22** (Lonergan is an assistant professor in the Army Cyber Institute at West Point and a research scholar at the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University; Yarhi-Milo is the Arnold A. Saltzman Professor of War and Peace Studies in the political science department and the School of International and Public Affairs, “Cyber Signaling and Nuclear Deterrence: Implications for the Ukraine Crisis,” War on the Rocks, 4/21/22, https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/)

So far, the Biden administration has attempted to dismiss Russia’s announcement as irresponsible saber-rattling. But as Putin continues issuing nuclear threats, **policymakers** are likely to **feel growing pressure to respond**. In particular, they may be tempted to **find ways** to signal to Russia **to deter the use of nuclear weapons**. One way this might be done is through cyber operations. In fact, some cyber experts are already calling for the United States to consider cyber attacks **for signaling purposes**. For example, writing in the Washington Post, Dmitri Alperovitch and Samuel Charap call on the Biden administration to consider a cyber “**shock-and-awe demonstration**” in response to a major Russian cyber attack against the West. They claim that such a response, which could include disrupting the Internet throughout Russia, would signal U.S. resolve and help prevent further **escalation** that they fear “**could result in nuclear war**.”

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.

The Limited Escalation Risks of Cyber Operations

But all of this focus on cyber operations causing nuclear escalation may be misplaced and, more importantly, distract policymakers from the dangers of a more plausible scenario: the use of ambiguous cyber signals during nuclear crises. Specifically, the nature of cyber operations reduces their inherent escalatory potential, particularly when compared to other ways a state could attack an adversary’s nuclear forces or command, control, and communications systems, like a direct counterforce strike or employing anti-satellite weapons. But their misuse as a signaling tool could do more harm than good.

First, successfully conducting cyber operations against strategic targets, like nuclear systems, is harder than the conventional wisdom might suggest. It requires a means of gaining access to a particular system and developing an exploit to cause a desired effect — and then maintaining persistent (and stealthy) access to be able to conduct an offensive operation at the desired time. Moreover, the overall outcome may be unpredictable and net less-than-desirable results.

Second, even if a state is able to conduct these kinds of operations, they typically prefer to do so in secret — and this mitigates some escalation concerns. That’s because, to cause an escalatory response, a state like Russia would have to uncover a cyber operation during a particular time period — such as while the Ukraine conflict is unfolding. For example, Russia would have to detect a cyber operation against a nuclear command and control system to cause Putin to perceive a “window of vulnerability,” perhaps assessing that it is part of a U.S. or NATO counterforce strategy to disable Russia’s ability to retaliate with nuclear weapons. But the likelihood of these circumstances arising is low because — unless a state is trying to signal with a cyber capability — it will try to keep these kinds of sensitive operations secret. Therefore, the chances of such an operation being discovered at a particular time period are relatively small.

Finally, even if, hypothetically, Russia was to discover a cyber operation taking place, the likelihood of it leading to escalation is low. This is due to the virtual nature of cyber “weapons” — they rarely cause destruction in the physical world, let alone permanent damage. For example, even Russia’s 2015 cyber attack against Ukraine’s power grid, an important example of a strategic cyber attack against civilian critical infrastructure, only resulted in service disruptions for a few hours. During the current conflict, Russia-linked actors have so far been stymied in using cyber operations for strategic impact, such as the failed cyber attack by the group Sandworm against Ukraine’s power grid.

Taken together, this reasoning suggests that, in practice, cyber operations may not rise to a level that would cause a state like Russia to actually fear the integrity of its nuclear command, control, and communications systems, creating few reasons to escalate to the level of nuclear employment.

Civil-Military Relations and the Risks of Cyber Signaling in Nuclear Crises

But what if a state, such as the United States, wanted a cyber operation to be visible to an adversary, such as Russia, during a nuclear crisis — in other words, to send a cyber signal?

Signaling is essential for coercive diplomacy and international crises because it helps states convey their intent to one another. The civil-military relations literature has found that **civilian** (rather than military) leaders are **more inclined to use military** **force as a form of signaling**, rather than for operational effect.

Why does this matter? When civilian and military leaders have different views, civilians could make decisions around using military force for signaling purposes in a way that exacerbates ongoing crises. For instance, writing about Cold War nuclear crises, Scott Sagan has shown that civilian decision-makers have made crises more dangerous by taking actions without fully understanding the military implications and risks of inadvertent escalation. Jack Levy, writing about the causes of World War I, discusses how, during the July Crisis preceding the outbreak of war, civilians saw military mobilization as a political tool for coercive diplomacy, whereas military leaders, who were focused on the operational implications, perceived mobilization as a means of preparing for imminent war.

Differences in how civilian and military leaders see the use of military power are likely to be even more salient in cyberspace, for three reasons. First, cyberspace is a highly technical environment where civilians typically lack subject matter expertise. Practitioners are likely to have far more up-to-date operational experience and, therefore, fluency with the technical issues and constraints posed by cyber operations than civilian leaders (even those with prior and, potentially, outmoded experience). Cyberspace is also a highly classified environment — one in which information is highly segmented and only accessible to a select group of individuals. Therefore, some civilian officials may not be privy to all of the details surrounding cyber operations. Finally, unlike other technical and secretive environments, cyberspace has an additional element that makes it even more difficult for non-experts to grasp its nature. Specifically, cyberspace is also an esoteric environment; cyber operations and their effects are not easily visible in a way that other types of military capabilities are, making it difficult to conceptualize their utility in a tangible manner.

There is evidence supporting this idea. For instance, senior civilian leaders across multiple U.S. administrations, as well as in Congress, typically describe cyber operations as useful for signaling deterrence and resolve. Chris Inglis, the Biden administration’s inaugural National Cyber Director, described how he’d “like to change the decision calculus of those who transgress in this space,” and contemplated that “[p]erhaps our actions should be felt by an adversary. They should know that they have just felt the hand of whomever.” Similarly, Senator Angus King, discussing the threat of Russian-linked ransomware attacks in the summer of 2021, noted that he wants “somebody … in the Politburo to say, ‘Gee, boss, I’m not sure we ought to do this because we’re liable to get whacked in some way by those Americans.’”

John **Bolton**, former national security advisor under President Donald Trump, in multiple public statements, has **depicted** the purpose of U.S. **cyber operations** — especially offensive ones — **as a means of influencing** adversary **perception**. He described how the employment of offensive cyber power creates “structures of deterrence, so that it’s publicly known,” and that “it is important that our adversaries know [that] …we have authorized offensive cyber operations to … demonstrate to our adversaries that the costs of engaging in operations against us is higher than they want to bear.” Michael Daniel, the Obama administration’s cyber czar, depicted the purpose of imposing costs on Russia in response to its 2016 election interference as “to openly **demonstrate** that we could do **it as a deterrent** and also clandestinely disrupt their operations as well.”

In contrast, while some military leaders do talk about cyber deterrence, the language they employ is anchored in tactical and operational objectives, rather than aiming to influence adversary perception and decision-making. This is evident in how both civilian and military leaders use the language of “imposing costs.” Military leaders tend to describe cost-imposition as supporting the disruption, degradation, denial, or destruction of adversary offensive capabilities and operations. For instance, in December 2021, Gen. Paul Nakasone, commander of U.S. Cyber Command and director of the National Security Agency (NSA), described “imposing costs” against Russian-linked ransomware groups as the goal in itself. The month prior, at the November 2021 Aspen Security Forum, he argued for the United States to impose costs in cyberspace, but stated that a traditional deterrence strategy “does not comport to cyberspace.” In another example, in 2019, Lt. Gen. Stephen Fogarty, commander of Army Cyber Command, voiced skepticism about cyber deterrence in remarks about defending the 2020 elections against cyber interference, noting that “I don’t know of a single thing we could do that would prevent [adversaries] from competing, but I want to impose as much cost on them as possible.”

Implications for the Ukraine Crisis and Beyond

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**.

The Biden administration has been commendable in clearly and consistently communicating to Russia, and other audiences, what the United States will not do in the Ukraine crisis — like sending American forces to Ukraine or establishing a no-fly zone. In addition, the administration should be equally clear about what is off the table in cyberspace — what Jacquelyn Schneider has termed a “strategic no-first-use” policy in cyberspace. Specifically, the **United States should** unequivocally **convey** to Russia **that it will refrain** from taking **actions in cyberspace** during this crisis that would undermine nuclear stability, such as conducting disruptive cyber-attacks against early warning satellites. This is different — the opposite, in fact — from drawing “red lines” in cyberspace, which are meant to deter unwanted behavior but can often backfire. Instead, the United States should communicate where it will exhibit restraint in cyber operations — a form of confidence-building. This could be conveyed publicly through statements by administration officials, similar to statements that Biden has made about other aspects of America’s role in Ukraine. It could also be privately communicated through ongoing backchannels taking place between U.S. allies, like France, and Russia.

There are also policy implications beyond the Ukraine conflict, especially in an environment in which the United States confronts potential future crises with other nuclear powers. In particular, senior national security officials have repeatedly emphasized that China represents a “pacing challenge” for the United States, including across the nuclear and cyber realms. In fact, Gen. Nakasone recently announced the creation of a China Outcomes Group under Cyber Command and the NSA. And researchers have identified how hypothetical crises involving the United States and China could escalate along dangerous trajectories, including to the use of nuclear weapons. The consequences of misunderstanding the utility of cyber signaling in this area are significant. Therefore, policymakers must consider how to improve civil-military coordination and cohesion so that the employment of military cyber power — especially when used against sensitive adversary systems, particularly nuclear ones, during delicate periods — is not out of sync with strategic objectives. The United States should also develop a more robust effort to clarify to adversaries, including China, how it will constrain its own behavior in cyberspace specifically during nuclear crises. The **potential implications of misperceptions surrounding cyber operations targeting nuclear systems during a future crisis with a nuclear-armed adversary are simply too significant.**

#### Exposure of offensive capabilities causes more cyberwar

Gil **Baram 18** (Gil Baram is the head of research at the Yuval Nee'man Workshop for Science, Technology and Security, and a research fellow at the Blavatnik Interdisciplinary Cyber Research Center. “The Theft and Reuse of Advanced Offensive Cyber Weapons Pose A Growing Threat,” 6/19/18, https://www.cfr.org/blog/theft-and-reuse-advanced-offensive-cyber-weapons-pose-growing-threat)

Almost exactly one year ago, the world experienced two destructive cyberattacks in which offensive **cyber tools** developed **by** the National Security Agency (**NSA**) **were stolen and shared with the public**. In May 2017, the **WannaCry** ransomware hit over 300,000 computers in 150 countries. One month later, the **NotPetya** attack hit the computer systems of companies and governmental entities across the globe causing millions of dollars in damages. These attacks **exploited numerous vulnerabilities**, and have subsequently **exposed the slow response time of targeted countries** and the lack of effective information sharing mechanisms between responsible agencies, something which could have mitigated the severe damage caused by the attacks.

The interesting feature of these attacks is that those responsible—**North Korea and Russia**—**used the leaked** offensive **tools** originally developed by the NSA. The investigation into WannaCry ultimately revealed that the attackers had exploited a security vulnerability called EternalBlue, originally developed by the NSA. NotPetya used a variant of the same vulnerability, which is still wreaking havoc a year later. For example, in February 2018, security researchers at Symantec reported that an Iran-based hacking group had used EternalBlue as part of its operations.

This situation whereby technologically-advanced countries are **investing** efforts **in** developing **offensive cyber capabilities** **only to have these very tools stolen and reused** raises three critical questions of urgent policy relevance.

First, are states going to start reusing each other’s leaked cyber tools as a matter of course? The ability to reuse stolen cyber tools may signal the beginning of a shift in the distribution of international cyber power, as weaker actors (including non-state actors) become increasingly able to use sophisticated malware to cause global damage and possibly target the cyber weapons’ original designers. Countries that are less technologically advanced and less vulnerable to cyberattacks might find the reuse of stolen vulnerabilities appealing for their own offensive activity.

Second, is it possible to prevent the leaking of cyber tools from occurring in the first place? There aren't many reasons to be optimistic. First, there’s the insider threat problem—a particularly thorny issue given the extensive use of contractors and the risk that they steal or mishandle sensitive information that they were exposed to during their service. A second and possibly more problematic reason is that it is cheaper to use stolen vulnerabilities than finding new ones. As new vulnerabilities like EternalBlue get exposed, the costs of using stolen cyber vulnerabilities and conducting attacks are being consistently lowered while benefits remain high. States with offensive capabilities know that putting their hands on unique vulnerabilities developed by their adversaries will **enable them to more easily launch sophisticated attacks** without the need pursue a lengthy and costly R&D process. This makes the **reuse of cyber tools especially appealing and may motivate different actors** to concentrate their efforts in this direction. As long as the benefits of using the stolen vulnerabilities are higher than the costs, these vulnerabilities will remain an attractive target.

A third question for policymakers is whether the theft and reuse of cyber vulnerabilities change the way states handle these vulnerabilities. States should be aware of the risk that vulnerabilities leak into the open and develop information-sharing mechanisms to address it. These information sharing mechanisms should exist between the intelligence agencies themselves and between the intelligence community and the tech industry. Once it has been recognized that a vulnerability, exploit or tool has been stolen, the relevant agency should immediately share the specific data with all the agencies and firms that might get affected by it, just like what the NSA is believed to have done. To minimize security concerns and to not expose sensitive sources and methods, there is no need to share the precise reasons for giving such warnings. Yet it is crucial to share this information in order to patch the vulnerabilities as soon as possible and lower future risks.

The U.S. government has its own vulnerabilities equities process (VEP) policy which sets out how the U.S. government discloses computer vulnerabilities it detects or acquires to other vendors. Countries across Europe have their own similar VEP mechanism, and an EU-wide VEP is being considered. But as so many countries around the globe are developing offensive cyber capabilities, and in light global damage costs of the WannaCry and NotPetya, there is an urgent need to create an international mechanism for vulnerability disclosures akin to a global VEP.

Formulating an effective response to **this growing type of cyber weapon proliferation** is clearly the responsibility of national governments. Quoting the words of Microsoft President Brad Smith: “The governments of the world […] need to take a different approach and adhere in cyberspace to the same rules applied to weapons in the physical world... This is one reason we called for a new 'Digital Geneva Convention' to govern these issues, including a new requirement for governments to report vulnerabilities to vendors, rather than stockpile, sell, or exploit them…” Alongside the development of these offensive capabilities, and in light of the success of recent attacks, **the theft and leak of offensive cyber weapons and their** subsequent **use is only likely to** **increase, potentially creating new international tensions** between governments and between them and the tech industry.

**\*\*article suggest intelligence sharing at the end -- XX**

#### OCOs perpetuate fear and suspicion – inadvertent escalation

**Valeriano** **and** **Jensen 19** (Brandon Valeriano is a senior fellow at the Cato Institute. He is also the Bren Chair of Military Innovation at the Marine Corps University and serves as senior adviser for the Cyber Solarium Commission. Benjamin Jensen holds a dual appointment as a Donald L. Bren Chair of Creative Problem Solving at Marine Corps University and as a Scholar-in-Residence at the American University, School of International Service. “The Myth of the Cyber Offense: The Case for Restraint,” 1/15/19, https://www.cato.org/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 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

### US OCO’s Bad

#### Increased US cyber operations provokes prolif of OCOs – destroys norms and incites adversaries

**Lin and Smeets 18** (Dr. Herb Lin is senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University. Max Smeets is a senior researcher at the Center for Security Studies (CSS) at ETH Zurich, director of the European Cyber Conflict Research Initiative, and author of “No Shortcuts: Why States Struggle to Develop a Military Cyber-Force”, published with Oxford University Press and Hurst in May 2022. “An Outcome-Based Analysis of U.S. Cyber Strategy of Persistence & Defend Forward,” November 28, 2018, https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward) //NB

One path towards escalation involves adversaries becoming more aggressive and conducting attacks that are highly disruptive to society—in other words, adversary activity leads to a less stable cyberspace. This could be the result of either an adversary’s increased willingness to conduct attacks using existing capacities or increased capacities of the adversary. Indeed, with respect to the latter, the U.S. vision—and associated changed course of action—may encourage other actors to grow their budgets to conduct offensive cyber operations. The proliferation literature on weapons of mass destruction has extensively covered the role of special interests in stimulating demand for weapon development. This makes it a strong possibility that the new U.S. vision can be used by those groups within a given country favoring a growing cyber command to justify and lobby for increased military spending.

A second possibility is that increased U.S. offensive cyber activity that operates below the threshold of armed attack activity reduces the value of cyber norms of behavior that support a more stable cyberspace. Even today, some observers believe that the high level of offensive activity in cyberspace today demonstrates quite forcefully that nations find value in conducting such activity, and that such activity points to the difficulty of establishing a more peaceful cyber norms regime. These observers argue that there is no reason to expect that increasing the U.S. contribution to such activity worldwide will make it easier to establish such a regime. Finally, a third possibility is that increased U.S. offensive cyber activity will complicate diplomatic relations with allies and other nations whose cyber infrastructures are used in support of such activity.

Increased aggressiveness by adversaries could also result from growing incentives to conduct offensive cyber operations of a highly disruptive nature. In this case, heightened aggressiveness might be a symptom of the U.S. strategy actually being effective in making the U.S. more powerful. Consider, for example, the current war against the Islamic State: losing territory and grip in the Middle East, the terrorist organization is said to be keen to recruit followers in Europe and other places in the world to conduct attacks outside of Iraq and Syria. These attempted mass killings are a way to show that the group still needs to be feared and potentially to help recruiting—but they do not change the balance of power in the region. Actors in cyberspace might become more noisy and aggressive purely to increase friction, gain attention and so on —and perhaps also to influence international public opinion in ways that drive the United States toward changing its strategy.

Finally, worst-case outcomes—that is, a United States that is less powerful in cyberspace along w,ith a less stable cyberspace—could stem from a multitude of sources. One possibility is that the United States could overplay its hand in terms of cyber capabilities. The USCYBERCOM is operating in a space in which it has to seize the initiative against a large and ever-growing number of actors. The dangers of fighting on multiple fronts—even for the most capable actors—are well known from conventional warfare. As the number of potential cyber “fronts” is much higher compared to conventional warfare, the risks of overextension have become much higher as well. The Defense Department vision’s explicit focus on Russia and China, following the USCYBERCOM vision’s silence on the issue of priorities, makes us less concerned about this scenario —though it is still a possibility.

### Nato OCO’s Bad

#### Addition of OCOs into frameworks like NATO risks misinterpretation and escalation

**Long 17** (Austin Long is a Research Scholar at the Arnold A. Saltzman Institute of War and Peace Studies and the Harriman Institute for Russian, Eurasian, and East European Studies at Columbia University. “A cyber SIOP? Operational considerations for strategic offensive cyber planning” in Journal of Cybersecurity, 18 February 2017, https://academic.oup.com/cybersecurity/article/3/1/19/3003367) //NB

For a cyber-equivalent to the SIOP (i.e. a plan for strategic OCO), planners need similar objectives. Deterrence is an obvious parallel objective between nuclear and cyber but deterrence of what? During the Cold War strategic nuclear forces were intended to deter both nuclear and conventional attacks, while more recently unclassified guidance “directs DOD to strengthen non-nuclear capabilities and reduce the role of nuclear weapons in deterring non-nuclear attacks” [17]. Are strategic OCO intended primarily to deter adversary OCO or are such operations part of a broader set of deterrent capabilities, including nuclear forces? The latter seems more likely but this is a policy choice different administrations may answer differently.

If deterrence fails, OCO planners need subsequent objectives. Here the parallel with nuclear operations, at least those from the Cold War context, may be less obvious. Is the next objective for strategic OCO the control of escalation? It could be but this might vary by adversary and scenario. Failure of deterrence regarding a great power like Russia or China might lead to a subsequent objective of escalation control but North Korea or Iran might be different, with the objective being the prompt neutralization of adversary strategic capabilities in order to limit (or eliminate) damage from enemy attack.

OCO could be a component of either objective, but would be planned very differently. For escalation control, planners would need to define targets that punish the adversary and/or deny objectives in order to demonstrate US resolve. Yet the targets would have to be of a nature unlikely to lead to further escalation by the adversary. The need to strike this balance – producing effects sufficient to show resolve without risking escalation – will be challenging to policymakers and planners alike. Inadvertent escalation was a major worry in the late Cold War with conventional and nuclear forces – a concern that is now returning in East Asia and potentially the eastern and southern flank of the North Atlantic Treaty Organization (NATO) [18–21]. The addition of OCO further compounds this problem by creating new pathways to inadvertent escalation.

A historical parallel to OCO and inadvertent escalation was the concern about the impact of electronic warfare (EW) in a conventional battle in Europe on Soviet early warning of a US strategic nuclear attack, particularly one directed at the Soviet strategic nuclear arsenal [18]. EW in this context was not intended to threaten Soviet strategic forces, but could nonetheless generate pressure for Soviet nuclear use as they became fearful their forces were vulnerable.

Soviet exercises reflected this fear. In a 1984 Soviet strategic exercise, US bombers exploited damage to Soviet air defense as well as the massive volume of electronic warfare to strike key Soviet command centers. This initial attack was promptly followed by a devastating attack on Soviet strategic nuclear forces [22]. Thus conventional air operations, including electronic warfare, in an actual war may have made the Soviets extremely concerned about the survival of their nuclear forces and thus potentially pressured them to use nuclear weapons first.

Strategic OCO could create similar fears, as attacks on even nonmilitarily critical systems (e.g. power supplies) could impact military capabilities or stoke fears that military networks had likewise been compromised. Indeed, OCO effects could be more escalatory than traditional electronic warfare, which even if it compromises air defense is nonetheless generally observable – radar operators will often know they are being jammed even if they can do nothing about it. OCO, if done well, could compromise systems without the target knowing. An adversary thus might not be able to distinguish between a system failure due to OCO and a natural system failure. In a crisis or conventional war, if some component of an adversary’s command and control failed it could easily be misinterpreted as successful OCO, creating escalatory pressures. Targeting strategic OCO for escalation control without risking inadvertent escalation may thus be a major planning challenge.

### Integration Bad

#### Integration of OCOs magnifies the risk of confliction among NATO members

Jeppe T **Jacobsen 21** (Jeppe T. Jacobsen is a Ph.D. candidate at the Danish Institute for International Studies and the Center for War Studies at the University of Southern Denmark. “Offensive Cyber Capabilities and State Violence: Three Logics of Integration,” 10/26/21

https://academic.oup.com/jogss/article/7/1/ogab028/6412386)

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.

#### [][[Sharing OCOs within NATO undermines cyber norms – increases risk of escalation

Jeppe T **Jacobsen 21** (Jeppe T. Jacobsen is a Ph.D. candidate at the Danish Institute for International Studies and the Center for War Studies at the University of Southern Denmark. “Offensive Cyber Capabilities and State Violence: Three Logics of Integration,” 10/26/21

https://academic.oup.com/jogss/article/7/1/ogab028/6412386)

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**.

Intelligence norm – shared assumption that cyberspace is for espionage – not for being aggressive – when you observe espionage means you do not escalate in an aggressive way

#### Relying on offense in cyberspace erodes cyber norms

Mariarosaria **Taddeo 19** (Fellow in Cyber Security and Ethics in the Department of Politics and International Studies at the University of Warwick and Research Associate at the Uehiro Centre for Practical Ethics, University of Oxford, UK, “Norms and Strategies for Stability in Cyberspace,” Chapter 3 in “The 2019 Yearbook of the Digital Ethics Lab,” edited by Christopher Burr and Silvia Milano, <https://link.springer.com/chapter/10.1007/978-3-030-29145-7_3>)

In this scenario, state actors make policy decisions to protect their abilities to launch cyber attacks. Strategic ambiguity is one of these decisions. According to this policy, states decide neither to define and nor inform the international community about their red lines—thresholds that once crossed would trigger state response—for non-kinetic cyber7 attacks (Mariarosaria Taddeo 2011). This approach leaves de facto unregulated cyber attacks that remain below the threshold of an armed attack.

Strategic ambiguity has often been presented as a way to confuse the opponents about the consequences of their cyber attacks. As the US National Intelligence Officer for Cyber Issues officer put it:

Currently most countries, including ours, don’t want to be incredibly specific about the red lines for two reasons: You don’t want to invite people to do anything they want below that red line thinking they’ll be able to do it with impunity, and secondly, you don’t want to back yourself into a strategic corner where you have to respond if they do something above that red line or else lose credibility in a geopolitical sense.7

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

The risks come with the cascade effect following the **absence of clear thresholds for cyber attacks**. The lack of thresholds **facilitates a proliferation of offensive strategies**. This, in turn, **favours an international cyber arms race** and the **weaponization of cyberspace**, which ultimately **spurs the escalation of cyber attacks**. This is why strategic ambiguity is a policy hazard that fuels, rather than arrest, escalation of interstate cyber attacks. Cyber attacks would be **deterred more effectively by a regime of international norms** **that makes attacks politically costly** to the point of being disadvantageous for the state actors who launch them.

### UQ -- Norms Strong Now

#### Clear Cyber norms shape cyberspace—created by public and private sector

Myriam Dunn Cavelty & Andreas Wenger 22, Myriam Dunn Cavelty is a Senior Lecturer for Security Studies and Deputy for Research and Teaching at the Center for Security Studies (CSS) at ETH Zurich. She studied International Relations, History, and International Law at the University of Zurich. She was a visiting fellow at the Watson Institute for International Studies, and Andreas Wenger is professor of International and Swiss Security Policy at ETH Zurich. He studied History, Political Science and German Literature at the University of Zurich. He holds a Doctorate from the University of Zurich and was a visiting fellow at the Woodrow Wilson School of Public and International Affairs and the Center of International Studies, Princeton University. “Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation,” 1st ed., Routledge, 01/18/2022, DOI.org (Crossref), doi:10.4324/9781003110224 https://library.oapen.org/bitstream/handle/20.500.12657/52574/9781000567113.pdf#page=201

Early internet pioneers, including John Perry Barlow, regarded cyberspace as a virtual environment not requiring formal rules or external controls (Barlow 1996). However, growing numbers of cyber security events affecting private as well as public information and communication technologies (ICTs) have undermined these non-interventionist positions. Over the course of the past two decades, voluntary norms of responsible behavior “have emerged along with confidence- and capacity-building measures as the principal policy tools of choice to meet the […] vision of an open, secure, accessible, and peaceful ICT environment” (Kavanagh 2017: 10).

Defined as shared expectations of appropriate behavior, norms can be of regulative (i.e. describing obligations, prohibitions and permissions) or constitutive (i.e. creating categories of actors and actions) nature (Finnemore and Sikkink 1998; Wiener 2017; Björkdahl 2002). “By shaping agents’ understandings of their social environments, associated interactions, and possible outcomes”, they foster coordination and predictability, and in turn reduce contextual ambiguities to manageable levels (Ferguson 2019: 1). In contrast to formal legal provisions, norms rely on softer means of enforcement and implementation.

According to Finnemore, the move to voluntary cyber security norms can partly be attributed to concerns about the suitability and effectiveness of binding treaties in fast-moving environments, as well as to fears of legal lock-in among leading cyber powers (Finnemore 2017: 3). Abbot and Snidal have argued that when circumstances are fundamentally uncertain, that is, when even the range and/or distribution of possible outcomes is unknown, [formal legal agreements] may not be desirable. In particular, if actors are ambiguity-averse, they will prefer to leave agreements imprecise rather than face the possibility of being caught in unfavorable commitments. (Abbott and Snidal 2000: 442) Despite perceived needs to reduce threats and corresponding levels of uncertainty, and more than two decades of concerted diplomatic efforts relating to the formulation of norms of responsible behavior for the digital domain, advancement has been slow and political compromise short-lived. In the wake of political contentions among governments surrounding debates about existing and emerging perils emanating from the digital realm and possible normative measures to address them, a number of non-state actors have stepped up and started to more actively make their voices heard (Grigsby 2017; Mačák 2017; Väljataga 2017).

International relations and international law literatures have taken note of the rise of private actors involved in global steering and rule-making processes, and have systematized and subsumed ideational efforts conducted by non-state actors under the umbrella of norm-entrepreneurship or soft-law, respectively (Finnemore and Sikkink 1998; Risse-Kappen, Ropp, and Sikkink 1999; Abbott and Snidal 2000). Norm entrepreneurs (or protagonists of soft-law instruments) challenge prevailing patterns of behavior, by suggesting normative ideas and mobilizing like-minded stakeholders or networks within and across states to endorse them (Sandholtz 2017: 2). “These alliances [then] bring pressure to bear from above (transnationally) and below (domestically)”, and help the standards proposed get more widely accepted (Sandholtz 2017: 2).

In order to reap the benefits of these fragmented processes, however, initiators need to deliberately plan for “complementarity” and “cross-pollination”. The next section summarizes leading norms-based efforts launched by Microsoft, Siemens, Telefónica, and Kaspersky Lab, and assesses the effectiveness of their activities along three dimensions: Output, outcome, and impact. Analyzing the effects of regulatory efforts has remained extremely challenging and has incited numerous scholarly debates. There are no unified approaches for assessing the success of norms or regimes. This chapter draws on the work conducted by Flohr et al. and Wolf who have proposed assessments along the dimensions mentioned above (Flohr et al. 2010; Wolf 2010). Only proposals with explicit normative nexus and only proposals launched post-2017 were selected for analysis.

Private cyber security norm development efforts

Non-state actors, in particular technology companies, have been key contributors to the development and expansion of cyberspace.4 As operators of network infrastructures, designers of products, and suppliers of services, they have made important contributions to the “international […] architecture for the governance of cyberspace” (Radu 2014: 4). In addition to producing hard- and software, they have come to contribute to the promotion of global cyber security norms and standards. So far, their normative contributions have received little academic attention. This chapter seeks to contribute to richer understandings of the normative parts played by technology companies and unveil the governing qualities of their activities by evaluating them across the dimensions of output, outcome, and impact.5

As key providers of ICTs, technology companies have strong incentives to pursue normative strategies to sustain their business models. Through the eyes of technology companies, norms provide useful tools for tackling contextual ambiguities and pre-empt costly changes to legal frameworks, or governmentled market interventions. While the reasons for corporate norm-shaping efforts pertaining to the virtual realm may primarily be grounded in commercial considerations, i.e. reducing costs and risks, securing their operations, gaining access to new markets/safeguarding existing customer bases, and strengthening corporate reputation and legitimacy, less self-serving reasons, i.e. upholding good-faithcommitments and values such as user privacy, should not be forgotten (Gorwa and Peez 2018). Not all of the activities undertaken by technology companies in the context of norms of responsible behavior for cyberspace can be explained by rationalist arguments.

Microsoft

One of the first corporate entities to engage in debates about responsible conduct in cyberspace was Microsoft (Microsoft Security Response Center 2010). Valued at over USD 1 trillion (2019), the company ranks among the four largest technology giants globally, the other three being Apple, Alphabet, and Amazon. Following prior norms-oriented ventures between 2013 and 2016, in February 2017, Microsoft President and Chief Legal Officer Brad Smith introduced the idea of a Digital Geneva Convention to Protect Cyberspace (Microsoft 2013; McKay et al. 2014; Charney et al. 2016; Smith 2017). Grounded in the belief that deeprooted collaboration among states, and between states, the private sector, and civil society is needed to curb nefarious doings in the digital realm, the convention as outlined by Smith, asks governments, among other things, to:

Refrain from attacking critical infrastructures (including civil and financial systems)

· Abstain from engaging in espionage · Engage in vulnerabilities disclosure processes

· Exercise restraint in developing cyber weapons and engaging in offensive activities, and

· Assist private sector entities in securing cyberspace. (Microsoft 2017)

It also calls on technology companies to behave as neutral actors and recommends the setting up of an independent non-governmental organization capable of investigating and publicly attributing (nation-state) cyberattacks (Smith 2017; Maurer and Taylor 2018). Met with little enthusiasm by governments, Microsoft’s call for a Digital Geneva Convention was succeeded by the unveiling of a Cybersecurity Tech Accord bringing together “global technology companies committed to protecting their customers and users”, 14 months later

In September 2018, Microsoft unveiled a Digital Peace Now campaign, which calls on citizens to protect cyberspace, e.g. through measures of cyber hygiene, and urges governments to refrain from endangering the global digital environment (Microsoft 2018). Only two months later, Microsoft co-sponsored the Paris Call for Trust and Security in Cyberspace. Introduced at the 12th Internet Governance Forum (IGF) in Paris, the Paris Call for Trust and Security in Cyberspace (short Paris Call) constitutes one of the most widely endorsed multi-stakeholder instruments pertaining to peace and security in the virtual realm to date (Ministère de l’Europe et des Affaires Étrangères 2018)

The Paris Call proposes the development of common principles for securing cyberspace through collaborative efforts across existing international platforms and mechanisms (Ministère de l’Europe et des Affaires Étrangères 2018). Although at first sight a French initiative, the Paris Call was vitally influenced by Microsoft, both in terms of origin and content. According to information presented by Le Monde and WIRED, it was Microsoft’s political lobbying that gave rise to the initiation of the Paris Call (Matsakis 2018a; Untersinger 2018). The Paris Call advances nine principles intended to resonate with both state and nonstate entities. Specifically, it asks supporters to:

Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure; • Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet; • Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities; • Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector; • Develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm; • Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain; Support efforts to strengthen an advanced cyber hygiene for all actors; • Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-state actors; • Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace. (Ministère de l’Europe et des Affaires Étrangères 2018)

Rather than reinventing the wheel in terms of normative prescriptions, the Paris Call constitutes an attempt at realigning scattered discussions and improving the complementarity of cyber security norm formation processes

While the Paris Call has seen fairly broad uptake among governments, private industry, the technical community, researchers, non-governmental organizations, and civil society, there have been a number of notable public abstentions, including the United States, Russia, China, Iran, and Israel (Matsakis 2018b).

#### UQ- Cyber norms internationally shape cyber policy

Erica Borghard et al. 22, Dr. Borghard holds a Ph.D. in political science from Columbia University, is a term member at the Council on Foreign Relations, and senior fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace. “Reviewing US Cyber Posture: An Analysis,” SSRN Electronic Journal, 2022, DOI.org (Crossref), doi:10.2139/ssrn.4077962

https://deliverypdf.ssrn.com/delivery.phpID=131074121084080064095101013088108093109023030014084091014024007126031069108084010090035056097013011097115067066028017082016123027020011005061088099086116110009080093061020081064111080021114113021023124100113002030083004089093110079087002018070092084073&EXT=pdf&INDEX=TRUE

Norms have played a large role in U.S. cyber strategies, dating back to the 2011 International Cyberspace Strategy. Norms, or a standard of appropriate behavior for actors with a given identity, often follow a lifecycle in which they first emerge, then receive enough acceptance to reach a tipping point for a norm cascade, and finally are internalized in behaviors. Norm emergence, the first stage of the lifecycle, advents with a norm entrepreneur who shepherds the idea and attempts to convince others to adopt it. These norms entrepreneurs play a critical role in framing the issues at hand. Struggles over framing have significant long-term consequences because the initial framing tends to be sticky and difficult to dislodge. This “stickiness” can create a first-mover advantage in struggles to frame new norms. Beyond framing, norm entrepreneurs often create organizational platforms from which they seek to promote and institutionalize norms.

Successful norm entrepreneurs diffuse their norm to a sufficient number of actors to create a “norm cascade” in which the norm is adopted across a plurality of pertinent actors. Scholars refer to this as the tipping or threshold point for significant norm adoption. Studies of norm adoption suggest that the critical mass usually occurs when one third of the relevant actors in the international system have adopted the norm. In some cases, some actors or states are so critical that a norm will not reach a tipping point without their endorsement. Therefore, identifying these critical actors as part of a norm diffusion strategy is essential to the successful development of the norm through the full lifecycle. The most mature norms are finally internalized so that they are taken for granted as appropriate and natural behaviors.

Not all norms complete the lifecycle, but some norms and norm entrepreneurs are more likely to succeed. Research has found that the norms that are most likely to be adopted are those that display the following three characteristics: specificity (clarify a definition); durability (length of time the norms have been in effect); and concordance (extent of acceptance).

During the Obama administration, the U.S. placed a strong emphasis on norm entrepreneurship in cyberspace. In a 2015 speech by then Secretary of State John Kerry, he articulated the United States’ vision for cyberspace norms, asserting that “the Internet should be open and accessible to everyone,” as well as “ interoperable, so it can connect seamlessly across international borders.” Kerry went on to detail that “people are entitled to the same rights of free expression online as they possess offline” and that the U.S. expected states to uphold these norms in cyberspace while deterring threats. Ultimately, Kerry argued that these norms of appropriate behavior in cyberspace would lead to economic growth, peace, and “a means for social empowerment that is also the most democratic form of public expression ever invented.”

Accordingly, the 2015 DoD cyber strategy called for the U.S. to “foster norms of responsible behavior to improve global strategic stability” and reiterated “The United States is committed to an open, secure, interoperable, and reliable Internet that enables prosperity, public safety, and the free flow of commerce and ideas.” While norms played a less central role in the 2018 DoD cyber strategy, the strategy continued to call for an open, free, and interoperable Internet.

Perhaps more notably for norm evolution, the 2018 strategy (and the 2018 Command Vision for Cyber Command) articulated a new implicit norm: that states could engage with each other in cyberspace, exchanging tit for tat responses in cyberspace, without escalating retaliation to the level of “armed conflict.” Specifically, the concept of persistent engagement relies on establishing acceptable forms of “agreed competition” between states in the cyber domain. The central premise is that, through a process of “tacit bargaining,” the U.S. can find consensus about acceptable behavior in cyberspace. What follows from this logic is that the cyber operations we observe states conducting should represent an “agreed competition” short of war—though this agreement may not be formally written down or accepted by states. Anything outside of the scope of this agreed competitive space should therefore be where interests diverge and where conflict can be anticipated.

But experts have raised the question of whether there are risks that how the DoD operates as part of defend forward and persistent engagement may be inadvertently undermining norms the U.S. seeks to promote. In particular, if agreed competition is constructed from tacit bargaining developed through iterative interactions over time, these agreements are only implied. There is a risk, therefore, that what the U.S. assumes is tacitly accepted by all parties is not, in fact, the case. A related concern is a lack of clarity about how confidence building measures (CBMs) could support the development of norms, particularly around promoting the stability of cyberspace. Unlike arms control regimes, CBMs are voluntary agreements that help promote transparency and clarity around cyber operations and intent. Explicitly linking CBM efforts with military cyber operations can not only promote stability, but also provide a mechanism for more explicit communication (especially with adversaries) about norms of appropriate behavior around offensive cyber operations.

Furthermore, the U.S. has agreed to international cyber norms through formal processes, such as the UN Group of Government Experts. To make meaningful progress on these, it is important to ensure that the words of the U.S. government match its deeds in cyberspace, to include how the DoD operates in and through the domain. Clarifying how the DoD restrains its own behavior and operates in a way that is consistent with the norms the U.S. seekstrying to promote will be essential for the diffusion of norms in the international system. In this sense, the DoD has the opportunity to act as a norm entrepreneur.

#### Established norms prevent large-scale attacks

David J. **Lonsdale 17** (David J. Lonsdale is a Senior Lecturer in War Studies at the School of Law and Politics at the University of Hull. “Warfighting for Cyber Deterrence: a Strategic and Moral Imperative,” 2/2/17, <https://link.springer.com/article/10.1007/s13347-017-0252-8#author-information>)

3.4 The Failure of Cyber Deterrence?

The potency of cyber deterrence is difficult to judge. This is partly because there exists no consensus on what constitutes an act of sufficient cyber aggression. Therefore, it is not entirely clear what is to be deterred. Where exactly the threshold for response should be will be discussed in section three of this paper. For now, we can state that **low-level** nuisance **attacks** are **a daily occurrence**. For example, U.S. military networks are probed and scanned millions of times each day (Work 2015, 1). Similarly, acts of cyber espionage are reasonably common. However, what is also evident is **the lack of major cyber attacks**. For a while, Stuxnet, Wiper, Shamoon and Bronze Soldier appeared to signal the rise of cyber attack as a potent new instrument of policy. However, **medium to large-scale attacks have** **essentially dried-up**. Indeed, reflecting the empirical evidence, and marking a shift in tone, in his September 2015 testimony to the Senate Armed Services Committee, Director of National Intelligence, James Clapper, talked down the possibility of an ‘electronic Pearl Harbor’. Instead, he focused on ongoing ‘low-to-moderate’ level threats (Clapper 2015, 2).

What does this all tell us? Is deterrence working? If one considers low-to-moderate threats as deterrable, then the answer would seem to be no. From this perspective, and according to some policy makers, deterrence is already failing. In a 2015 Senate Armed Services Committee Hearing, Chairman John McCain was scathing in his assessment: ‘Our adversaries view our response ... as timid and ineffectual. Put simply, the problem is a lack of deterrence. The administration has not demonstrated to our adversaries that the consequence of continued cyber attacks against us outweigh the benefit.’ (Takala 2015) However, if we take the view that **cyber deterrence should really concern itself only with large-scale attacks**, the **picture** **is** more **positive**. Indeed, Valeriano and Maness (2015) have identified **considerable levels of restraint in state cyber behaviour**. This could be due to a lack of confidence in the strategic utility of cyber attack. It may also reflect the **development of norms against aggressive forms of cyber** **behaviour** and the **efficacy of deterrence**. Indeed, **norms** increasingly **form part of ‘complex deterrence’**, within which military and non-military elements operate together. In cyberspace, although a settled understanding of universal rules of behaviour is still lacking, **norms appear to be crystalising around acceptable forms of intrusion** rather than a blanket non-use position (Stevens 2012, 25). This may explain the continuance of lowlevel probes whilst large attacks have trailed off.

#### NATO’s cyber policy is rooted in defensive actions – reluctance to discuss pre-emptive warfare within current cyber norms

**Saltzman 13** (Dr. Ilai Saltzman is the Israel Institute Visiting Assistant Professor of Israel Studies at the University of Maryland and previously served as a professor of government at Claremont McKenna College where he taught classes in International Relations, Israeli foreign and security policy as well as US foreign policy. “Cyber Posturing and the Offense-Defense Balance,” 11 March 2013, <https://www.tandfonline.com/doi/full/10.1080/13523260.2013.771031>) //NB

Both agencies represent a highly defensive reaction to NATO's security challenges involving cyber warfare. As the Bucharest summit declaration proclaimed, the official cyber policy ‘… emphasizes the need for NATO and nations 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’.109 Yet Russia's continued use of cyber warfare during the war in Georgia highlighted its escalatory nature and the possible negative implications on conventional military conflicts. In April 2009, as part of the Declaration on Alliance Security, NATO moved further to identify cyberattacks alongside terrorism and the proliferation of weapons of mass destruction (WMD) as the key global threats to member states and the international community.110

But the major breakthrough in NATO strategic thinking regarding cyber warfare, which went beyond the strictly technical aspect of network protection, occurred during mid 2010. A team of leading experts in matters of security, headed by former American Secretary of State Madeleine Albright, was asked to prepare a preliminary report to be used as a basis for NATO's new Strategic Concept. According to this report, entitled NATO 2020: Assured Security; Dynamic Engagement and submitted in May:

The next significant attack on the Alliance may well come down a fibre [sic] optic cable. Already, cyber attacks against NATO systems occur frequently, but most often below the threshold of political concern. However, the risk of a large-scale attack on NATO's command and control systems or energy grids could readily warrant consultations under Article 4 and could possibly lead to collective defence measures under Article 5. Effective cyber defence requires the means to prevent, detect, respond to, and recover from attacks.111

Still, the recommendations reflected the defensive posture that was already advocated and implemented thus far by NATO. Furthermore, and extremely relevant to the Alliance's strategic planners, the Albright Commission was reluctant to engage the question of whether cyberattacks against NATO member states would constitute a direct act of aggression that would trigger the collective security clause. Instead, it defined a rather ambiguous principle according to which such a decision must be made considering ‘… the nature, source, scope, and other aspects of the particular security challenge’.112 The same defensive reasoning can be observed in the ensuing final version of the Strategic Concept adopted at the Lisbon summit six months later. In the words of the document, NATO will:

develop further our ability to prevent, detect, defend against and recover from cyberattacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations.113

Yet again, the numerous references to cyber warfare as a security threat were extremely narrow to include at best espionage, hacking, or disruption and there was no discussion about the possibility to conduct pre-emptive or retaliatory cyber warfare.114 In fact, Stephane Abrial, commander of Allied Command Transformation (ACT) responsible for leading the Alliance's transformation of capabilities and forces, was against defining the Strategic Concept's notion of ‘in-depth cyberdefense’ as a ‘military-only, or even a military-centric, strategy’. Instead, Abrial focuses on NATO's ‘permanent mission [which] involves countering the daily attempts made by hackers to break into our systems, which are by necessity interconnected, making a weakness in one country's systems a weakness in all’.115 Other key NATO officials, including General Secretary Anders Fogh Rasmussen, continued to conceptualize cyber warfare in defensive terms, arguing that recent cyberattacks ‘… increased the urgency to strengthen cyber defences not only at NATO, but across the Alliance as a whole’. There is no public discourse involving NATO officials that suggests treating cyber capabilities as an offensive feature of the Alliance's cyber strategy. The most proactive proposal to date was the option to dispatch NATO's cyber Rapid Reaction Teams in order to assist member countries suffering from cyberattacks, or ‘incidents’ as Rasmussen calls them, should they ask for such assistance.116

It appears that NATO is focused on prevention of attacks on its institutional assets and member countries rather than initiating cyberattacks against others. As the American representative to the CCDCOE concluded, when it comes to NATO, its major contribution to cyber defence will probably involve eroding the ‘… hacker's greatest advantages – anonymity’.117 NATO's strategic thinking will continue to utilize its pooled capabilities in order to promote defensive solutions to cyber warfare of various kinds and it will continue to treat it as a threat rather than as an offensive feature to be proactively utilized.

### Aff -- Sharing Key

**\*\* this card is weird – not really about sharing OCOs but intelligence sharing in general – author critiques OCOs in general**

#### Intelligence sharing of OCOs key to

**Valeriano** **and** **Jensen 19** (Brandon Valeriano is a senior fellow at the Cato Institute. He is also the Bren Chair of Military Innovation at the Marine Corps University and serves as senior adviser for the Cyber Solarium Commission. Benjamin Jensen holds a dual appointment as a Donald L. Bren Chair of Creative Problem Solving at Marine Corps University and as a Scholar-in-Residence at the American University, School of International Service. “The Myth of the Cyber Offense: The Case for Restraint,” 1/15/19, https://www.cato.org/policy-analysis/myth-cyber-offense-case-restraint)

Intelligence Sharing and Coordination

There are also benefits to **sharing threat intelligence** with industry and **allies**. The United States operates a global security network that connects not just treaty allies but businesses and civil society actors.79 Any cyber strategy must embrace this fact as a **source of strength**, not a point of vulnerability. A greater number of actors identifying adversary cyber operations provides early warning indicators and reveals adversary capabilities.

To date, intelligence sharing associated with cyber operations has been prone to interagency debate and coordination challenges. There are organizational seams, such as the divide between the FBI and CIA before the September 11th terrorist attacks, that often limit intelligence sharing and create barriers to effective response within the federal government.80 This dilemma is compounded with respect to alliance partners and industry. States and many other organizations tend to stovepipe information and undermine effective coordination based on security risks. Yet, closing off information in a network limits responsiveness.

Rather than limit information sharing, the United States should reengage processes such as the Obama administration’s Vulnerabilities Equities Policy, which sought **disclosures** of newly discovered and unknown malware that might pose a global threat.81 **Sharing threat intelligence** is central to not just inter­agency coordination, but working **with partner states**, businesses, and civil society. In order to strengthen the defense of the network through depth, the United States will need to assume risk in sharing information, and hence lose some offensive options. This includes working with nontraditional actors, such as the white hat hacker community, which conducts probes in order to help strengthen networks from adversary attacks.82 It also implies sacrificing some espionage and offensive cyber options to ensure partners can patch their networks and update their defenses.

### Processing

#### Disclosing OCOs moots their efficiency and undermines any potential stability

**Borghard and Lonergan 18** (Dr. Erica D. Borghard is an Adjunct Research Scholar in the Saltzman Institute of War and Peace Studies and an Adjunct Associate Professor in the Department of Political Science at Columbia University. Shawn Longergan Shawn W. Lonergan is a Senior Advisor to the U.S. Cyberspace Solarium Commission. “Confidence Building Measures for the Cyber Domain,” Fall 2018, https://www.proquest.com/docview/2166950058/abstract/4B6C015E3058436BPQ/1?accountid=11091)

However, rather than solely observing defensive exercises, the spirit behind the exchange of observers in the Helsinki Final Act was to provide reassurance among potential adversaries regarding each other's offensive forces-in other words, those that could pose a threat to stability. However, **building offensive cyber operations** into existing defensive exercises **is fraught with difficulties**. Currently, cybersecurity exercises typically have a defensive focus and are used to identify both technical and procedural vulnerabilities on internal networks.58 For example, most exercises spearheaded by the United States typically do not showcase the units that would conduct offensive operations or their capabilities and, therefore, are not designed to signal confidence in the command and control and efficacy of their offensive cyber forces.

It is possible to incorporate offensive actions into existing defensive exercises. For instance, a state could build into a defensive scenario a counterstrike that targets an infected server commanding the attack. However, any **capability for access and attack** that would be used in the scenario would most likely be **limited to publicly available open source tools** or would be **fictionalized** so as not to give away to the adversary the **specific vulnerability** in the target system it would be exploiting. Again, this reflects the **fundamental requirement of secrecy** for operational success. The ephemeral nature of offensive cyber capabilities and accesses means that **revealing information** about them effectively **renders them moot**.59 If a state used real cyber weapons from its arsenal, it is likely that any observing state (including allies) would develop hardware and software upgrades to render the demonstrated capability inert. Similar to the paradox presented by cyber arms control, this may **undermine the very stability CBMs seek to create**. However, public notification of the successful execution of such an exercise could increase the adversary's confidence in the actor's ability to command and control cyber capabilities, thereby serving a confidence building purpose.

## Defense

### 2NC – No Follow-On

### 2NC – Allied Mistrust

#### Either allies won’t integrate OCOs due to political, cultural, and legal constraints OR they’ll feel pressured to which causes premature, faulty system development.

Black & Lynch, 20 – Research Leader Defence, Security and Infrastructure RAND Europe J=(James Black & Alice Lynch; "Cyber Threats to NATO from a Multi-Domain Perspective"; RAND; https://ccdcoe.org/uploads/2020/12/7-Cyber\_Threats\_NATO\_Multidomain\_Perspective\_ebook.pdf; 07-2020, Accessed 6-28-2022)//ILake-NoC

B. Policy Tensions

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). 138 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).

#### **No intra-NATO info-sharing – allies are reluctant to disclose info; they value autonomy and fear weaker countries cannot protect their info.**

University of Exeter 20 – public research university in Exeter, Devon, South West England, United Kingdom. Its predecessor institutions, St Luke's College “Should NATO Adopt a Joint Offensive Cyber Capability?” 09-2020, Accessed 06-28-2022, <https://socialsciences.exeter.ac.uk/media/universityofexeter/strategyandsecurityinstitute/pdfs/mstrat/James_Prideaux.pdf>. //ILake-NoC

Nevertheless, the largest barrier to a joint cyber capability is national intelligence agencies’ tendency to keep their activities in cyberspace highly classified.182 As Chapter 2 discussed, effective cyberattacks are utterly dependent on excellent intelligence.183 Members have significantly stepped up intelligence-sharing over the last two decades. They established the NATO Intelligence Fusion Centre in 2006, the Joint Intelligence, Surveillance and Reconnaissance initiative in 2012 and the Joint Intelligence and Security Division (JISD) in 2017. The JISD’s first Assistant Secretary General, Arndt Freytag von Loringhoven, says it has fostered a new culture of intelligence cooperation, increased efficiency and has helped avoid the duplication 37 of effort.184 Notably, he claims this new fusion of intelligence has ‘positioned the JISD to contend effectively with the… cyber… threats increasingly confronting NATO’.185

However, von Loringhoven’s optimism glosses over the great difficulty of intra-Alliance intelligence sharing. Divulging secret information is a trade-off between trusting a partner enough to share information that could endanger one’s own source against the benefits of doing so.186 Therefore, national agencies are reluctant to share it with international organisations, instead preferring bilateral cooperation on a case-by-case basis.187 It is shared between states with closely aligned interests, mutual trust and good diplomatic relations, as seen in the Anglo-American UKUSA Agreement.188 The exclusive ‘Five Eyes’ Alliance this evolved into is a rare example of multilateral intelligence sharing, involving NATO members America, Canada and the UK. These agreements tend to be more concerned with the security of the intelligence shared rather than its content, due to concerns over how other states will circulate the information. 189 Accordingly, wider intelligence cooperation within NATO would be much harder to achieve, primarily because many states do not share strong levels of trust, common interests and diplomatic relations with each other. For instance, France remains unsympathetic to intelligence integration in any multilateral environment, preferring strategic autonomy.190 This is compounded by an uneasy relationship with the Alliance, with President Emmanuel Macron calling it ‘brain dead’ in 2019.191 Furthermore, some allies fear that if countries with lower resilience are infiltrated, they could possibly compromise sensitive information shared between members.192 Consequently, apprehension about Italy’s weak cyber systems hinders allies’ propensity to share with Rome, since the potential for leaks undermines their trust.193

These concerns have resulted in a division between those member states that possess more advanced intelligence assets and those that do not. The former have been resisting serious intelligence integration, while the latter – including Belgium and The Netherlands – have even pressed for a CIA-style European agency.194 So far, NATO’s more powerful members have successfully repelled such initiatives. Following the 2015 Paris terror attacks, Belgian Prime Minister Charles Michel proclaimed the need for a ‘European CIA’.195 Nonetheless, German Interior Minister Thomas de Maizière shot this proposal down, claiming that ‘I cannot imagine we will be willing to give up our national sovereignty’.196

Unsurprisingly, NATO’s own collaborative efforts to date have also been heavily limited by national agencies’ desire for secrecy and autonomy. Pushback against greater transparency is especially strong on the part of the US, which owns a large share of NATO’s intelligence capabilities.197 not have access to all US intelligence, but NATO releasable information only.198 Such secrecy is a big practical obstacle to a joint offensive cyber capability. Although it is justified, elevating America’s role in Alliance cyber policy without increasing transparency would likely limit the tactical and strategic effectiveness of a combined offensive cyber capability.199 NATO’s intelligence fusion efforts have suffered from other, less important problems too. Different languages, cultures and infrastructures have proved to be structural constraints, while battlefield commanders have criticised the intelligence provided for lacking the strategic dimension.200 For instance, Lieutenant-General Mark Hertling judged NATO’s information on Islamic State too narrow and target-oriented, thus missing the bigger picture.201

Overall, the establishment of a joint capability would face some serious practical problems, both when confronting NATO’s internal politics and national intelligence agencies’ clandestine modus operandi. There would be significant legal hurdles to overcome too, which Chapter 4 discusses in more detail.

### 2NC – A/C – Mistrust

#### NATO is rife with mistrust and disunity – cooperation is structurally impossible.

Antonopoulos, '21 – independent geopolitical analyst (Paul Antonopoulos; "2021: A year of NATO disunity like no other"; BRICS; https://infobrics.org/post/34879/; 12-29-2021, Accessed 6-25-2022)//ILake-NoC

2021 is arguably the year when intra-NATO tensions and rivalry widened more so then ever since the alliance's inception in 1949. Although NATO most recently expanded its membership to include Montenegro in 2017 and North Macedonia in 2020, the rift caused by competing interests and the emboldening of revisionist ideologies (neo-Ottomanism and Anglo Chauvinism) among bloc members has only widened in recent years, but no other like 2021.

Intense NATO disunity first became prevalent during the Syrian War. Turkey continues to be enraged that the US, France and other member states train, fund and arm the People’s Protection Units (YPG), the Syrian branch of the Kurdistan Workers Party (PKK) that Ankara recognizes as a terrorist organization. Meanwhile, Washington is furious that Turkey defied warnings to not purchase the Russian-made S-400 missile defense system, and thus in December 2020 imposed sanctions on its fellow NATO member, an unprecedented action. With former US President Donald Trump unwilling to confront Turkey in a serious way in order to not jeopardize his personal business interests in the country, his successor Joe Biden has more willingly confronted his Turkish counterpart Recep Tayyip Erdoğan.

On Armenian Genocide Remembrance Day (April 24, 2021), Biden recognized the Turkish-perpetrated Armenian Genocide, something successive presidents refused to do out of fear of alienating a Turkey that was once seen as a bulwark against the Soviet Union/Russian Federation. Seeing as the previous non-recognition of the genocide was for political and geopolitical reasons, the recognition signifies a major change in Washington’s attitude towards Ankara.

Although Washington bemoans Ankara as being revisionist, its own contradictory revisionism actually caused a deeper disunity among NATO members in 2021 following the announcement of AUKUS, a trilateral Anglo security pact between Australia, the UK and the US. Under the pact, the US will share nuclear propulsion technology with Australia. This culminated in Canberra cancelling without notice the French–Australian submarine deal worth €56 billion, ending efforts for the two countries to develop a deeper strategic partnership.

The sudden cancellation of a lucrative contract and defense strategy with Australia was a humiliation for Paris as its ambitions for more global influence was dealt a blow. The French Ambassadors to Washington and Canberra were recalled to Paris, and Foreign Minister Jean-Yves Le Drian said “With Britain, there is no need. We know their constant opportunism.”

Washington pleaded to Paris that it had no knowledge that Canberra was about to “backstab”, as Le Drian termed it, their planned strategic alliance. The UK’s post-Brexit Anglo Chauvinistic ideology, something that Canberra naturally aligns with, motivated the humiliating manner in which France was sidelined to make way for AUKUS. This total disregard for French industry and strategic interests made Paris lose trust in NATO.

This “backstab” spurred on Paris to seek greater strategic alliances at a bilateral level, leading to a mutual defense pact that supersedes NATO with Greece. Greece is also frustrated with NATO as daily Turkish violations against its airspace, Turkish threats of a casus belli if it expands its maritime zone in the Aegean Sea to 12 nautical miles from its six (as permitted by international law), and Turkish attempts to exploit energy deposits in Greece’s maritime space, is met with indifference. In this way, Athens lost trust in NATO as a peace guarantor, something that made its pact with France a security necessity.

The Biden administration praised what Greek Prime Minister Kyriakos Mitsotakis termed as “strategic autonomy” from Washington, a minor concession likely to try and appease Paris as it lost its more lucrative agreement with Australia. However, Ankara continually berates the French-Greek pact, with Turkish Defense Minister Hulusi Akar saying that Greece’s alliance with France will cause cracks in NATO. On another occasion he said “[Greece is] trying to overpower Turkey with armaments and challenges, in cooperation with some other countries,” an indirect reference to France. Akar added: “[Greece] has different ambitions that it seeks to achieve through other alliances.”

There is clearly a major breakdown in NATO unity as accusations are being made between member states on who is responsible for causing cracks. This comes as the US continues to expect all member states to be compliant, as the UK retracts to Anglo Chauvinism under the guise of “Global Britain”, as France attempts to have more international influence, and as Turkey more aggressively pursues a neo-Ottoman policy.

2021 saw Greece and France lose trust in NATO, Turkey accuse Greece of causing disunity, the US angered as Turkey announces it wants to purchase another S-400 unit from Russia, and the formation of an Anglo bloc that seemingly supersedes NATO and French interests. Throw into this quagmire the massive disparity of interest among NATO members to support Ukraine against Russia, and it appears that the bloc is disunited like never before.

These events suggests that 2021 is a year where NATO’s fragility and disunity was more apparent than any other year, especially in the post-Cold War period. With these tensions, particular as the Anglo bloc and Turkey pursue revisionist policies and ideologies, disunity within NATO will not only continue into 2022, but intensify.

# Impact D- Cards

## No Russia cyberwars/hybrid

#### No Russia cyber war—regular deterrence stop them

Sue Gordon & Eric Rosenbach 22, Gordan is a Senior Fellow at the Harvard Kennedy School's Belfer Center for Science and International Affairs. She served as Principal Deputy Director of National Intelligence, after three decades at the CIA. Rosenbach is Co-Director of the Harvard Kennedy School's Belfer Center. He served as the Pentagon's Chief of Staff and as U.S. Assistant Secretary of Defense for Homeland Defense and Global Security. "America's Cyber-Reckoning: How to Fix a Failing Strategy" (2022) 101:1 Foreign Aff 10. https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/fora101&id=12&men\_tab=srchresults

A decade ago, the conventional wisdom held that the world was on the cusp of a new era of cyberconflict in which catastrophic computer-based attacks would wreak havoc on the physical world. News media warned of doomsday scenarios; officials in Washington publicly fretted about a "cyber-Pearl Harbor" that would take lives and destroy critical infrastructure. The most dire predictions, however, did not come to pass. The United States has not been struck by devastating cyberattacks with physical effects; it seems that even if U.S. adversaries wanted to carry out such assaults, traditional forms of deterrence would prevent them from acting.

Behind those mistaken warnings lay an assumption that the only alternative to cyberpeace must be cyberwar. But in the years since, it has become clear that like all realms of conflict, the domain of cyberspace is shaped not by a binary between war and peace but by a spectrum between those two poles-and most cyberattacks fall somewhere in that murky space. The obvious upside of this outcome is that the worst fears of death and destruction have not been realized. There is a downside, however: the complex nature of cyberconflict has made it more difficult for the United States to craft an effective cyberstrategy. And even if lives have not been lost and infrastructure has mostly been spared, it is hardly the case that cyberattacks have been harmless. U.S. adversaries have honed their cyberskills to inflict damage on U.S. national security, the American economy, and, most worrisome of all, American democracy. Meanwhile, Washington has struggled to move past its initial perception of the problem, clinging to outmoded ideas that have limited its responses. The United States has also demonstrated an unwillingness to consistently confront its adversaries in the cyber-realm and has suffered from serious self-inflicted wounds that have left it in a poor position to advance its national interests in cyberspace.

To do better, the United States must focus on the most pernicious threats of all: cyberattacks aimed at weakening societal trust, the underpinnings of democracy, and the functioning of a globalized economy. The Biden administration seems to recognize the need for a new approach. But to make significant progress, it will need to reform the country's cyberstrategy, starting with its most fundamental aspect: the way Washington understands the problem.

#### No impact to cyberwar- too expensive and difficult to be devastating

Maschmeyer Lennart & Dunn Cavelty Myriam 22, Lennart Maschmeyer is a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich and holds a PhD in Political Science from the University of Toronto and an M.Phil in International Relations from the University of Oxford. Myriam Dunn Cavelty is a Senior Lecturer for Security Studies and Deputy for Research and Teaching at the Center for Security Studies (CSS) at ETH Zurich , “Goodbye Cyberwar: Ukraine as Reality Check,” ETH Zurich, 05/2022, p. 4 p. https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP10-3\_2022-EN.pdf

Before Russia’s invasion of Ukraine, a series of experts predicted cyberwar: the massive use of Russian offensive cyber capabilities to “shock and awe” Ukraine’s defenses and undermine their will to fight. Some even suggested Russia need not invade because it could achieve the same outcomes by going to cyberwar. When that did not happen, the same experts predicted that Russia would still use offensive cyber capabilities sometime later – not only against Ukraine, but also against the West and its critical infrastructure as a punishment for its sanctions and support of Ukraine. Three months later, this has not happened either. Some experts are still expecting cyberwar to come, just sometime in the future. Others say that they were right, and cyberwar is here, except that the threat in Ukraine was deterred, or that attacks were launched but then neutralized in time. In contrast, we claim that experts who expect cyberwar to happen keep underestimating the practical limitations of cyberattacks (also called cyber effects operations) and consequently overestimating their strategic value – despite ample empirical evidence that cyberattacks are not very effective at coercive and destructive action. We aim to correct the distorted cyber threat debate by better grounding it in observable reality. While cyber operations remain important for intelligence operations and mildly disruptive attacks, destructive cyberattacks on key military or civilian infrastructure are challenging to implement and ineffective when compared to conventional attacks. The reason is an operational trilemma that constrains the speed, intensity, and control that cyber operations can achieve – thus limiting their strategic value and rendering catastrophic attacks highly improbable. Policymakers should focus on countering and mitigating actual threats, rather than on catastrophic scenarios that are theoretically possible, yet exceedingly unlikely in practice.

Expectations and Fallacies

Doom scenarios about devastating cyberattacks have plagued policy debates for 30 years and have proven to be stubbornly persistent. There are two interlinked problems that keep the specter

of cyberwar alive:

The first problem is the inflationary use of the term “cyberwar” for all politically motivated cyber operations. This glosses over important differences concerning the perpetrators, capabilities, and strategic effects. Every incident is read as a proof for rampant vulnerabilities of modern societies and as a harbinger of doom. In this view, cyberwar is already here.

Second, there is no consensus about the likelihood of a high-level, destructive cyberattack on civilian critical infrastructures – the expert definition of cyberwar. By pointing to society’s vulnerabilities and from there deducing the high likelihood of doom to come, many still expect it to be imminent. For them, cyberwar will come or is almost here.

Such predictions are guided by four fallacies that stem from ignoring interaction-effects between technology and politics:

The “vulnerability” fallacy: The assumption that when vulnerabilities exist, they will be exploited. In reality, the existence of a vulnerability does not reveal anything about why, how, and when

it would make sense for an adversary to exploit it.

The “the hack is the success” fallacy: The belief that the network intrusion, or hack, itself is proof of success. In reality, the success of any operation can only be determined by the political or strategic effects that are achieved through that operation.

The “cheap and easy” fallacy: The belief that cyber tools (software) are a low-risk “weapon” for the weak. In reality, controlled, targeted attacks suitable to reach strategic goals are not cheap and easy but hard, complicated, and risky.

The “just pull the trigger” fallacy: The belief that cyber tools work like conventional arms. In reality, cyber operations usually take months if not years to prepare and deliver. They are not something we can simply “launch” at a whim, and their use requires planning and integration into chains of command.

Technology constrains what is achievable politically, whereas politics constrains what will be attempted technologically. Russian cyberattacks, clearly attributed to the Russian government, in Ukraine since 2014 are an excellent example to demonstrate this both in a hybrid conflict setting and in an actual war.

#### No Russian Hybrid War-they know it isn’t effective

Maschmeyer Lennart & Dunn Cavelty Myriam 22, Lennart Maschmeyer is a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich and holds a PhD in Political Science from the University of Toronto and an M.Phil in International Relations from the University of Oxford. Myriam Dunn Cavelty is a Senior Lecturer for Security Studies and Deputy for Research and Teaching at the Center for Security Studies (CSS) at ETH Zurich , “Goodbye Cyberwar: Ukraine as Reality Check,” ETH Zurich, 05/2022, p. 4 p. https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP10-3\_2022-EN.pdf

Evidence from Ukraine, 2014–2022

Russia’s aggression against Ukraine since 2014 presents a useful case to examine the effects and strategic value of cyberattacks for at least three reasons. First, Russia is widely held to be one of the world’s foremost cyber powers with significant offensive capabilities. Second, from 2014 to 2022 Russia resorted to a strategy of low-intensity aggression enhanced by cyberattacks that many analysts have held to be the future of war. Significantly, such “hybrid war,” as it has since been christened, is supposed to be as effective as, if not more effective than, conventional war due to the effectiveness of cyberoperations. Third, Russia has used its cyber capabilities so frequently and in such varied contexts that some observers have described Ukraine as its “test lab for cyberwar.” Below we examine the sobering results.

Hybrid War (2014–2017). In this conflict phase,

Russia used five disruptive cyber operations against Ukraine (Table 1). These pursued election interference, critical infrastructure sabotage, and economic warfare. While some operations achieved observable effects, a sober look at evidence reveals the shortcomings of such operations. Cyber operations offer unique strategic advantages because they proceed in secret and exploit an adversary’s own computer systems to use them against the adversary. As such, they are primarily instruments of subversion rather than war. Yet exploitation involves a distinct set of challenges that create an operational trilemma among speed, effects intensity, and control over effects. Actors can only increase the effectiveness of one of these variables at the cost of losing out across the remaining ones.

This trilemma is clear across Russia’s cyber operations against Ukraine, as these operations were either too slow, too weak, or too volatile to produce strategic value.

Even the single exception, the NotPetya malware of 2017 that spread globally and caused massive economic damage, ultimately proved this limitation: Its wide spread was an accident – the hackers lost control over it.

Due to their shortcomings, these operations failed to contribute measurably towards Russia’s dual strategic objectives of changing Ukraine’s pro-Western foreign policy and undermining public support for this policy. Interestingly, Russia stopped attempting disruptive cyberattacks against Ukraine from 2017. Russia failed to achieve its core objectives through hybrid war. Ukraine maintained its pro-Western foreign policy despite continuing Russian aggression, including its annexation of Crimea and ongoing semi-covert warfare in the Donbas.

War (2022–). Hybrid war had failed, hence Russia changed strategy. In February 2022 it invaded Ukraine, commencing an actual large-scale war. While Russia amassed its troops along Ukraine’s border in the preceding months, many analysts predicted that if Russia would invade, it would also unleash cyberattacks of unprecedented destructiveness. As the conflict changed from low-intensity hybrid war to high-intensity conventional war, the theory went, so would cyberconflict.

As before, these expectations built more on theoretical possibilities than strategic realities and practical constraints. The essential point to consider here is that Russia had already tried and failed to achieve its objectives through cyber operations. Strategically, there was thus little reason to expect cyberwar to ramp up once Russia had made the choice in favor of conventional war.

Even if Russia did aim to cause greater destruction through cyber means, doing so requires significant planning, preparation, and resources – foremost, time. None of this was evident. Rather, we witnessed a string of rushed, haphazardly implemented, and outright botched cyberoperations (Table 2).

The operational trilemma predicts that the faster one operates, the lower the intensity of effects, and the greater the risk of control loss. Both constraints are in evidence. Most operations used “fast and easy” yet low-intensity effects like data wiping, website defacements, and DDoS attacks. More complex attacks failed or ran out of control. The attempt to cause a power blackout in April 2022 with the same malware as in 2016 stands out as a complete failure. Meanwhile, a disruption of the Viasat satellite communications network evidently aimed at cutting Ukrainian military communications failed to produce a measurable effect on these communications. Instead, it spread uncontrollably, causing significant collateral damage for the service’s other European customers, including thousands of wind turbines in Germany.

Overall, there is no evidence that any of the Russian-sponsored operations or, in fact, any of the operations related to this conflict (including the various hacktivist “armies” that have sprung up) measurably affected the course of the conflict, provided observable tactical advantages – such as sabotaging military equipment or disrupting enemy communications during battle – or produced strategic value.

Reality Check

The constraints posed by the operational trilemma render

cyberoperations relatively slow, ineffective, and unreliable.

These shortcomings limit their strategic value, both in hybrid and conventional conflict. Yet overestimation of their strategic potential continues, evident most recently in the dramatic warnings of impending cyberwar in Ukraine. These predictions both overestimated what cyber operations can achieve while underestimating Ukrainian defenses.

Due to the cyber-fallacies outlined above, experts continue to misrepresent the utility of cyberattacks, focusing on possibilities rather than considering their actual effects. Hence, in assessing the reports on cyberattacks it remains important to separate hype from reality.

Moreover, most analyses underestimated both the effects of victims’ learning – with Ukraine being targeted by Russian “cyber experimentation” for years – and the role of defensive measures. In particular, Ukraine’s collaboration with defensive cyber teams from abroad is a potential

## No impact to grid collapse

#### Alt causes to grid collapse- Indian cyber attacks

N. S. Sodha & M. L. Sachdeva 22, Cyber Physical Security of the Critical Infrastructure | SpringerLink, https://link.springer.com/chapter/10.1007/978-981-16-8727-3\_25 Accessed 24 June 22

Power Sector, a critical electrical infrastructure in India, is at risk due to increasing cyber incidences. The electrical infrastructure depends on electronic control systems for its operation which are Cyber physical IT systems. Cyber threats to system can take many forms e.g. failure of a system/element to act/react in designed way due to virus, software bugs, intrusion and congestion in the underlying/supervising system and it may lead the misguidance to the operating engineers and there by taking false decision in real time operation. Non availability of ICT systems is also a form of Cyber Security vulnerability. Cyber intrusions are costly to Power Sector and many are preventable following safe design and Cyber Security Standards. The effect of vulnerabilities in centralized systems e.g. SCADA/Automation etc. used in Transmission and Distribution sector is wider and has potential impact on the synchronous operation of entire Power System, leading to Grid collapse. As far as Distribution sector is concerned where bulk of Smart Grid activities are visible, the impact of compromise of a centralized SCADA/DMS can lead to disruption of services to critical customers like Hospitals, Metro Rail etc. which is critical for the units/Services involved but at the same time not global and widespread. The impact of cyber vulnerabilities is proportional to the criticality of the functions and systems being impacted. The paper details the Cyber threats and prevention techniques involving IoT sensors, communication protocols, cloud architecture and predictive data analytics.

## No impact to meltdowns

#### No impact to Meltdowns-even worse case scenario only causes health damages to plant employees

WNA 22, World Nuclear Association is the international organization that represents the global nuclear industry: including AEA, WANO, and the OECD-NEA. March 2022 Safety of Nuclear Reactors - World Nuclear Association, https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/safety-of-nuclear-power-reactors.aspx Accessed 25 June 22

A particular nuclear scenario was loss of cooling which resulted in melting of the nuclear reactor core, and this motivated studies on both the physical and chemical possibilities as well as the biological effects of any dispersed radioactivity. Those responsible for nuclear power technology in the West devoted extraordinary effort to ensuring that a meltdown of the reactor core would not take place, since it was assumed that a meltdown of the core would create a major public hazard, and if uncontained, a tragic accident with likely multiple fatalities. In avoiding such accidents the industry has been very successful. In the 60-year history of civil nuclear power generation, with over 18,500 cumulative reactor-years across 36 countries, there have been only three significant accidents at nuclear power plants:

Three Mile Island (USA 1979) where the reactor was severely damaged but radiation was contained and there were no adverse health or environmental consequences.

Chernobyl (Ukraine 1986) where the destruction of the reactor by steam explosion and fire killed two people initially plus a further 28 from radiation poisoning within three months, and had significant health and environmental consequences.

Fukushima Daiichi (Japan 2011) where three old reactors (together with a fourth) were written off after the effects of loss of cooling due to a huge tsunami were inadequately contained. There were no deaths or serious injuries due to radioactivity, though about 19,500 people were killed by the tsunami.

Of all the accidents and incidents, only the Chernobyl and Fukushima accidents resulted in radiation doses to the public greater than those resulting from the exposure to natural sources. The Fukushima accident resulted in some radiation exposure of workers at the plant, but not such as to threaten their health, unlike Chernobyl. Other incidents (and one 'accident') have been completely confined to the plant. Apart from Chernobyl, no nuclear workers or members of the public have ever died as a result of exposure to radiation due to a commercial nuclear reactor incident. Most of the serious radiological injuries and deaths that occur each year (2-4 deaths and many more exposures above regulatory limits) are the result of large uncontrolled radiation sources, such as abandoned medical or industrial equipment. (There have also been a number of accidents in experimental reactors and in one military plutonium-producing pile – at Windscale, UK, in 1957 – but none of these resulted in loss of life outside the actual plant, or long-term environmental contamination.) See also Table in Appendix 2: Serious Nuclear Reactor Accidents cumulative reactor years of operation experience nuclear plants It should be emphasised that a commercial-type power reactor simply cannot under any circumstances explode like a nuclear bomb – the fuel is not enriched beyond about 5%, and much higher enrichment is needed for explosives.The International Atomic Energy Agency (IAEA) was set up by the United Nations in 1957. One of its functions was to act as an auditor of world nuclear safety, and this role was increased greatly following the Chernobyl accident. It prescribes safety procedures and the reporting of even minor incidents. Its role has been strengthened since 1996 (see later section). Every country which operates nuclear power plants has a nuclear safety inspectorate and all of these work closely with the IAEA.While nuclear power plants are designed to be safe in their operation and safe in the event of any malfunction or accident, no industrial activity can be represented as entirely risk-free. Incidents and accidents may happen, and as in other industries, what is learned will lead to a progressive improvement in safety. Those improvements are both in new designs, and in upgrading of existing plants. The long-term operation (LTO) of established plants is achieved by significant investment in such upgrading.The safety of operating staff is a prime concern in nuclear plants. Radiation exposure is minimised by the use of remote handling equipment for many operations in the core of the reactor. Other controls include physical shielding and limiting the time workers spend in areas with significant radiation levels. These are supported by continuous monitoring of individual doses and of the work environment to ensure very low radiation exposure compared with other industries. The use of nuclear energy for electricity generation can be considered extremely safe. Every year several hundred people die in coal mines to provide this widely used fuel for electricity. There are also significant health and environmental effects arising from fossil fuel use. Contrary to popular belief, nuclear power saves lives by displacing fossil fuel from the electricity mix. Achieving safety: the reactor core Concerning possible accidents, up to the early 1970s, some extreme assumptions were made about the possible chain of consequences. These gave rise to a genre of dramatic fiction (e.g. The China Syndrome) in the public domain and also some solid conservative engineering including containment structures in the industry itself. Licensing regulations were framed accordingly. It was not until the late 1970s that detailed analyses and large-scale testing, followed by the 1979 meltdown of the Three Mile Island reactor, began to make clear that even the worst possible accident in a conventional western nuclear power plant or its fuel would not be likely to cause dramatic public harm. The industry still works hard to minimize the probability of a meltdown accident, but it is now clear that no-one need fear a potential public health catastrophe simply because a fuel meltdown happens. Fukushima Daiichi has made that clear, with a triple meltdown causing no fatalities or serious radiation doses to anyone, while over two hundred people continued working onsite to mitigate the accident's effects. The decades-long test and analysis programme showed that less radioactivity escapes from molten fuel than initially assumed, and that most of this radioactive material is not readily mobilized beyond the immediate internal structure. Thus, even if the containment structure that surrounds all modern nuclear plants were ruptured, as was the case with one of the Fukushima reactors, it is still very effective in preventing the escape of most radioactivity.

## No impact to warming

#### No climate impact---bad studies and adaption.

Nils P. Gleditsch 21, Research Professor at the Peace Research Institute Oslo, “This time is different! Or is it? NeoMalthusians and environmental optimists in the age of climate change,” Journal of Peace Research, pg. 5-6, 2021, SAGE. clarification denoted with brackets.

The most extreme contrarian position is, of course, to deny one or both key conclusions of the IPCC: the reality of global warming or the human contribution to it. However, most environmental optimists accept these two key conclusions but raise other problems with the panel’s discussion of the social effects of climate change and even more so with popular interpretations of the panel reports. For instance, Hausfather & Peters (2020), by no means ‘climate deniers’, decry the common use of choosing the high-risk [scenario] RCP8.59 to illustrate ‘business as usual’ as misleading.

The causal chains from climate change to the proposed effects on human beings are long and complex, and the uncertainty increases every step of the way. In the literature on the social effects of climate change, including the IPCC reports, statements abound that something ‘may’ lead to something else, or that a variable ‘is sensitive to’ another, without any guidelines for how to translate this into probabilities (Gleditsch & Nordås, 2014: 87f). Uncritical use of the precautionary principle, where any remotely possible calamity unwittingly becomes a probable event, is not helpful.

Gleditsch & Nordås (2014: 85) note that while AR5 (IPCC, 2014) did not find strong evidence for a direct link between climate change and conflict, it argued that climate change is likely to impact known conflict-inducing factors like poverty and inconsistent political institutions and therefore might have an indirect effect on conflict. But this assumes that correlations are transitive, which is not generally the case. If A correlates with B and B with C, we know nothing about how A relates to C unless both correlations are extremely high. The strongest case for the climate–conflict link is the effect of interaction between climate change and factors like poverty, state failure, or ethnic polarization. It may be more cost-effective to try to deal with these other risk factors than with global warming itself if the goal is to reduce the ‘risk multiplier’ effect of climate change on armed conflict.

The articles in this special issue do not generally see scarcity by itself as necessarily resulting in strongly negative outcomes. Factors like development, state failure, and previous overload on ecosystems continue to play an important role in that they interact with climate change to produce conflict and other social outcomes. For instance, Ide, Kristensen & Bartusevicˆius (2021) conclude that the impact of floods on political conflict are contingent on other factors such as population size and regime type. Moreover, most of the articles do not assume that scarcities are likely to arise at the global level. They may be regional (mostly in Africa), national, or local. Urban and rural areas may be affected by different scarcities. Climate change may also affect particularly strongly groups that are already at an economic or political disadvantage. The effects can be alleviated and adaptations constructed at these levels.

The argument about how climate change may indirectly impact conflict leans heavily on the negative economic consequences of climate change, but with little or no reference to the research that explicitly deals with this topic. In fact, the relevant chapter in AR5 concluded that for most sectors of the economy, the impact of climate change was likely to be dwarfed by other factors. Tol (2018) finds that the long-term global economic effects are likely to be negative, but that a century of climate change will have about the same impact on the economy as the loss of one year of economic growth. Other economists are more cautious, but the dean of climate change economics, William Nordhaus (2018: 345, 359), estimates that ‘damages are 2.1 percent of global income at 3C warming and 8.5 percent of income at 6C’, while also warning that the longer the delay in taking decisive action, the harsher the necessary countermeasures. Stern (2006) is more pessimistic, based mainly on a lower discount rate (the interest rate used to calculate the present value of future cash flows) as are Wagner & Weitzman (2015). Heal (2017) argues that the Integrated Assessment Models generally used in the assessment of the economics of climate change are not accurate enough to provide quantitative insights and should not be taken as serious forecasts. Yet, all these economists take the basically optimistic view that climate change is manageable with appropriate policies for raising the price on the emission of greenhouse gases. With a chapter heading from Wagner & Weitzman (2015: 17): ‘We can do this’.

This more optimistic assessment of climate change does not assume that the challenge will go away by itself or can be left to the market. A plausible approach, favored by most economists,10 is the imposition of a robust and increasing price on carbon emissions (whether as a carbon tax or through a cap and trade scheme) high enough to reduce the use of fossil fuels and encourage the search for their replacement. More than 25 countries had such taxes by early 2018 (Metcalf, 2019), but generally not at a level seen as necessary for limiting global warming to, say, 2C. This approach relies on the use of the market mechanism, but with targets fixed by public policy. Income from a carbon tax can be channeled back to the citizens to avoid increasing overall taxation. To speed up the transition, funds can also be allocated to the research and development of cheaper and more efficient production of various forms of fossil-free energy, including nuclear power (Goldstein & Qvist, 2019).

The response of the environmental optimists continues to emphasize the role of innovations; technological innovations, such as improvements in battery technology, the key element in the 2019 Nobel Prize in chemistry,11 but also social innovations, as exemplified by the experimental approach to the alleviation of poverty, rewarded in the same year by the Nobel Prize in economics.12

While the most important countermeasures will be directed at the mitigation of climate change, there is also a strong case for adaptation. If sea-level rise cannot be totally prevented, dikes and flood barriers will be cost-effective and necessary, at least in high-value urban areas. If parts of Africa suffer from drought, there will be increased use for new crops that are more suitable for a dry climate, possibly developed in part by GMO technology. Industrialization in Africa can decrease the one-sided reliance on rain-fed agriculture, as it has in other parts of the world, which have moved human resources from the primary sector to industry (and then to services). Continuing urbanization will move millions out of the most vulnerable communities (Collier, 2010). While structural change failed to produce economic growth in Latin America and Africa after 1990, Africa has experienced a turnaround in the new millennium (McMillan & Rodrik, 2014) and there are also potentials for increasing productivity by structural change within agriculture in Africa (McCullough, 2017).

## NATO bad/not key

#### NATO obsolete – causes more harm than good

Jacobs 2022 (Seth Jacobs is a history professor who studies the political and cultural history of the U.S. in the 20th century. His research focuses on the connection between U.S. domestic culture and foreign policy, “On NATO”, <https://www.bc.edu/content/bc-web/sites/bc-magazine/summer-2022/features/new-world-order-/on-nato.html> )//MargaretE

Three decades on, we are still stuck with the alliance, and as recent events demonstrate, it is no laughing matter. **NATO has become obsolete**. Indeed, Washington’s whole Europe-first orientation is anachronistic, a wasteful, expensive holdover from the cold war that ought to have been abandoned years ago and that distracts us from the true dangers we face abroad.

Mearsheimer, to his credit, deplored this development more vehemently than anyone. A self-described “unrepentant realist,” he had no patience for the aggressive internationalism that defined Western statecraft in the Clinton, Bush, and Obama presidencies. NATO as an anti-Soviet bloc made sense to him; NATO as an ever-expanding club of vaguely like-minded nations was foolish—and dangerous. According to the tenets of realism, when one great power trespasses upon another’s sphere of influence, the result is nearly always conflict, and Mearsheimer insisted that that was the case with NATO’s eastward march. It did not matter that officials from the United States and its European allies insisted that they had no designs on Russia. Russian President Vladimir Putin was not convinced. He perceived their encroachment as an existential threat and responded violently, first by annexing Crimea in 2014, then by invading Ukraine in 2022. While most pundits in the West denounced Putin’s barefaced breach of international law, Mearsheimer proclaimed that **NATO was to blame**, that its leaders ought to have recognized that their apparent intent to incorporate Russia’s bordering countries into their alliance would trigger war, and that Putin was only doing what an American president would do if, say, Iran built a military association and invited Mexico and Canada to join. In a gauntlet-flinging guest essay for the Economist in March and a follow-up interview in the New Yorker, Mearsheimer condemned NATO for naiveté and called for a pragmatic solution to the crisis that would keep Ukraine as a neutral country and leave Putin in power, with Crimea and the Donbas in his grasp.

I am not a realist, repentant or otherwise, and I have problems with Mearsheimer’s glibness and moral relativism. Nonetheless, I agree with him that **NATO no longer serves a coherent purpose**. The principal geopolitical challenge to U.S. primacy in the 21st century comes from China. That is where America’s focus should be. Russia might still qualify as a great power in terms of boots on the ground, but its economy is one-dimensional and shot through with corruption, its population shrinking and aging, its weapons and equipment outmoded, and its troops demoralized. By no stretch of the imagination could it overrun Europe as the old Soviet Union once seemed capable of doing. Britain and France have nuclear weapons. They do not need the United States to defend them. Why, then, does Washington continue to station forces in Europe and bear most of the cost of this transatlantic military partnership?

Institutional factors play a role, of course—NATO employs many bureaucrats who have a stake in its preservation, and no business dissolves itself voluntarily—but the main reason, in my opinion, is that Americans have yet to outgrow the delusions that prevailed in what neoconservative columnist Charles Krauthammer called the “unipolar moment,” that heady time after the cold war ended and no one appeared to threaten the security of the United States. Flush with victory, Washington policymakers believed that they could use this period of unprecedented economic, military, diplomatic, and geopolitical supremacy to remake the world in the American image, and they thought NATO was the perfect vehicle for accomplishing this goal on the Eurasian landmass. Thus they changed NATO’s original mandate and set about trying to foster liberal democracies in new member states like Hungary, Estonia, Bulgaria, and Slovakia. (Of course, the War on Terror saw this pattern extended to the greater Middle East, as the George W. Bush administration sought to democratize Afghanistan and Iraq.) A widely held assumption was that increasing the number of liberal democracies would make war less likely, since democracies do not fight one another. NATO aggrandizement would therefore create a broad zone of peace from the Elbe River to the gates of Russia, and perhaps beyond.

Events have not played out in that fashion. Far from nourishing democracy, NATO has seen the rise of far-right nationalist political movements in four of its oldest and most powerful members—Britain, Germany, France, and the United States—while Viktor Orbán’s second term as Hungarian prime minister witnessed an erosion of press freedom, a decrease in judicial independence, and Hungary’s descent by eleven places on the Democracy Index. Similar democratic backsliding has characterized Recep Tayyip Erdoğan’s Turkey and Jaroslaw Kaczynski’s Poland. As for being a force for peace, the carnage in Ukraine serves as eloquent testimony to NATO’s failure in this regard. Mearsheimer’s diagnosis of the origins of the conflict may be wrong—Putin might have tried to integrate neighboring nations into a greater Russia regardless of Western actions—but NATO did nothing to halt his aggression. And, of course, there is the perennial free-riding problem, with America’s allies counting on Washington to protect them even if their economies are robust enough to pay for their own defense. Moving NATO eastward has increased the number of countries America is obliged to safeguard at a time when a COVID-induced recession makes such commitments unaffordable.

Clearly, NATO has outlived its usefulness to the United States**. The Biden administration should disengage from the alliance as soon as practicable.** This can be done diplomatically, with some face-saving rhetoric and assurances that the departure of U.S. troops will not adversely affect Euro-American investment or trade. We could also remind nations like Spain and Turkey that they remain free to arm themselves to the teeth with American-made weapons—provided, of course, that they foot the bill. Then Washington should recalibrate its grand strategy to conform to the changed global balance of power.

#### NATO cooperation worsens deterrence and provokes Russia war

Carpenter 2022 (Ted Galen Carpenter is senior fellow for defense and foreign policy studies at the Cato Institute. Carpenter served as Cato’s director of foreign policy studies from 1986 to 1995 and as vice president for defense and foreign policy studies from 1995 to 2011, “NATO Security Dependents Are Not Useful Allies”, <https://www.cato.org/commentary/nato-security-dependents-are-not-useful-allies> )//MargaretE

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.

# T-Cybersecurity

## 1NC – Defensive

### 1NC Topicality – “Cybersecurity”

#### Cybersecurity is defensive – tactics that protect systems in the securer’s possession. NOT attacks on other systems.

**Ricoh USA. (n.d.).** *What is cybersecurity?* What is Cyber Security? | Definition, Types. How It Works. Retrieved June 24, 2022, from <https://www.ricoh> usa.com/en/insights/articles/an-intro-to-cybersecurity //kinsey

Cybersecurity is the act of implementing sophisticated layers of network defense and firewalls to protect critical systems and sensitive information against threats from digital attacks. The reality is that the types and severity of cybercrime are constantly evolving and multiplying. There are malware attacks such as viruses that attempt to destroy data. Ransomware is a particularly nasty type that locks down systems and threatens to erase data unless a ransom is paid. Phishing scams try to trick unsuspecting end users into giving up sensitive personal information such as social security (SSI) and credit card numbers to sell on the dark web. There are Distributed denial-of-service (DDoS) attacks that overwhelm a website with traffic. Man-in-the-Middle attacks involve hackers trying to intercept messages between two parties to steal company data. And not all threats are external. Current or former employees with a grudge and intimate network knowledge can wreak havoc on a business from behind the firewall. Companies must be on the lookout for cybercrime from all directions. Cybersecurity solutions, therefore, are applications, measures, and devices that constantly monitor network traffic for suspicious activity. Upon detecting a threat, it isolates and quarantines affected files and devices, and immediately alerts IT staff as to the exact location and proper response to the breach, limiting its impact and assisting with recovery. Cybersecurity management includes physical controls, procedural controls, technical controls, and compliance controls. There are tools that search for signs of stolen credentials on the dark web, and silicon-based boot processes to validate servers have not been compromised in Zero-trust environments. Maintaining cybersecurity in a constantly evolving threat environment is a never ending challenge, and one that usually requires outside expertise.

#### OCO’s are attacks not protection – inherently offensive.

**Aftergood ’14** Aftergood, Steven, directed the [FAS Project on Government Secrecy](https://fas.org/issues/government-secrecy/) from 1991-2021 and  was the plaintiff in a Freedom of Information Act lawsuit against the Central Intelligence Agency which led to the declassification and publication of the total intelligence budget for the first time in fifty years “Offensive Cyber Operations in US Military Doctrine.” Federation Of American Scientists, FAS, 22 Oct. 2014, https://fas.org/blogs/secrecy/2014/10/offensive-cyber/. //kinsey

A newly disclosed Department of Defense doctrinal [publication](https://fas.org/irp/doddir/dod/jp3_12r.pdf) acknowledges the reality of offensive cyberspace operations, and provides a military perspective on their utility and their hazards. Attacks in cyberspace can be used “to degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time.” Or they can be used “to control or change the adversary’s information, information systems, and/or networks in a manner that supports the commander’s objectives.” However, any offensive cyber operations (OCO) must be predicated on “careful consideration of projected effects” and “appropriate consideration of nonmilitary factors such as foreign policy implications.” “The growing reliance on cyberspace around the globe requires carefully controlling OCO, requiring national level approval,” according to the newly disclosed [Cyberspace Operations](https://fas.org/irp/doddir/dod/jp3_12r.pdf), Joint Publication 3-12(R). That publication was first issued by the Joint Chiefs of Staff as a SECRET document in February 2013 (as JP 3-12, without the R). But this week it was reissued as a public document. It is unclear whether the public document has been redacted or modified for release. The discussion of “offensive cyberspace operations” in the original, classified version of JP 3-12 led to adoption of that term in the official DoD lexicon for the first time in [March 2013](https://fas.org/irp/doddir/dod/jp1_02-march-2013.pdf), where it has remained through [the latest edition](https://fas.org/irp/doddir/dod/jp1_02.pdf). Offensive cyberspace operations (OCO) are “intended to project power by the application of force in and through cyberspace. OCO will be authorized like offensive operations in the physical domains, via an execute order (EXORD).” The [DoD document](https://fas.org/irp/doddir/dod/jp3_12r.pdf) is fairly candid about the challenges and limitations of cyberspace operations. “Activities in cyberspace by a sophisticated adversary may be difficult to detect” and to attribute to their source. Yet such detection and attribution capabilities are “critical” for enabling offensive and defensive cyberspace operations. By the same token, “first-order effects of [US cyberspace operations] are often subtle, and assessment of second- and third-order effects can be difficult,” requiring “significant intelligence capabilities and collection efforts” to evaluate.

#### Violation: Integrating OCO’s is offensive, not defensive, cooperation, meaning it is outside the realm of cybersecurity.

#### Vote negative to preserve predictable limits and negative ground.

#### 

#### Constraining the topic creates a stable mechanism for both teams that accesses a timely but manageable literature base and guarantees predictable neg ground.

#### 

#### Including offensive security mechanisms encourages small cases that ignore the core controversy of the impact of NATO security cooperation and dodge neg generics because the aff impacts will always be more timely/probable.

#### 

#### This impact turns aff flexibility — unlimited topics structurally discourage in-depth clash, decreasing cumulative, season-long content mastery and skill development which are voters for education.

#### 

## 2NC

### Ext-Interpretation

#### Cybersecurity is defensive, involves protection of systems in the securer’s possession. NOT attacks on other systems.

Merriam-Webster n/d “Cybersecurity Definition,” Merriam Webster, <https://www.merriam-webster.com/dictionary/cybersecurity>. Accessed 6/24/22 //kinsey

Definition of cybersecurity **:** measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

Examples of cybersecurity in a Sentence:

Recent Examples on the WebBy working together on cybersecurity, the EU and U.S. aim to help countries that otherwise might be eager to accept funding from China, an EU official said.— Catherine Stupp, WSJ, 15 June 2022. These entities can govern from within, setting their own goals and priorities for cybersecurity based on experience and real-world applications of technologies.— Ryan Moody, Forbes, 13 June 2022Levine and Republican cybersecurity equipment manufacturer Robert Howell are virtually tied for the runner-up spot, at around 17%— Los Angeles Times, 13 June 2022

#### Prefer it:

Broader interpretations explode the topic —utilizing an inprecise definition without intention to exclude destroys conceptual coherence and creates an unmanageable research burden. The case list under their interpretation would be enormous.

**Turns their offense—limits are vital to creativity and innovation**

David **Intrator** (President of The Creative Organization) October 21, **2010** “Thinking Inside the Box,” http://www.trainingmag.com/article/thinking-inside-box  //kinsey

One of the most pernicious myths about creativity, one that seriously inhibits creative thinking and innovation, is the belief that one needs to “think outside the box.”  As someone who has worked for decades as a professional creative, nothing could be further from the truth. This a is view shared by the vast majority of creatives, expressed famously by the modernist designer Charles Eames when he wrote, “Design depends largely upon constraints.”  The myth of thinking outside the box stems from a fundamental misconception of what creativity is, and what it’s not.  In the popular imagination, creativity is something weird and wacky. The creative process is magical, or divinely inspired.  But, in fact, creativity is not about divine inspiration or magic. It’s about problem-solving, and by definition a problem is a constraint, a limit, a box. One of the best illustrations of this is the work of photographers. They create by excluding the great mass what’s before them, choosing a small frame in which to work. Within that tiny frame, literally a box, they uncover relationships and establish priorities. What makes creative problem-solving uniquely challenging is that you, as the creator, are the one defining the problem. You’re the one choosing the frame. And you alone determine what’s an effective solution. This can be quite demanding, both intellectually and emotionally. Intellectually, you are required to **establish limits**, set priorities, and cull patterns and relationships from a great deal of material, much of it fragmentary. More often than not, this is the material you generated during brainstorming sessions. At the end of these sessions, you’re usually left with a big mess of ideas, half-ideas, vague notions, and the like. Now, chances are you’ve had a great time making your mess. You might have gone off-site, enjoyed a “brainstorming camp,” played a number of warm-up games. You feel artistic and empowered. But to be truly creative, you have to clean up your mess, organizing those fragments into something real, something useful, something that actually works. That’s the hard part. It takes a lot of energy, time, and willpower to make sense of the mess you’ve just generated. It also can be emotionally difficult. You’ll need to throw out many ideas you originally thought were great, ideas you’ve become attached to, because they simply don’t fit into the rules you’re creating as you build your box.

**The entire game breaks down if we can’t agree on what to debate about – the topic committee is the comparatively best mechanism for establishing agreement about what all debates should revolve around, like whether the USFG should restrict Trump or not**

**Shively 00** (Ruth Lessl, Assistant Prof Political Science – Texas A&M U., Partisan Politics and Political Theory, p. 181-182)

The requirements given thus far are primarily negative. The ambiguists must say "no" to-they must reject and limit-some ideas and actions. In what follows, we will also find that they must say "yes" to some things. In particular, they must say "yes" to the idea of rational persuasion. This means, first, that they must recognize the role of agreement in political contest, or the basic accord that is necessary to discord. The mistake that the ambiguists make here is a common one. The mistake is in thinking that agreement marks the end of contest-that consensus kills debate. But this is true only if the agreement is perfect-if there is nothing at all left to question or contest. In most cases, however, our agreements are highly imperfect. We agree on some matters but not on others, on generalities but not on specifics, on principles but not on their applications, and so on. And this kind of limited agreement is the *starting* condition of contest and debate. As John Courtney Murray writes: We hold certain truths; therefore we can argue about them. It seems to have been one of the corruptions of intelligence by positivism to assume that argument ends when agreement is reached. In a basic sense, the reverse is true. There can be no argument except on the premise, and within a context, of agreement. (Murray 1960, 10) In other words, we cannot argue about something if we are not communicating: if we cannot agree on the topic and terms of argument or if we have utterly different ideas about what counts as evidence or good argument. At the very least, we must agree about what it is that is being debated before we can debate it. For instance, one cannot have an argument about euthanasia with someone who thinks euthanasia is a musical group. One cannot successfully stage a sit-in if one's target audience simply thinks everyone is resting or if those doing the sitting have no complaints. Nor can one demonstrate resistance to a policy if no one knows that it is a policy. In other words, contest is meaningless if there is a lack of agreement or communication about what is being contested. Resisters, demonstrators,and debaters must have some shared ideas about the subject and/or the terms of their disagreements. The participants and the target of a sit-in must share an understanding of the complaint at hand. And a demonstrator's audience must know what is being resisted. In short, the contesting of an idea presumes some agreement about what that idea is and how one might go about intelligibly contesting it. In other words, contestation rests on some basic agreement or harmony.

### A2 C/I:Cyber Sec = Sec of Cyberspace

#### Both the Barret and Jaihan cards flow aff.

#### While cybersecurity can have many definitions, in the context of public policy it means protection of infrastructure, data, and users. OCO’s are not part of that list.

**Jaikaran 20** – Analyst in Cybersecurity Policy

Chris Jaikaran, "Cybersecurity: A Primer," Congressional Research Service, 12-15-2020, <https://www.everycrsreport.com/files/2020-12-15_IF10559_1d7e5206bb579bce86b7889e28a8ae293466a517.pdf> //kinsey

The Nature of Cybersecurity

The term “cyber” is frequently attached to a variety of security issues, underscoring that issues surrounding the management of cyberspace and its security are big and complicated.

As an example, consider a single smartphone. An American company may have designed the device, but the device may be built by a different company abroad using material from yet another country. The phone runs on software built by one company but modern operating systems borrow code from other companies and developers. Once a user has the device it will likely be connected to a variety of networks such as a home wireless network, a corporate network, and a cellular network. Each of these networks has its own infrastructure, but also share common internet infrastructure. The user will also install applications that contain code and use infrastructure by yet other myriad companies. Imagining users at the center, one can see large and intricate systems on one side and the other to create these devices and ensure those devices work.

To highlight how complicated it is, consider that the federal government does not have a single definition of cyberspace or cybersecurity. Recently, the Cyberspace Solarium Commission—defined “cyber” as

Relating to, involving, or characteristic of computers, computer networks, information and communications technology (ICT), virtual systems, or computer-enabled control of physical components.

While this definition may be suitable for a broad discussion about information technology, it does not account for relevant policymaking considerations concerning cybersecurity. Essentially, cybersecurity is the security of cyberspace.

When users go online they might work with their bank, get their email, conduct business, or get the news by accessing services. But those services don’t exist independently. Those services rely on a common infrastructure of servers and switches, miles of cabling, wireless spectrum, and routers. That same infrastructure is used by other services too, such as utilities and shipping to ensure products arrive as intended—or by businesses to develop new products more efficiently and manage their operations. The entire infrastructure and all those services that are part of cyberspace exist to deliver an experience to a user, a human.

Thus, from a policymaking standpoint cybersecurity can be considered the security of cyberspace—which includes the devices, infrastructure, data, and users that make it up. To support cybersecurity policymaking, adjacent fields also need consideration. Education, workforce management, investment, entrepreneurship, and research and development are necessary to get a product to market. Developers, law enforcement, intelligence, incident response, and national defense are necessary to respond when something goes awry in cyberspace.

### A2 C/I: Cybersecurity includes deterrence

#### Cybersecurity is deterrence through denial; distinct from deterrence through punishment.

#### Denning ’16 Denning, Dorothy; Emeritus Distinguished Professor of Defense Analysis. “Cybersecurity's next Phase: Cyber-Deterrence.” The Conversation, 22 Dec. 2021, https://theconversation.com/cybersecuritys-next-phase-cyber-deterrence-67090. //kinsey

Cybersecurity aids deterrence primarily through the principle of denial. It stops attacks before they can achieve their goals. This includes beefing up login security, encrypting data and communications, fighting viruses and other malware, and keeping software updated to patch weaknesses when they’re found.

But even more important is developing products that have few if any security vulnerabilities when they are shipped and installed. The Mirai botnet, capable of [generating massive data floods that overload internet servers](https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/), takes over devices that have gaping security holes, including [default passwords hardcoded into firmware](https://krebsonsecurity.com/2016/10/iot-device-maker-vows-product-recall-legal-action-against-western-accusers/) that users can’t change. While some companies such as [Microsoft invest heavily in product security](https://blogs.microsoft.com/microsoftsecure/author/stevelipner/), others, including many Internet-of-Things vendors, do not.

Cybersecurity guru [Bruce Schneier](http://www.schneier.com/) aptly characterizes the prevalence of insecure Internet-of-Things devices as a [market failure akin to pollution](https://www.washingtonpost.com/posteverything/wp/2016/11/03/your-wifi-connected-thermostat-can-take-down-the-whole-internet-we-need-new-regulations/). Simply put, the market favors cheap insecure devices over ones that are more costly but secure. His solution? Regulation, either by imposing basic security standards on manufacturers, or by holding them liable when their products are used in attacks.

### A2 OCO’s are Defensive/Prevent Attacks

#### Distinction between prevention of attacks through deterrence by denial versus deterrence by punishment.

Nor et al. ’20 Jörg Noll, Osman Bojang, Sebastiaan Rietjens NL ARMS Netherlands Annual Review of Military Studies 2020, 2021 ISBN : 978-94-6265-418-1 [https://link.springer.com/chapter/10.1007/978-94-6265-419-8\_7 Accessed 6/24/22](https://link.springer.com/chapter/10.1007/978-94-6265-419-8_7%20Accessed%206/24/22). //kinsey

The security and defense policies of the Baltic states are strongly influenced by the Russian aggression of 2014.[Footnote1](https://link.springer.com/chapter/10.1007/978-94-6265-419-8_7#Fn1) This also holds true for NATO. The alliance has deployed around 4,500 troops to Poland and the Baltic States since 2017. There is a large consensus amongst academics and practitioners that this mission, labelled Enhanced Forward Presence (eFP), should deter Russian aggression. However, the strategy to do so remains highly ambiguous and unclear (see also Running’s chapter in this volume). While many official NATO documents as well as observers simply refer to the strategy as deterrence, others, either explicitly or implicitly, distinguish between *deterrence by denial*[Footnote2](https://link.springer.com/chapter/10.1007/978-94-6265-419-8_7#Fn2) or *deterrence by punishment.*[Footnote3](https://link.springer.com/chapter/10.1007/978-94-6265-419-8_7#Fn3) The exact nature of the strategy can have far reaching consequences in terms of allocation of resources, strategic communication, (perceived) effectiveness as well as the very foundation of the alliance itself: the trust of every ally that it is protected by NATO in case of aggression.

Traditional deterrence theory presumes a rational actor perspective. Over time the role of psychology and actor specific perceptions has become more appreciated, in particular in the third wave in the deterrence literature. Most of these studies have focused on the history of the deterrent relationship and the nature of signaling behaviour.[Footnote4](https://link.springer.com/chapter/10.1007/978-94-6265-419-8_7#Fn4) However, although strategic culture has been widely acknowledged as an important shaping factor of strategic behaviour,[Footnote5](https://link.springer.com/chapter/10.1007/978-94-6265-419-8_7#Fn5) the role of strategic culture has been largely ignored in deterrence studies. This contribution aims to address this gap. Specifically, this chapter focuses on how strategic culture influences the Baltic countries’ behavior towards deterrence.

While most of the literature analyses eFP from the perspective of NATO or the troop contributing countries, this chapter addresses the question how the host nations, i.e. in this contribution Estonia, Latvia and Lithuania, perceive the strategy underlying eFP and their own strategies. Given the fact that NATO’s responses in the Baltics post-2014 were also intended to be ‘assurance measures’, such a perspective is important because similar or diverging perspectives can have far reaching consequences for NATO’s strategy and its credibility. We found that in Latvia official documents reflect the official NATO narrative based on deterrence by punishment. In Estonia and Lithuania, documents, officials and experts emphasize deterrence by denial as opposed or sometimes even parallel to deterrence by punishment. To understand these tendencies, this contribution contends that the respective strategic cultures of the host nations influence their perspectives on the NATO’s strategy. To that end, Sect. [7.2](https://link.springer.com/chapter/10.1007/978-94-6265-419-8_7#Sec2) briefly addresses the debate on deterrence and the different perspectives observers take on the eFP mission. Section [7.3](https://link.springer.com/chapter/10.1007/978-94-6265-419-8_7#Sec3) subsequently introduces strategic culture theory as a lens to explain the perspectives of the host nations. Section [7.4](https://link.springer.com/chapter/10.1007/978-94-6265-419-8_7#Sec4) outlines the methods we used. We discuss the results in Sect. [7.5](https://link.springer.com/chapter/10.1007/978-94-6265-419-8_7#Sec5) and provide a discussion and conclusions in Sect. [7.6](https://link.springer.com/chapter/10.1007/978-94-6265-419-8_7#Sec9).

#### OCO’s are attack by punishment.

**Devanny ’20** Devanny, D PhD. Lecturer in the Department of War Studies and Deputy Director of the Centre for Defense Studies. “The Ethics of Offensive Cyber: Reflections on the role of the national...” (2020, December 7). Feature from King's College London. Retrieved June 24, 2022, from https://www.kcl.ac.uk/the-ethics-of-offensive-cyber-reflections-on-the-role-of-the-national-cyber-force //kinsey

Turn off the lights in Moscow? This is just one of the possible uses of offensive cyber operations (OCOs) briefed to the press by senior British defence sources. Put simply, OCOs ‘project power to achieve military objectives in, or through, cyberspace.’ In everyday language, we are talking about ‘cyber attacks’ – from knocking websites offline to disabling computers on a network, shutting down a power grid, manipulating centrifuges in uranium enrichment facilities, or undermining an adversary’s air defences.

Over the last decade, the UK government has talked more openly about its cyber capabilities. The latest step was the prime minister’s [recent avowal of the National Cyber Force (NCF)](https://www.bbc.com/news/amp/technology-55007946), which has been operational since April. Uncertainty remains, however, about the role of OCOs in wider UK strategy and how our political leaders are navigating the complex choices involved in deciding when to use cyber operations to secure national objectives and project British values overseas. For example, should OCOs only target an adversary’s defence and security infrastructure, or should the UK follow the contemporary trend in targeting civilian infrastructure, as implied in the Moscow scenario briefed to the press?

### EXTRA STUFF:

### More definitions:

#### Cybersecurity is protection

**CISA 19.** *What Is Cybersecurity? | CISA* << government agency of cyber security and infrastructure that is compromised of researchers and experts hired through the bureaucratic process >>, <https://www.cisa.gov/uscert/ncas/tips/ST04-001> Accessed 24 June 2

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. It seems that everything relies on computers and the internet now—communication (e.g., email, smartphones, tablets), entertainment (e.g., interactive video games, social media, apps ), transportation (e.g., navigation systems), shopping (e.g., online shopping, credit cards), medicine (e.g., medical equipment, medical records), and the list goes on. How much of your daily life relies on technology? How much of your personal information is stored either on your own computer, smartphone, tablet or on someone else's system?

#### Security is protection which is different from prevention.

**Bacon n/d “**What Is Security?” <<QUALS>>, *SearchSecurity*, <https://www.techtarget.com/searchsecurity/definition/security> Accessed 24 June 22

Security for information technology (IT) refers to the methods, tools and personnel used to defend an organization's digital assets. The goal of IT security is to protect these assets, devices and services from being disrupted, stolen or exploited by unauthorized users, otherwise known as [threat actors](https://www.techtarget.com/whatis/definition/threat-actor). These threats can be external or internal and malicious or accidental in both origin and nature.

An effective security strategy uses a range of approaches to minimize vulnerabilities and target many types of cyberthreats. Detection, prevention and response to security threats involve the use of [security policies](https://www.techtarget.com/searchsecurity/definition/security-policy), software tools and IT services.

Unfortunately, technological innovation benefits both IT defenders and [cybercriminals](https://www.techtarget.com/searchsecurity/definition/cybercrime). To protect business assets, companies must routinely review, update and improve security to stay ahead of cyberthreats and increasingly sophisticated cybercriminals.

IT security consists of two areas: physical and information.

Security is the protection of people, hardware, software, network information and data from physical actions, intrusions and other events that could damage an organization and its assets. Safeguarding the physical security of a business means protecting it from threat actors, as well as accidents and natural disasters, such as fires, floods, earthquakes and severe weather. A lack of physical protection could risk the destruction of servers, devices and utilities that support business operations and processes. That said, people are a large part of the physical security threat.

Theft and vandalism are examples of human-initiated threats that require physical security solutions. A physical security breach doesn't necessarily require technical knowledge, but it can be just as dangerous as a [data breach](https://www.techtarget.com/searchsecurity/definition/data-breach).

### Protection vs. Prevention

#### Protection and prevention are distinct in the context of security.

**Invision Security 18**, <<security service information organization >>, “Protection And Prevention. What Is The Difference?,” *Invision Security Group*, 05/29/2018, <https://invisionsecuritygroup.com/protection-and-prevention-what-is-the-difference/>

**Prevention** is the act of assessing a hazard in advance and taking steps designed to lower its chances of happening. **Protection** is safeguarding your company against threats you know you’ll have to face or are currently facing.

#### True in the context of cybersecurity – protection must prevent an existing threat.

Grinavich, '20 – Director of Engineered Solutions at Vector Security (Jim Grinavich; "Business Security: The Difference Between Protection and Prevention"; Vector Security; https://www.vectorsecurity.com/blog/business-security-the-difference-between-protection-and-prevention; 1-23-2020, Accessed 6-25-2022)//ILake-NoC

Prevention generally comes before protection and is meant to avert the threat before it occurs. An example of prevention for business security includes a set of rules or reminders about best safety practices for cyber security.

Protection is the next step and usually takes over if prevention fails. Protection is a combination of security equipment and safety procedures used to defend against and eliminate threats. A monitored fire alarm and subsequent emergency evacuation plan are examples of quality protection.

Although prevention and protection are different, use both simultaneously to secure your business from possible threats.

## case

#### Research shows escalation through cyber ops is unrealistic

**Lonergan & Montgomery 22** (Mark Montgomery is the Executive Director of the Cyberspace Solarium Commission. Erica D. Lonergan is an Assistant Professor in the Army Cyber Institute. She is also a Research Scholar in the Saltzman Institute of War and Peace Studies at Columbia University.) 1/25/22, accessed 6/24/22, “Pressing Questions: Offensive Cyber Operations and NATO Strategy”, <https://mwi.usma.edu/pressing-questions-offensive-cyber-operations-and-nato-strategy/#:~:text=At%20the%202018%20Brussels%20summit,Provided%20Voluntarily%20by%20Allies%20process.> (JB)

Finally, there is an obvious risk that moving toward a more offensive posture in cyberspace will increase the likelihood of [escalation](https://academic.oup.com/ia/article/97/3/703/6205395?login=true). While these concerns should not be ignored, academic [research](https://www.jstor.org/stable/26760131?seq=1#metadata_info_tab_contents) has found [**little**](https://academic.oup.com/cybersecurity/article/5/1/tyz007/5575971)[**support**](https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf) **for the argument that cyber operations cause escalation**. That said, the alliance should consider how to strengthen existing [confidence-building measures](https://www.jstor.org/stable/26481908?seq=1#metadata_info_tab_contents), particularly with Russia, to enable more effective communication and transparency about cyber operations. The expert consultations between Russia and the United States that both governments agreed to in [June 2021](https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/), for example, or recent [diplomatic](https://www.nytimes.com/live/2022/01/10/world/russia-us-ukraine-talks) [dialogue](https://www.nato.int/cps/en/natohq/news_190924.htm) between Russia and NATO members over the Ukraine crisis, are important to strengthen processes for crisis management and reduce the risk of instability—including that which may stem from cyber operations.

NATO has slowly begun to address the use of offensive cyber operations, and has generally limited itself to the use of these tools in traditional military campaigns. The ongoing crisis with Russia on Ukraine’s border is exposing the risk in this approach. **NATO needs to figure out a way forward fast.**

## DA – PTX [neg]

### 1NR – L – OCOs

Offensive cyber operations are partisan with both Congress and the public

Bailey 20 – Associate Professor at the National Intelligence University specializing in national security law, international law, and professional ethics. He is also an adjunct instructor in the Master of Science in Cyber Security program at the University of Charleston (Christopher E. Bailey; ""; No Publication; https://www.bu.edu/ilj/files/2020/08/10.-Article\_Bailey.pdf; 8-10-2020, Accessed 6-25-2022)//ILake-AZ

The use of force has been a contentious topic throughout U.S. history, with the debate often split based upon partisan lines both in Congress and in the American public. The President has ample authority, under both constitutional and statutory law, to use force in a range of offensive and defensive scenarios– subject to certain process and substantive limitations. There is also ample room for abuse through the characterization of a covert activity as conduct that it is not a clandestine operation or a TMA, and by evasion of the Chief of Mission’s oversight. Offensive cyberspace operations raise questions about whether such operations are intelligence or military activities, whether operations are under the direction and control of civilians or uniformed military officers, whether the congressional reporting is exclusively limited to the intelligence committees or also includes the Armed Services committees, and whether there is coordination with the U.S. ambassadors serving abroad. Indeed, effective oversight over covert actions, both within the Executive branch and the Congress, is necessary to avoid an adverse impact on U.S. foreign policy and important liaison relationships, while promoting operational effectiveness and mitigating a risk of abuse.