# Aff---OCOs 2---BFHR

### Notes

Thanks a ton to Chanden Climaco, Brandon Yang, and Marshall Green for their work on this file.

Wave 2 of OCO’s aff/neg builds upon the starter pack OCO’s aff/neg file --- the NSA and Cybercom Tradeoff DA’s are designed to ideally apply to as many cyber affs as possible. The NSA DA in this file doesn’t reproduce every card in the starter pack. The aff section includes AT: new disads, a new zero-days mod, and various aff patchwork updates.

Please email [khirn10@gmail.com](mailto:khirn10@gmail.com) with any questions or concerns

# OCO Aff Updates

## Case

### Zero-Days Good---1AC

#### NATO OCO doctrine solves zero-day vulnerabilities---intel sharing improves warfighting outcomes, while disclosure enables allied to protect vulnerable networks from attacks

Fiddler 15. Marilyn Fiddler - Marshall Scholar, Department of Politics and International Relations, University of Oxford; Summer, 2015; “Regulating the Zero-Day Vulnerability Trade:A Preliminary Analysis”; I/S: A Journal of Law and Policy for the Information Society, 11, 405. <https://www.academia.edu/37789953/Regulating_the_Zero-Day_Vulnerability_Trade_A_Preliminary_Analysis> //BY

2. Analysis of NATO as an Institution for Zero-Day Trade Discussions

NATO is an influential body, and, if it addressed trade in zero-days, its policies would have global importance. NATO has been relatively successful in addressing new collective defense challenges, so it may have the institutional flexibility to take on zero-days. NATO membership maps well with participants in the zero-day market, including countries with notable buyers and sellers. Additionally, because NATO is a collective defense organization for allies, conceptions of the underlying security problem and opinions about approach may be more aligned than among states not engaged in collective defense. Given the difficulties of other forms of international cooperation, achieving consensus among allies might be strategically attractive.

NATO has developed a focus on cyber defense, and zero-days are relevant to that agenda. Not only could trade in zero-days facilitate attacks against NATO networks, but the stockpiling behavior of member states also leaves other members vulnerable. Key NATO members, such as the United States and United Kingdom, are purchasers of zero-days. [327](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=af1d795a-cfe3-4e91-9dd9-df15f57509a0&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Furn%3AcontentItem%3A5J0C-R6K0-02C9-B0YX-00000-00&pdcontentcomponentid=292707&pdteaserkey=sr4&pditab=allpods&ecomp=szznk&earg=sr4&prid=87902115-d576-4fb1-9e09-38944f5332d7) NATO's commitment to cyber defense has resulted in the development of a cyber policy- and decision-making structure and processes that could also be used to address the zero-day issue without significant alteration.

Despite this institutional base, NATO would have to experience a policy shift before addressing zero-days. Zero-days are inherently [[\*479]](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=af1d795a-cfe3-4e91-9dd9-df15f57509a0&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Furn%3AcontentItem%3A5J0C-R6K0-02C9-B0YX-00000-00&pdcontentcomponentid=292707&pdteaserkey=sr4&pditab=allpods&ecomp=szznk&earg=sr4&prid=87902115-d576-4fb1-9e09-38944f5332d7) exploitable: although they have significant implications for cyber defense, they are also closely tied with offensive capabilities of member states and the potential for NATO offensive capabilities. NATO, as an organization, is currently not positioned to discuss offensive cyber issues and has demonstrated wariness of an expanded cyber mandate. Still, as demonstrated by Libya and Russia's actions in Crimea, cyber is an increasing reality of security threats facing NATO. NATO must address cyber capabilities, not just passive cyber defense. Zero-days, as a technology that overlaps both categories, could be a useful place to start this shift.

If this shift occurred, NATO could use its existing structure to foster guidelines for addressing zero-days. The Cyber Defense Management Board (CDMB), which implemented the 2011 Action Plan, could be a starting place for discussions about zero-day policy. NATO could do this in several ways, including using CDMB to increase transparency and information sharing about zero-day issues within member states.

For instance, NATO could establish zero-day a threat-sharing program, in which governments share information about the nature of the zero-day threats they face. This kind of program would probably be least resisted by member states, but NATO could go further. NATO could institute a group disclosure program: when one member stockpiles a vulnerability, it could also disclose the vulnerability to a NATO clearinghouse. NATO members could then protect themselves against that vulnerability or make use of it. NATO could also push for harmonized purchasing policies, perhaps agreeing that NATO members will only purchase or stockpile certain vulnerabilities from certain countries or suppliers.

#### **Allied cyperwarfare enables rapid crisis response and the use of OCO’s in warfighting**

**Cushing ’14** [Seychelle; November 28; M.A. Political Science from Simon Fraser University; “Leveraging Information as Power: America’s Pursuit of Cyber Security,” <http://summit.sfu.ca/item/14703>]

In comparison, the zero-days used in cyber weapons require the US to constantly discover new vulnerabilities to maintain a deployable cyber arsenal. Holding a specific zero-day does not guarantee that the vulnerability will remain unpatched for a prolonged period of time by the targeted state.59 Complicating this is the fact that undetected vulnerabilities, once acquired, are rarely used immediately given the time and resources it takes to construct a cyber attack.60 In the time between acquisition and use, a patch for the vulnerability may be released, whether through routine patches or a specific identification of a security hole, rendering the vulnerability obsolete. To minimize this, America deploys several zero-days at once in a cyber attack to increase the odds that at least one (or more) of the vulnerabilities remains open to provide system access.61 Multiple backdoor entry points are preferable given that America cannot be absolutely certain of what vulnerabilities the target system will contain62 despite extensive pre-launch cyber attack testing63 and customization.64 A successful cyber attack needs a minimum of one undetected vulnerability to gain access to the target system. Each successive zero-day that works adds to the strength and sophistication of a cyber assault.65 As one vulnerability is patched, America can still rely on the other undetected vulnerabilities to continue its cyber strike. Incorporating multiple undetected vulnerabilities into a cyber attack reduces the need to create new cyber attacks after each zero-day fails. Stuxnet, a joint US-Israel operation, was a cyber attack designed to disrupt Iran’s progress on its nuclear weapons program.66 The attack was designed to alter the code of Natanz’s computers and industrial control systems to induce “chronic fatigue,” rather than destruction, of the nuclear centrifuges.67 The precision of Stuxnet ensured that all other control systems were ignored except for those regulating the centrifuges.68 What is notable about Stuxnet is its use of four zero-day exploits (of which one was allegedly purchased)69 in the attack.70 That is, to target one system, Stuxnet entered through four different backdoors. A target state aware of a specific vulnerability in its system will enact a patch upon detection and likely assume that the problem is fixed. Exploiting multiple vulnerabilities creates variations in how the attack is executed given that different backdoors alter how the attack enters the target system.71 One patch does not stop the cyber attack. The use of multiple zero-days thus capitalizes on a state’s limited awareness of the vulnerabilities in its system. Each phase of Stuxnet was different from its previous phase which created confusion among the Iranians. Launched in 2009, Stuxnet was not discovered by the Iranians until 2010.72 Yet even upon the initial discovery of the attack, who the attacker was remained unclear. The failures in the Natanz centrifuges were first attributed to insider error73 and later to China74 before finally discovering the true culprits.75 The use of multiple undetected vulnerabilities helped to obscure the US and Israel as the actual attackers.76 The Stuxnet case helps illustrate the efficacy of zero-day attacks as a means of attaining political goals. Although Stuxnet did not produce immediate results in terminating Iran’s nuclear program, it helped buy time for the Americans to consider other options against Iran. A nuclear Iran would not only threaten American security but possibly open a third conflict for America77 in the Middle East given Israel’s proclivity to strike a nuclear Iran first. Stuxnet allowed the United States to delay Iran’s nuclear program without resorting to kinetic action.78

#### Solves rogue state prolif

**Cushing ’14** [Seychelle; November 28; M.A. Political Science from Simon Fraser University; “Leveraging Information as Power: America’s Pursuit of Cyber Security,” <http://summit.sfu.ca/item/14703>]

Actively seeking to exploit and plant vulnerabilities helps the United States maintain a competitive advantage. Nuclear or conventional weapons, once developed, can remain dormant yet functional until needed. In comparison, the zero-days used in cyber weapons require the US to constantly discover new vulnerabilities to maintain a deployable cyber arsenal. Holding a specific zero-day does not guarantee that the vulnerability will remain unpatched for a prolonged period of time by the targeted state.59 Complicating this is the fact that undetected vulnerabilities, once acquired, are rarely used immediately given the time and resources it takes to construct a cyber attack.60 In the time between acquisition and use, a patch for the vulnerability may be released, whether through routine patches or a specific identification of a security hole, rendering the vulnerability obsolete. To minimize this, America deploys several zero-days at once in a cyber attack to increase the odds that at least one (or more) of the vulnerabilities remains open to provide system access.61 2.4. One Attack, Multiple Vulnerabilities Multiple backdoor entry points are preferable given that America cannot be absolutely certain of what vulnerabilities the target system will contain62 despite extensive pre-launch cyber attack testing63 and customization.64 A successful cyber attack needs a minimum of one undetected vulnerability to gain access to the target system. Each successive zero-day that works adds to the strength and sophistication of a cyber assault.65 As one vulnerability is patched, America can still rely on the other undetected vulnerabilities to continue its cyber strike. Incorporating multiple undetected vulnerabilities into a cyber attack reduces the need to create new cyber attacks after each zero-day fails. Stuxnet, a joint US-Israel operation, was a cyber attack designed to disrupt Iran’s progress on its nuclear weapons program.66 The attack was designed to alter the code of Natanz’s computers and industrial control systems to induce “chronic fatigue,” rather than destruction, of the nuclear centrifuges.67 The precision of Stuxnet ensured that all other control systems were ignored except for those regulating the centrifuges.68 What is notable about Stuxnet is its use of four zero-day exploits (of which one was allegedly purchased)69 in the attack.70 That is, to target one system, Stuxnet entered through four different backdoors. A target state aware of a specific vulnerability in its system will enact a patch upon detection and likely assume that the problem is fixed. Exploiting multiple vulnerabilities creates variations in how the attack is executed given that different backdoors alter how the attack enters the target system.71 One patch does not stop the cyber attack. The use of multiple zero-days thus capitalizes on a state’s limited awareness of the vulnerabilities in its system. Each phase of Stuxnet was different from its previous phase which created confusion among the Iranians. Launched in 2009, Stuxnet was not discovered by the Iranians until 2010.72 Yet even upon the initial discovery of the attack, who the attacker was remained unclear. The failures in the Natanz centrifuges were first attributed to insider error73 and later to China74 before finally discovering the true culprits.75 The use of multiple undetected vulnerabilities helped to obscure the US and Israel as the actual attackers.76 The Stuxnet case helps illustrate the efficacy of zero-day attacks as a means of attaining political goals. Although Stuxnet did not produce immediate results in terminating Iran’s nuclear program, it helped buy time for the Americans to consider other options against Iran. A nuclear Iran would not only threaten American security but possibly open a third conflict for America77 in the Middle East given Israel’s proclivity to strike a nuclear Iran first. Stuxnet allowed the United States to delay Iran’s nuclear program without resorting to kinetic action.78

#### Extinction

**Kassenova 20** (Togzhan Kassenova – nonresident fellow in the Nuclear Policy Program at the Carnegie Endowment. <KEN> "The Exploitation of the Global Financial Systems for Weapons of Mass Destruction (WMD) Proliferation," *Carnegie Endowment for International Peace*. March 2020. <https://carnegieendowment.org/2020/03/04/exploitation-of-global-financial-systems-for-weapons-of-mass-destruction-wmd-proliferation-pub-81221>)

1. WMD PROLIFERATION AS A SECURITY RISK1

Weapons of mass destruction – nuclear, biological, and chemical weapons - present a persistent risk to the U.S. and international security. If a 10-kiloton nuclear bomb, like the one tested by North Korea in 2013, is dropped in Washington, DC, a fireball of almost 500 feet in radius will cover the city.2 The radiation will reach such high levels within a half a mile radius that 50-90% percent of people could die without medical help – some of them within hours.

When it comes to preventing WMD proliferation, we need to be conscious of both state and non-state actors. North Korea continues to procure sensitive goods for its nuclear and missile program in defiance of sanctions. Iran is procuring missile-related goods. Agents working on behalf of Syria have sought chemical goods on the commercial market. Several groups, such as Al Qaeda and ISIS, demonstrated interest in acquiring a WMD capability. We do not have a full picture of who might be interested in obtaining a WMD capability in the future.

2. How Proliferation Networks Operate

Stealing or buying a ready-made weapon is a next to impossible feat. The main path to a WMD is to procure components, material, and technology and then build a weapon. Because most goods usable in a WMD program are dual-use in nature, with indispensable civilian purposes, they are available on the international commercial market.

The international community attempts to minimize the risk that trade in dual-use and military goods entails. The international export control regimes and national export control systems are designed to regulate trade in sensitive items by requiring traders to obtain licenses. Additionally, the international and unilateral sanctions regimes target known proliferators.

The goal of proliferators and their agents is to acquire goods that can contribute to WMD programs without being caught. Proliferators and their networks continue to defy both export controls and sanctions.

Proliferation networks come in all sizes and shapes. They can be small or large, loose, or more organized. Those buying WMD-related goods can be directly connected to proliferator states, or they can do it purely for profit by inserting themselves into the illicit market to make money.

Proliferators have perfected methods that help them stay under the radar.3 One of the standard techniques they use is to buy goods that are slightly below the controlled threshold. This means that unless exporting companies are incredibly vigilant,4 they would not apply for an export license and subject transaction to government scrutiny. However, these slightly inferior goods can still be used for nefarious purposes.

There is another method proliferators use to avoid government oversight and licensing—they pretend they are ordering goods for a domestic company. In such cases, supplier companies do not have to apply for licenses.

To avoid export controls and sanctions, proliferators lie about the end-use and end-user and hide behind front and shell companies all the time. They never declare that they are buying components for North Korea’s nuclear program, Iran’s missile program, or Syria’s chemical arsenal. For example, they can tell a supplying company they need goods for scientific research or other peaceful purposes. In 2006, an Iranian company ordered sensitive bioresearch equipment from Norway purportedly for a scientific laboratory. On closer look, an attentive Norwegian supplier determined that the equipment Iranians sought was technically superior to what would be necessary for a civilian lab and that it did not fit the physical layout of the laboratory.5

Increasingly, shipping companies and vessels are used prominently in sanction evasion. For example, Iran and North Korea falsify documents, reflag vessels, and switch off automatic identification systems to avoid being discovered in the process of illicit transfers of goods.6

Supplier companies that provide goods to proliferators can be complicit or not complicit. Larger companies have resources to implement strong internal compliance programs that help them detect any suspicious orders. But some companies, especially smaller ones, do not have resources to invest in compliance and remain negligent. In some cases, supplier companies or individuals within know precisely what they are doing. They do it either because of ideology (to support a sanctioned state) or for profit. In one notorious case, a U.S.-based company MKS Instruments sent pressure transducers to its subsidiary in China after duly applying for a U.S. export license, thinking that the goods would be used in China. The co-opted employee of the MKS Instruments’ subsidiary ordered transducers from an unsuspecting parent company and pretended they would be used by Chinese companies but planned all along to ship those goods to Iran.7 Pressure transducers can be used in uranium enrichment centrifuges, making possible the production of fissile material that can also be used in a nuclear weapon.

Proliferators prefer to buy good quality goods – mostly from the U.S., European, and Asian suppliers. This means that in most cases, they have to pay for those goods through the formal financial system, making financial institutions part of their proliferation schemes.

### Zero-Days Good---2AC

#### Zero-days key to cyber warfighting

**Cushing ’14** [Seychelle; November 28; M.A. Political Science from Simon Fraser University; “Leveraging Information as Power: America’s Pursuit of Cyber Security,” <http://summit.sfu.ca/item/14703>]

The Internet has made information seeking easier given its lax security structure that privileges offense over defence. Where the US once relied on its own ingenuity to support its national security innovations, it can now also purchase the necessary tools keep up with its peer competitors in cyberspace. Buying zero days in the vulnerabilities market thus serves a dual purpose: it takes away potential attack tools from its adversaries while building America’s own cyber arsenal. The problem, however, is that zero days may not work when you need them. Unlike nuclear or conventional weapons, there is no guarantee that an acquired zero-day can remain dormant yet functional. As a result, the US must consistently discover and collect zero-days to maintain a deployable cyber arsenal. America, despite its cyber superiority, cannot credibly threaten to use crushing cyber power to defeat its adversaries without revealing part of its capabilities. Compounding this problem is the fact that a cyber attack alone, while disruptive, is survivable at this time. America is thus experiencing a shift in its security strategy, albeit incrementally. What previously worked in the physical domain does not necessarily translate into successful primacy in the electronic domain. Although Cold War models of deterrence by denial and retribution may help frame the cyber problem, these models will eventually need to give way to new thinking about security in cyberspace. Deterrence, despite its Cold War successes, is not enough to stop your adversaries from attacking you in cyberspace. Instead, resiliency to absorb a cyber attack will carry America further in securing a net security advantage. While absorbing attacks seems counterintuitive, it is a short term risk that will garner important information. Resiliency then is as much about learning about your adversaries, their capabilities, and targets, and it is about comparatively measuring your own vulnerabilities and strengths in cyber offense and defence. The more information America can acquire, the better equipped it will be to face the cyber threat. Preparations for kinetic conflict are likely to begin in cyberspace as states collect vast information about their adversaries. Tapping into the millions of gigabytes of data that passes through the Internet is necessary to help America build a better picture of its adversaries’ actions and intent, including “the readiness of foreign militaries.”250 America, despite its cyber sophistication, cannot undertake such a task alone.251 Instead, the United States strategically shares information and capabilities with its partners to influence the intelligence priorities of the Five Eyes.252 Sharing initially puts the United States in a vulnerable position – exclusive control over a part of its cyber capabilities are conceded to its partners. From a vulnerable position, American cyber power can nevertheless influence conditions necessary to execute innovative, albeit high risk, intelligence operations. Information gathered from cyber can both reflect the strengths and weaknesses of America’s (and by extension, its adversaries’) offensive and defensive capabilities both within and outside cyberspace. Amassing an informational advantage to use against its adversaries will enable the US to enhance its security posture. Information, as the new realm of cyber security illustrates, is still a growing foundation of power. Leveraging information in cyberspace is key to producing a long-term net gain in security. In seeking a cyber advantage, the United States must endure short-term cyber insecurity. Tipping the security seesaw may not produce immediate advantages but instead, can be understood as a step towards long-term security. Consistently working to tip the seesaw towards advantage, while managing the associated vulnerabilities, helps produce a long-term advantage. The US’ ability to enhance its cyber posture while managing the associated vulnerabilities ultimately produces a net gain in national security.

#### Innovation is crucial to preventing cyberattack

**Cushing ’14** [Seychelle; November 28; M.A. Political Science from Simon Fraser University; “Leveraging Information as Power: America’s Pursuit of Cyber Security,” <http://summit.sfu.ca/item/14703>]

Adversaries study America’s cyber tool and techniques “to capitalize on [US…] ideas” for their own strategic advantage.89 On the one hand, innovating on its own code allows America to continue executing its security objectives in cyberspace. On the other hand, innovation allows the United States to speculate on how variations in its attack code may evolve to help anticipate potential attacks from its adversaries. While the United States may not be able to close all of its potential vulnerabilities,90 it can at least flag the unpatched vulnerabilities most likely exploited in a cyber strike. Red-teaming cyber games further allow the US to test both anticipated attacks and potential responses to maintain an informational advantage.91 Cyber favours offense over defence given its lax security architecture. Sophisticated cyber states that are able to innovate first will enjoy a relative advantage.92 Amassing an arsenal of undetected vulnerabilities does not necessarily produce an immediate, usable advantage. Instead, these vulnerabilities provide important information to gauge the strengths and weaknesses of America’s offensive and defensive capabilities. Finding undetected vulnerabilities, and knowing how to exploit those, positions the US to capitalize on the offense-defence innovation cycle to preserve a cyber advantage. The strike methods of nuclear or conventional weapons are largely unchanged and can be used to great effect. Cyber weapons, in comparison, only successfully work once. Innovation is required to not only manage the “constant pressure to keep up,”93 but to also tip the balance of informational advantage in your favour.

#### Cushing ev says that maintaining the offensive use of zero-days allows rapid crisis response capabilities --- the impact is every major security threat

**Berkowitz, 8** - research fellow at the Hoover Institution at Stanford University and a senior analyst at RAND. He is currently a consultant to the Defense Department and the intelligence community (Bruce, STRATEGIC ADVANTAGE: CHALLENGERS, COMPETITORS, AND THREATS TO AMERICA’S FUTURE, p. 1-4)

THIS BOOK is intended to help readers better understand the national security issues facing the United States today and offer the general outline of a strategy for dealing with them. National security policy—both making it and debating it — is harder today because the issues that are involved are more numerous and varied. The problem of the day can change at a moment's notice. Yesterday, it might have been proliferation; today, terrorism; tomorrow, hostile regional powers. Threats are also more likely to be intertwined—proliferators use the same networks as narco-traffickers, narco-traffickers support terrorists, and terrorists align themselves with regional powers. Yet, as worrisome as these immediate concerns may be, the long-term challenges are even harder to deal with, and the stakes are higher. Whereas the main Cold War threat — the Soviet Union — was brittle, most of the potential adversaries and challengers America now faces are resilient. In at least one dimension where the Soviets were weak (economic efficiency, public morale, or leadership), the new threats are strong. They are going to be with us for a long time. As a result, we need to reconsider how we think about national security. The most important task for U.S. national security today is simply to retain the strategic advantage. This term, from the world of military doctrine, refers to the overall ability of a nation to control, or at least influence, the course of events.1 When you hold the strategic advantage, situations unfold in your favor, and each round ends so that you are in an advantageous position for the next. When you do not hold the strategic advantage, they do not. As national goals go, “keeping the strategic advantage” may not have the idealistic ring of “making the world safe for democracy” and does not sound as decisively macho as “maintaining American hegemony.” But keeping the strategic advantage is critical, because it is essential for just about everything else America hopes to achieve — promoting freedom, protecting the homeland, defending its values, preserving peace, and so on. The Changing Threat If one needs proof of this new, dynamic environment, consider the recent record. A search of the media during the past fifteen years suggests that there were at least a dozen or so events that were considered at one time or another the most pressing national security problem facing the United States — and thus the organizing concept for U.S. national security. What is most interesting is how varied and different the issues were, and how many different sets of players they involved — and how each was replaced in turn by a different issue and a cast of characters that seemed, at least for the moment, even more pressing. They included, roughly in chronological order, • regional conflicts — like Desert Storm — involving the threat of war between conventional armies; • stabilizing “failed states” like Somalia, where government broke down in toto; • staying economically competitive with Japan; • integrating Russia into the international community after the fall of communism and controlling the nuclear weapons it inherited from the Soviet Union; • dealing with “rogue states,” unruly nations like North Korea that engage in trafficking and proliferation as a matter of national policy; • combating international crime, like the scandal involving the Bank of Credit and Commerce International, or imports of illegal drugs; • strengthening international institutions for trade as countries in Asia, Eastern Europe, and Latin America adopted market economies; • responding to ethnic conflicts and civil wars triggered by the reemergence of culture as a political force in the “clash of civilizations”; • providing relief to millions of people affected by natural catastrophes like earthquakes, tsunamis, typhoons, droughts, and the spread of HIV/AIDS and malaria; • combating terrorism driven by sectarian or religious extremism; • grassroots activism on a global scale, ranging from the campaign to ban land mines to antiglobalization hoodlums and environmentalist crazies; • border security and illegal immigration; • the worldwide ripple effects of currency fluctuations and the collapse of confidence in complex financial securities; and • for at least one fleeting moment, the safety of toys imported from China. There is some overlap in this list, and one might want to group some of the events differently or add others. The important point, however, is that when you look at these problems and how they evolved during the past fifteen years, you do not see a single lesson or organizing principle on which to base U.S. strategy. Another way to see the dynamic nature of today's national security challenges is to consider the annual threat briefing the U.S. intelligence community has given Congress during the past decade. These briefings are essentially a snapshot of what U.S. officials worry most about. If one briefing is a snapshot, then several put together back to back provide a movie, showing how views have evolved.2 Figure 1 summarizes these assessments for every other year between 1996 and 2006. It shows when a particular threat first appeared, its rise and fall in the rankings, and in some cases how it fell off the chart completely. So, in 1995, when the public briefing first became a regular affair, the threat at the very top of the list was North Korea. This likely reflected the crisis that had occurred the preceding year, when Pyongyang seemed determined to develop nuclear weapons, Bill Clinton's administration seemed ready to use military action to prevent this, and the affair was defused by an agreement brokered by Jimmy Carter. Russia and China ranked high as threats in the early years, but by the end of the decade they sometimes did not even make the list. Proliferation has always been high in the listings, although the particular countries of greatest concern have varied. Terrorism made its first appearance in 1998, rose to first place after the September 11, 2001, terrorist attacks, and remains there today. The Balkans appeared and disappeared in the middle to late 1990s. A few of the entries today seem quaint and overstated. Catastrophic threats to information systems like an “electronic Pearl Harbor” and the “Y2K problem” entered the list in 1998 but disappeared after 2001. (Apparently, after people saw an airliner crash into a Manhattan skyscraper, the possible loss of their Quicken files seemed a lot less urgent.) Iraq first appeared in the briefing as a regional threat in 1997 and was still high on the list a decade later—though, of course, the Iraqi problem in the early years (suspected weapons of mass destruction) was very different from the later one (an insurgency and internationalized civil war). All this is why the United States needs agility. It not only must be able to refocus its resources repeatedly; it needs to do this faster than an adversary can focus its own resources.

### Cyber Resilience---2AC

#### US-NATO cyberwarfare must be defined by resilience---interoperability and cyberwarfighting are crucial

**Moens ’15** [Alexander, Seychelle Cushing, and Alan Dowd; March; professor of political science at Simon Fraser University and a Senior Fellow in Canadian-American Relations at the Fraser Institute; M.A. with Distinction from the Department of Political Science at Simon Fraser University in 2014; Alan W. Dowd is a Senior Fellow and Senior Editor with the Fraser Institute; “Cybersecurity Challenges for Canada and the United States,” https://www.fraserinstitute.org/sites/default/files/cybersecurity-challenges-for-canada-and-the-united-states.pdf]

The absence of formal international agreements on cybersecurity does not mean there are no rules or boundaries in practice. The rule of consequences and of self-interest is in play, as is the logic of cost-benefit in escalation. For example, using cyberspace to inflict fatalities on foreign citizens or physical damage to key economic assets is not something APTs would consider lightly. Experts debate whether such extensive attacks are even possible given current capabilities (Rid, 2013; Libicki, 2009; Samaan, 2010; Clarke and Knake, 2010). To illustrate: it may be possible to interfere with the operation of a large dam via cyberspace from abroad, but destroying the concrete structure and drowning a city down river is quite another matter. To be sure, President Barack Obama is on record warning hostile players that cyberattacks are not isolated from the rest of defence policy and national security. In 2011, he used the loaded term “all necessary means” to describe the possible American reaction should the nature of the attack so warrant (U.S. White House, 2011: 14). Interestingly, Russian military officials have argued that “the use of information warfare against Russia or its armed forces will categorically not be considered a non-military phase of a conflict, whether there were casualties or not” (Hildreth, 2001: 11). If deterrence is what kept the peace during the Cold War and the Nuclear Age, resilience may be the governing principle of the Digital Age. Deterrence, after all, works best when your adversaries have a clear idea of what you can and will do if attacked (Betts, 2013). Yet, in cyberwarfare, secrecy is paramount in maintaining a competitive edge. Defining what weapons you will retaliate with when attacked invariably reveals part of your capabilities. Having an effective deterrent in cyberspace is thus problematic. The apparent attack by the North Korean government under the name of “Guardians of Peace” against the Sony Corporation in late 2014 seems to have set off a US reaction. The wiper malware used against Sony wreaked havoc on the company and brought to a halt its imminent release of the satirical movie about Kim Jong-un called “The Interview”. A few days later, North Korea’s admittedly small Internet went dark for a period of time. Possibly, Obama made good on his threat that North Korea’s “cyber vandalism” would be met with “a proportional response” (Perlroth and Sanger, 2014, December 22). In short, the operational concept best suited for cybersecurity per se is resilience. Resilience is quite different from deterrence, since resilience presupposes weathering an attack, while the aim of deterrence is to prevent an attack through the avowal of overwhelming retaliation. Moreover, given that the nature of cyberattacks is still evolving and that attackers increasingly use third and fourth parties to channel their attacks, and thus create false leads for those trying to find the attacker (Geers, 2010), traditional notions of deterrence may not apply in cyberspace. A better defence is the ability to sustain one or more cyberattacks and to be able to counter and restore defensive capacity (Lindsay, 2013). How you recover and how you function when compromised becomes of utmost importance. This appears to be the path NATO has chosen. The alliance regularly conducts defensive war games, such as Baltic Cyber Shield and Locked Shields, in cyberspace. In 2013, NATO defence ministers agreed to establish Rapid Reaction Teams to provide better protection for NATO’s networks (NATO, 2014a). In 2014, the alliance declared cyberdefence “part of NATO’s core task of collective defence” and noted that cyberattacks could lead to invocation of Article 5 of the North Atlantic Treaty, NATO’s all-for-one collective defence commitment, which has been the foundation of Western deterrence since 1949 (NATO, 2014b: §72). Still, NATO’s 2011 policy on cybersecurity focuses on “prevention, resilience and defence of critical cyber assets to NATO and Allies” (NATO, 2011: 1).

#### Innovation fosters resilience ---- it’s the only internal link to long-term stability

**Cushing ’14** [Seychelle; November 28; M.A. Political Science from Simon Fraser University; “Leveraging Information as Power: America’s Pursuit of Cyber Security,” <http://summit.sfu.ca/item/14703>]

Adversaries study America’s cyber tool and techniques “to capitalize on [US…] ideas” for their own strategic advantage.89 On the one hand, innovating on its own code allows America to continue executing its security objectives in cyberspace. On the other hand, innovation allows the United States to speculate on how variations in its attack code may evolve to help anticipate potential attacks from its adversaries. While the United States may not be able to close all of its potential vulnerabilities,90 it can at least flag the unpatched vulnerabilities most likely exploited in a cyber strike. Red-teaming cyber games further allow the US to test both anticipated attacks and potential responses to maintain an informational advantage.91 Cyber favours offense over defence given its lax security architecture. Sophisticated cyber states that are able to innovate first will enjoy a relative advantage.92 Amassing an arsenal of undetected vulnerabilities does not necessarily produce an immediate, usable advantage. Instead, these vulnerabilities provide important information to gauge the strengths and weaknesses of America’s offensive and defensive capabilities. Finding undetected vulnerabilities, and knowing how to exploit those, positions the US to capitalize on the offense-defence innovation cycle to preserve a cyber advantage. The strike methods of nuclear or conventional weapons are largely unchanged and can be used to great effect. Cyber weapons, in comparison, only successfully work once. Innovation is required to not only manage the “constant pressure to keep up,”93 but to also tip the balance of informational advantage in your favour.

#### Resilience is key

**Creighton ’15** [Neal Creighton, October 19, 2015, “The New Cyber Resiliency: Absorption, Containment And Real-Time Offensive,” <http://www.hstoday.us/columns/critical-issues-in-national-cybersecurity/blog/new-the-new-cyber-resiliency-absorption-containment-and-real-time-offensive/0301a26262ddbebbab4bf5e28dc094ab.html>]

Organizations today are subjected to meticulously scoped, expertly developed and targeted attacks by nation-states and criminal groups. Given how public large-scale data breaches have become, cybersecurity has become a household term. But this new normal means no one rests easy.

Emerging from the shadows of the news coverage of devastating breaches in retail, government, healthcare and finance, is the need for government agencies to think about their role and how to better withstand a breach that compromises proprietary information and could threaten critical infrastructure.

Organizations—particularly their enterprise security teams—are working tirelessly to keep attackers out, to mitigate the damage perpetrators cause and to innovate for the future. Cybersecurity has become a new battlefield with an endless number of attacks ahead.

Like a real battlefield, where adversaries are using all types of weapons, hackers are also using innovation to develop new attack methods and even build new variants of tried and true methods like SQL injection attacks. The threat landscape that organizations have to deal with is all-encompassing and evolving consistently--malware-based attacks (rootkits, ransomware); zero-day's and APT's; code injection attacks and nation-state attacks, who are now attacking multinationals--meaning it’s not just espionage.

In the past, cybersecurity was about building a bigger wall to keep criminals out—we’re no longer living in that world because the network perimeter has become ubiquitous. A new security mindset is required. We have to shift to thinking not “if,” but “when,” it happens.

A recent Gartner report, Six Principles of Resilience to Address Digital Business Risk and Security, underscores the situation at hand and categorizes a new macro trend as of 2015: the growing capacity and sophistication of digital adversaries to breach our defenses and cause major business disruptions in business operations. There should be no doubts that we need to act now.

Applying a targeted military-style strategy

Government agencies (and all organizations) need a strategy that maps to the tried and tested military strategy of resilience to defeat the cyberworld’s adversaries on multiple levels. The primary objective is protecting the agency while preserving continuity and IP. No longer can you think about winning every cyber battle—instead, it’s about proving long-term that your organization doesn’t have to succumb to methodical, targeted attacks if resiliency sits at the core of the fundamental security strategy.

National Security Agency Director and Commander of US Cyber Command Admiral Mike Rogers, helped draw the parallel of how important it is to focus attention on being more cyber-resilient in the face of emerging threats last year. As a 30 year-plus veteran of the Navy, he pointed to the military and says they do not abort their missions in the face of resistance, but instead they accept they will sustain a certain amount of collateral damage without laying down their arms.

The comparison here is how, in the past, and even still today, many security and IT teams simply “nuke and pave” machines that become infected—essentially taking them offline and/or wiping them entirely. This is the equivalent of inviting more attackers to attack, as they ultimately have visibility into machine status if they are sophisticated and persistent enough.

This outdated process across thousands of infected endpoints starts to drive costs and resources astronomically. In fact, the average security organization faces over 17,000 security notifications today, with typically the ability to only investigate about 700. At that point, they’ve already burned 395 incident response man-hours. This means security incident handling has become an expensive proving ground for incidents to either go uninvestigated, investigated for too long … or for incidents to proliferate as advanced threats.

What it comes down to is that attackers got in because current tools weren’t detecting their presence. Simple.

Achieving victory in a battle or a war requires showing resiliency in the face of fire, and prevailing despite enduring some level of loss along the way. The cyber equivalent of this is actually accepting that an attacker might penetrate your network, but being able to rapidly detect their presence and counter their techniques with the capability to quarantine the threat to mitigate its effectiveness, ultimately closing the doors to further infiltration.

### Yes Cyber Escalation---2AC

#### Cyber attacks escalate---miscalc and misperception, tit for tat retal, and grid collapse ensure it

Healey 22. Jason Healey is a senior research scholar and adjunct professor at the School of International and Public Affairs, Columbia University. He is also a senior fellow with the Cyber Statecraft Initiative at the Atlantic Council, where he was the program's founding director; “PREPARING FOR INEVITABLE CYBER SURPRISE”; January 12, 2022; War on the Rocks; <https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/> //BY

Surprise in cyberspace is more important than in other domains for four reasons. The dynamics of cyber conflict lend themselves to surprising uses across all five meanings of surprise. They rely on deception and trickery; enable the unexpected and unforeseen; are sudden and fast, audacious and daring; and are especially useful early in a conflict. There are also significant first-use pressures, as they may present five ways to increase the danger of a [security dilemma](https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/). Because cyber capabilities are not easily observable, it is extremely difficult to assess an adversary’s order of battle or relative strength, or to detect the equivalent of tanks massing on the border. Any particular attack might have an asymmetric impact, keeping defenders on perpetual and [exhausting](https://www.securitymagazine.com/articles/96169-hacking-burnout-addressing-stress-among-security-professionals) [high alert](https://www.microsoft.com/security/blog/2021/02/17/6-strategies-to-reduce-cybersecurity-alert-fatigue-in-your-soc/).

There is also a nearly limitless realm of the possible. Cyber capabilities can bypass fielded military forces to affect a seemingly indefinite range of elements within an adversary’s society, economy, and psychology. The pace of innovation and dependence creates countless paths to attain technical surprise, as does the use of “[existing weapons and forces in new and different ways](https://core.ac.uk/download/pdf/36732393.pdf).” Even more so than in other kinds of intelligence warning, “[[t]here are few limits on what can be imagined](https://www.amazon.com/dp/B004OA6IO4/ref=dp-kindle-redirect?_encoding=UTF8&btkr=1),” so defenders have less chance of assessing where a blow may fall.

Further, economies, societies, and militaries are increasingly interconnected and deeply cyber-dependent, so cyber capabilities offer an attacker more opportunities to believe that they can shift the correlation of forces in their favor. Some experts assert that “[[c]yber attack does not threaten crippling surprise or existential risk](https://www.amazon.com/Rethinking-Cybersecurity-Strategy-Effect-Reports/dp/1442280514),” as past attacks have only disrupted computer components that can be replaced relatively quickly. Yet this misses the scope of potential future cyber operations.

With the “internet of things” and cyber physical systems, attacks can now impact electrical grids, pipelines, and dams, [objects made of concrete and steel](https://eandt.theiet.org/content/articles/2013/12/interview-with-jason-healey/), thereby boosting the potential impact of and opportunities for surprise attacks. The [shift of the Internet as primarily a communications tool between people to increasingly a control mechanism for physical systems](https://www.lauradenardis.com/internet-in-everything) will result in operations and outcomes far outside the expectations of academic theories and government strategies which can still treat cyber-physical systems as an edge case.

Even hard targets aren’t as hard as they might seem. Too difficult to directly hack FireEye or the Department of Justice? The Russians got both, plus thousands more, by going after SolarWinds.

States are also not limited to the capabilities that they patiently build over time, as with more conventional forces. Iran has [rapidly expanded](https://www.cnbc.com/2021/11/18/iran-leapfrogging-our-defenses-in-cyber-war-hacking-expert-mandia-.html) its capabilities so that Leon Panetta, the then-Secretary of Defense, told New York Times reporter [Nicole Perlroth](https://www.amazon.com/dp/B0877D6H28/ref=dp-kindle-redirect?_encoding=UTF8&btkr=1) the Department of Defense “was astounded that Iran could develop” sophisticated capabilities. Iran’s Gulf rivals, such as the United Arab Emirates, have [used contractors](https://www.lawfareblog.com/prosecuting-project-raven-new-frontier-export-control-enforcement) for a turn-key cyber command. States are more likely to deliver offensive surprises when their reach is not just limited by what they nurture, but also by what they can buy.

Lastly, there is high potential for mistake and miscalculation. The novelty of cyber attacks means that adversaries are more likely to misjudge how their operations will be perceived by the recipient. The attacker might believe that its attack is within the norms, justified because it is a tit-for-tat reprisal, or similar to a past operation that acted as a pressure release, defusing a crisis. A rival might shrug off being the target of a disruptive operation conducted in relative peacetime (“Ah, it’s just an intelligence contest,”) only to respond aggressively to a lesser attack in the midst of a crisis (“This could be the prelude to a surprise attack!”).

Cyber attacks are likely to flop (or worse, messily cascade) if they are not backed by meticulous intelligence, careful planning, and extensive testing — although these only reduce, rather than eliminate, the risks. Mistakes can take the target (and indeed, the attacker) by surprise, as happened with North Korea and Russia with WannaCry and [NotPetya](https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html), respectively.

Surprise, Russia, and Ukraine

The Russian buildup in late 2021 for a possible invasion of Ukraine highlights the worrying role of cyber surprise in geopolitics. Just a year ago, the cybersecurity company Mandiant discovered an [extensive Russian intrusion](https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html) that had been propagated through network management software made by SolarWinds. Imagine for a moment that this intrusion were still undiscovered — or that the Russians have a similar but as yet undiscovered campaign, perhaps built using the [massive log4j vulnerability](https://warontherocks.com/2022/01/log4j-cyber-threat-requires-new-approach-to-design-flaws/).

### Cohesion Adv---2AC

#### Absent coordinating unified NATO policy over OCO’s, Russia will exploit divisions to wreck the alliance

Smeets 19. 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; “Cyber Command’s Strategy Risks Friction With Allies”; May 28, 2019; Lawfare; <https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies> //BY

Much has been written about the fundamental changes in U.S. cyber strategy. U.S. Cyber Command’s vision of “[persistent engagement](https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010)” and the Department of Defense’s new strategy of “[defend forward](https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf)” have, in particular, led to numerous [critical remarks](https://www.thecipherbrief.com/triggering-new-forever-war-cyberspace) about the [risks](https://www.lawfareblog.com/what-absent-us-cyber-command-vision) [of](https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward) [escalation](https://medium.com/freeman-spogli-institute-for-international-studies/bytes-bombs-and-spies-261564d51157) between the U.S. and [its](https://www.lawfareblog.com/american-perspective-chinese-perspective-defense-departments-cyber-strategy-and-defending-forward) [main](https://www.lawfareblog.com/deepening-us-china-cybersecurity-dilemma) [adversaries](https://www.lawfareblog.com/chinese-perspective-pentagons-cyber-strategy-active-cyber-defense-defending-forward) in [cyberspace](https://www.lawfareblog.com/what-really-matters-defending-forward).

These debates are worth continuing, including about what the change in strategy means for [establishing](https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace) [norms](https://www.lawfareblog.com/what-agreed-competition-cyberspace) [in](https://www.lawfareblog.com/there-are-too-many-red-lines-cyberspace) [cyber](https://www.lawfareblog.com/through-persistent-engagement-us-can-influence-agreed-competition)[space](https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace). But commentators have so far ignored a key dimension: The strategy’s main implications may not reside in how it changes the dynamics between the U.S. and its adversaries but, instead, in how it affects broader alliance relationships, especially beyond the Five Eyes (Australia, Canada, the U.K., the U.S. and New Zealand). U.S. Cyber Command’s mission to cause friction in adversaries’ freedom of maneuver in cyberspace may end up causing significant friction in allies’ trust and confidence—and adversaries may be able to exploit that.

Operating “Seamlessly, Globally, and Continuously”

Cyber Command’s new strategy seeks to operate “seamlessly, globally, and continuously.” It states that “[s]uperiority through persistence seizes and maintains the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver.” According to the strategy document, Cyber Command intends to do this “as close as possible to adversaries and their operations,” connecting persistent engagement to the Pentagon’s principle of “defending forward.”

In an article for [Joint Force Quarterly](https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-92.aspx) (JFQ), NSA Director and Cyber Command head Gen. Paul Nakasone writes: “We must instead maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries.”

When Nakasone says the U.S. must get “as close as possible to adversaries and their operations,” he implies that the U.S. seeks to achieve effects that are outside of its own networks and beyond the networks of its adversaries. This vast area is not ungoverned space. It includes, for example, routers in Nairobi, servers in Denmark or operating infrastructure in any other country around the world.

Blue Space, Gray Space and Red Space

In the JFQ article, Nakasone also states that “if we are only defending in ‘blue space’ we have failed.” This use of terminology as well as talk about “operating close to the adversary” evades one issue: It is unclear whether Cyber Command only seeks to cause friction in “red space” or if it seeks to compete in “gray space” as well. These terms are often confused and not well-understood. (The terms “gray zone”—areas where it’s unclear whether the government has legal authority to act—and “gray space” are also frequently confused.) In fact, the issue was raised for “further exploration” at Cyber Command’s 2018 symposium, [specifically](https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%20Proceedings%202018.pdf?ver=2018-07-11-092344-427) understanding the “relevance of concepts like area of responsibility and red-blue-gray space to the cyberspace domain.”

[Joint Publication 3-12](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150) (JP 3-12) on cyberspace operations, prepared under the direction of the chairman of the Joint Chiefs of Staff, explains the terminology:

The term “blue cyberspace” denotes areas in cyberspace protected by the US, its mission partners, and other areas DOD may be ordered to protect. Although DOD has standing orders to protect only the Department of Defense information network (DODIN), cyberspace forces prepare on order, and when requested by other authorities, to defend or secure other United States Government (USG) or other cyberspace, as well as cyberspace related to critical infrastructure and key resources (CI/KR) of the US and PNs [partner nations]. The term “red cyberspace” refers to those portions of cyberspace owned or controlled by an adversary or enemy. In this case, “controlled” means more than simply “having a presence on,” since threats may have clandestine access to elements of global cyberspace where their presence is undetected and without apparent impact to the operation of the system. Here, controlled means the ability to direct the operations of a link or node of cyberspace, to the exclusion of others. All cyberspace that does not meet the description of either “blue” or “red” is referred to as “gray” cyberspace.

Gray space is defined based on the nodes adversaries control. This means the vast area between U.S. government-owned networks and adversaries is not considered to be gray space. Instead, if for instance the GRU (Russia’s military intelligence agency) controls a node in the Netherlands, it is considered to be red space based on JP 3-12. And it’s worth mentioning that the notion of control is open to interpretation by states.

This means that if Cyber Command seeks to operate only in “red space,” its activities will still have global reach (globally). It also suggests that red space grows as adversaries expand their operational activity. Most importantly, this implies that if Cyber Command seeks to achieve “effects” in gray space, this will involve operating infrastructure that adversaries do not control—which is to say those systems or networks on which adversaries merely have a presence or are not active at all.

What’s New Under the Sun?

What’s really new here? The United States has long operated in networks “close to the adversary.” As Ben Buchanan’s book, “[The Cybersecurity Dilemma](https://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780190665012.001.0001/acprof-9780190665012),” demonstrates, the U.S. has long acted as an “observer” in gray space, gathering intelligence of adversarial activity in those others’ networks. In fact, information has become public concerning a case in which the Five Eyes collected intelligence about an espionage platform (dubbed [“Snowglobe” by the Canadian Intelligence Agency CSEC](https://resources.infosecinstitute.com/animal-farm-apt-and-the-shadow-of-france-intelligence/#gref) and [“Animal Farm” by Kaspersky Lab](https://securelist.com/animals-in-the-apt-farm/69114/)) of an allied country, France, likely operating in adversarial networks in the Middle East. In other words, the [practice of fourth-party collection](https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07170728/Guerrero-Saade-Raiu-VB2017.pdf) is nothing new. And the U.S. has also long acted in foreign nonadversarial networks as a “passerby,” transiting through gray space networks to access an adversarial network.

But the new Cyber Command and Defense Department strategy changes the nature of the U.S. military’s behavior within those systems and networks. Under the new strategy, Cyber Command wants to be an active disrupter on those networks. It wants to achieve effects.

The only [known](https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.736ecd105d75) [precedent](https://www.cyberscoop.com/us-cyber-command-nsa-government-hacking-operations-fight/) is Cyber Command operators wiping Islamic State propaganda material off a server located in Germany. The German government was[notified in some fashion but not asked for advance consent](https://www.lawfareblog.com/title-10-and-title-50-issues-when-computer-network-operations-impact-third-countries), causing much frustration.

This will likely lead to a systematic scaling up: Cyber Command now also seeks to be an active disrupter on those networks “globally, continuously and seamlessly”—not regionally and sporadically.

The Danger of Operating Seamlessly in Allied Networks

Operating instantly makes sense considering the potential operational tempo of adversaries: You can’t have protracted diplomatic discussions for two months with an ally about whether or not to take down some command and control infrastructure of an adversary hosted in the allied country. You don’t have days, let alone months. As a participant mentioned at the recent Chatham House Rule 2019 Cyber Command Symposium on strategy: “Opportunities within this domain are fleeting.”

Operating seamlessly could also make sense if an ally does not mind the U.S. coming into its networks to address the malicious activity. In this vein, the U.S. can continue to build partnerships with countries that do not have the capacity to defend against cyber attacks on their own.

But, what if an allied country is not keen on having the U.S. military in its networks, actively, seamlessly, and continuously disrupting an adversary’s cyber operations? As the German case shows, this scenario will likely come up a lot more in the near future.

In other words, in seeking to successfully create friction in cyberspace for adversaries, Cyber Command may also seek to act within allied networks, even if the ally does not approve. It might even be successful in its mission, causing friction in adversaries’ operations before they cause serious harm to the U.S. But this strategy runs a real risk of undermining allies’ trust and confidence in ways that are subtle and not easily observable. This ought not to be overlooked, especially since this element may itself be exploited by adversaries.

Adversaries don’t randomly choose which intermediate nodes to direct their operations through. If Russia has the choice to go through a network that would raise some serious diplomatic friction between the U.S. and a U.S. ally, or operate through a network that would cause no diplomatic friction for the U.S., what would it prefer? It would make sense for adversaries to operate through the networks of exactly those countries with which the U.S. has a strong relationship but that do not want the U.S. to operate within their networks causing any effects.

Russia is already good at exploiting divisions between the U.S. and its allies. Cyber Command’s new strategy might give it another avenue to do so.

#### Consolidated OCO norms are key to democratic governance and the liberal international order

Liebetrau 22. Tobias Liebertrau is a Affiliated researcher at the Danish Institute for International Studies; “Cyber conflict short of war: a European strategic vacuum”; February 4, 2022; Taylor and Francis; <https://doi.org/10.1080/09662839.2022.2031991> //BY

This article examined how three European NATO members – the Netherlands, France, and Norway – perceive and respond to continuous adversarial cyber operations short of war. The analysis demonstrated that the Dutch, French, and Norwegian decisions to develop offensive military cyber capabilities date 10–15 years back. In all three countries, the development of offensive cyber measures has been portrayed as a timely investment in necessary capabilities intended to deter and support military operations in armed conflict. The analysis also showed that the three countries – to different degrees and clarifications – have acknowledged that the adversarial nature of cyber operations short of war forms part of the current strategic reality. Yet, their cyber strategies and military doctrines continue to primarily centre on warfare and armed conflict.

Thus, the paper identifies a strategic vacuum as none of the three countries have formulated strategic frameworks that map onto the identified strategic reality. The recent publications of military cyber doctrines in France and the Netherlands provide initial strategic guidance for armed conflict, but it remains underspecified how the impact of continuous cyber conflict short of war affects the countries’ view on international political competition, their strategic positioning, and their military-intelligence relations. Questions concerning when, how, who and to what extent cyber countermeasures are deployed against hostile cyber operations short of war remain ambiguous and secretive. This lack of clarity, strategic guidance, and public debate puts societies at risk and undermines democratic governance.

The insistence on the importance of formulating strategy and publicly discussing how to deal with cyber conflict short of war does not deny that all three countries are already engaged in countering hostile cyber operations short of war in various ways. It is rather to argue that scholars should become more involved in research on European perspectives on cyber conflict short of war on the one hand, and European governments should strive to clarify the strategic consequences of continuous cyber conflict short of war, on the other. Both scholars and politicians need to engage with the security, political and democratic difficulties related to countering adversarial cyber hostilities short of war. This is not to say that European countries should blindly adopt the American strategy of persistent engagement and defending forward. They should, however, move beyond the current standstill and design strategic solutions to prevent, discourage, and respond to continuous cyber incidents short of war. In conclusion, the paper suggests three avenues for future scholarly and policy conversation on how European countries can accomplish this goal and fill this strategic vacuum. These suggestions are neither exhaustive, a panacea nor an argument for a one-size-fits-all European strategic approach. Based on the premise of a changing strategic environment in which cyber conflict short of war forms a fundamental part of strategic competition, they offer basic propositions for policy-makers and academics to engage.

First, European countries should define the problem to be solved, “as ambiguous terminology creates problems for distinguishing between different conceptions of strategy” (Hoffman [2019](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991), p. 133). They would benefit from operationalising cyber conflict short of war, unpack its core dynamics, and determine its strategic impact. At a macro-level, this includes elucidating whether cyber conflict short of war is an expression of fundamental strategic competition? Whether it taps into the intensified global technological competition, which includes control of internet infrastructure, power over international ICT supply chains and markets, global data flows, and innovation in emerging technologies?[21](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991) To what extent, if at all, cyber conflict short of war weakens the position of European countries in international politics?

At a meso-level, European countries should develop strategically guided frameworks for counter linked and coordinated cyber operations that accumulated over time do significant harm to European societies. In relation to this, European countries should clarify interagency competencies and processes to handle tensions between military and intelligence agencies. The analysis showed that inter-agency relations vary across countries: from a French separation model over a Dutch cooperation model to a Norwegian unity model. It furthermore demonstrated that challenges remain in developing operational and legal frameworks for the deployment of cyber capabilities at the intersection of the already indistinct and blurring categories of offence and defence, with consequences for escalation management and strategic stability (Buchanan [2016](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991)). Moreover, when formulating strategies European countries ought to consider the risk of exacerbating the tension between the stabilising effects of intelligence collection on international relations and the destabilising modes of its collection (Goie et al. [2020](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991)). At a micro-level, as part of developing such frameworks and interagency processes, European countries should consider establishing procedures for classifying and operationalising various forms of malicious cyber activity and formulating thresholds and trigger points. At all three levels, these are continuous efforts that are contingent on various factors counting developments in global politics, digital technologies, and strategic culture.[22](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991)

Second, national strategy building does not take place in a vacuum. European countries are involved in international cooperation engaging cyber conflict short of war in NATO,[23](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991) EU,[24](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991) and among the intelligence services.[25](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991) National strategy building should thus take place in conversation with allies and partners on how to strategise the involvement of military and intelligence entities in the increased cyber competition short of war. The significance of which was recently underlined by the 2021 NATO Brussels Summit Communique ([2021](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991), p. 10) stressing that “allies recognise that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack”. The development of a new Strategic Concept for NATO – to be done in time for the Madrid summit in June 2022[26](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991) – provides an excellent opportunity to formalise this conversation and increase NATO coordination on cyber strategy.

This broad conversation could focus on intelligence versus military norms and practices for cyberspace (see also Boeke and Broeders [2018](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991), Smeets [2020](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991), Jacobsen [2021](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991)). It might include discussions on establishing common and transparent vulnerability equities processes and decreasing the grey market trading by government agencies purchasing cyber weapon components (Christensen and Liebetrau [2019](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991), Perlroth [2021](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991)), working on creating a global governance framework for cyber weapons (Stevens [2018b](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991)), and enhancing the protection of global supply chain integrity and the public core of the internet (Broeders [2017](https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991)). Moving these discussions forward, European countries could boost norm-codification and progressive norm-making concerning cyber competition short of war with the shared goal of restoring confidence in a liberal rule-based order that can prove its relevance and avoid further poisoning of the global digital well.

Third, the present lack of transparent strategic approaches raises concerns about oversight and the democratic goal of fostering informed political and public debate. It is important to engage society in the deliberation on countering cyber conflict short of war, not least because citizens, private companies, and public authorities are often the victims of such cyber operations. Ensuring a continuous debate on the political and military framing of malign cyber operations and the opportunities to counter them is vital to democratic governance. The current situation thus demands greater transparency and debate about the deployment of cyber power – for all purposes including countering cyber hostilities short of war – across society from parliamentary scrutiny over oversight bodies to the media. The discussion on how to categorise, react, and respond to cyber hostilities short of war cannot entirely be left to military or intelligence authorities and experts. While the exact capabilities and tasks of intelligence and military cyber units are much likely to remain secret and classified, the increased acknowledgement of their existence needs to be supplemented with a targeted effort to increase transparency as well as public and political debate about their role in defence and foreign policy.

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

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

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

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

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

## AT: OCO’s Bad

### AT: OCOs Bad---2AC

#### The best studies prove that effective OCO’s deter conflicts --- Alternatives risk quick escalation

**Leuprecht et al. 19** – Professor at the Royal Military College of Canada and Queen's University, and Matthew Flinders Fellow at the Flinders University of South Australia Christian Leuprecht, Joseph Szeman, David B. Skillicorn, “The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity,” Contemporary Security Policy, Vol. 40, Issue 3, 2019, https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1590960

At a more strategic level, OCOs can be used to **constrain** or **enhance** the **effects** of **other capabilities** and **strategies**. Whether they can be used for deterrence, and whether the concept of deterrence is even meaningful under conditions of persistent attack, is a matter of controversy. OCOs have the advantage that **costs incurred** or **damage caused** to an adversary can be **controlled** so that it **falls short** of the **generally accepted level** of an **armed attack**, and can be even **reversible** (Owens et al., 2009). In his book about the Trump White House, Woodward (2018) comments that military advisers to the President were reluctant to recommend offensive cyberattacks against North Korea because they thought the U.S. itself was too poorly defended to withstand retaliatory cyberattacks, a nascent example of deterrence in the cyber domain. **To date**, **no direct use** of **OCO capabilities** has resulted in the **outbreak** of **traditional conflict**, perhaps owing to **uncertainties** in the **novelty** of the **attacks**, the **difficulty** of **attribution**, and the **reluctance** of **national cyber actors** to **retaliate** when the **path of escalation** is **unclear** (Rid & Buchanan, 2015). Most importantly, however, the actions of armed forces in democratic countries are **constrained** by the **rule of law**, which translates into **multiple authorities** to **ensure responsible** and **acceptable use**, and **safeguard against escalation**. The **fine-grained control** of **OCOs** compared to conventional military force provides a way to **manage escalation** without the **direct use** of physical or military assets, whose effect in sparking conflict is **much better known**. In other words, instead of reacting to an **escalating conflict** by **deploying physical military assets** to a region, an OCO can be **employed covertly** to **incur more controllable costs** on the adversary, with the benefit of **plausible deniability** (Hare, 2018). Depending on the type of OCO employed, if there is a reduction in tension, the **effects** of the OCO can be **reversed** or **scaled back**.

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

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

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

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

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

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

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

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

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

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

Deterrence-in-kind: developing offensive cyber capabilities

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

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

Limnéll 13 – Professor of Cybersecurity, Aalto University, Finland

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

Offensive Weaponry is Required for Credibility and Deterrence

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

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

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

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

## T

### 2AC---Includes Info Sharing

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

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

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

## AT: NSA DA

### UQ---Split Now---2AC

#### Biden’s splitting CYBERCOM from the NSA now.

Greg Hadley 3/18, Congressional editor of Air Force Magazine, 3/18/2022, “Biden Administration Considers Splitting NSA, CYBERCOM,” <https://www.airforcemag.com/biden-administration-considers-splitting-nsa-cybercom/>, cc

President Joe Biden’s administration and the Defense Department are looking at the possibility of splitting up control of U.S. Cyber Command and the National Security Agency, reviving a long-running debate over how the two organizations are led.

Since the stand-up of CYBERCOM in 2009, its commander has functioned in a dual-hat role as the director of the NSA, an arrangement meant to help the new combatant command get off the ground. Gen. Paul M. Nakasone currently holds both titles.

For years now, lawmakers, analysts, and DOD officials have debated when or even if to separate the two positions. In December 2020, then-President Donald Trump’s administration delivered a proposal to split the leadership roles, only for the plan to be rejected as officials said CYBERCOM had not met the conditions to do so required by law, according to The Washington Post.

The issue came up again March 17 in a hearing before the House Armed Services intelligence and special operations subcommittee, as Rep. Don Bacon (R-Neb.) asked Ronald S. Moultrie, undersecretary of defense for intelligence and security, for his view on the potential change.

“I would say that from a Department of Defense perspective, we certainly recognize the value of the dual-hat role that Gen. Nakasone has played for the last four years and the role of Cyber Command and NSA over the last 12 years plus,” Moultrie said.

“I believe that the dual hat will be looked at again, just by this administration, just to ensure that we understand what the value added is, but also what the impacts are. And so that discussion is still ongoing within the department today. We understand that there’s a sentiment on both sides to really not do any harm. But I believe that it will be looked at. I think it’ll be an objective look, and we’ll make sure we reach out to you, sir.”

### Link---Normal Means---2AC

#### The NSA can serve as an implementing agency for the plan.

DSCA 21, Defense Security Cooperation Agency, carries out all security cooperation, 10/01/2021 (carbon dated), “THE SECURITY COOPERATION ENTERPRISE,” <https://www.dsca.mil/50th-anniversary/the-security-cooperation-enterprise>, cc

The Military Departments (MILDEPs) advise the Secretary of Defense on all SC matters for their respective departments. The MILDEPs also execute foreign sales and training as Foreign Military Sales (FMS) “Implementing Agencies” (IAs):

Office of the Deputy Assistant Secretary of the Army for Defense Exports and Cooperation (DASA (DE&C)) provides policy oversight for international affairs functions, including FMS.

U.S. Army Security Assistance Command (USASAC) provides management oversight of Army SC programs.

Office of the Deputy Assistant Secretary of the Navy (International Programs) (Navy IPO) provides policy oversight of Navy, Marine Corps, and Coast Guard SC Programs.

Office of the Deputy Under Secretary of the Air Force, International Affairs (SAF/IA), provides policy oversight for all Air and Space Force SC programs.

Air Force Security Assistance Command (AFSAC) provides management oversight for all Air Force SC programs.

Other organizations which serve as IAs include the National Geospatial-Intelligence Agency (NGA), the Defense Logistics Agency (DLA), the Missile Defense Agency (MDA), and the National Security Agency (NSA).

#### CYBERCOM legally can’t execute security cooperation.

Robert Chesney 18, the Charles I. Francis Professor in Law and Associate Dean for Academic Affairs at the University of Texas School of Law and serves as the Director of UT-Austin's interdisciplinary research center the Robert S. Strauss Center for International Security and Law, 4/12/2018, “Title 10 and Title 50 Issues When Computer Network Operations Impact Third Countries,”’ <https://www.lawfareblog.com/title-10-and-title-50-issues-when-computer-network-operations-impact-third-countries>, cc

Does Title 10 impose a legal barrier on U.S. Cyber Command conducting operations outside of the Pentagon’s own networks?

That’s the question raised earlier this week by this story from Chris Bing at Cyberscoop (an increasingly interesting site), which builds on recent congressional testimony from Admiral Rogers. The story depicts a “quiet but constant tug of war … between the intelligence community and the military over the future of government—backed hacking,” with the central issue concerning the allocation of lead responsibility for conducting computer network operations outside the government’s own systems in order to “strike back at foreign targets.” More specifically, the story depicts something of a turf war between NSA and an increasingly independent CYBERCOM (highlighting a number of key themes, including the inherent challenge of balancing intel collection equities against the interest in having disruptive effect on some targets; on that point, read all the way to the bottom for spot-on observations from Jamil Jaffer of George Mason).

Critically, the story suggests that Title 10 and Title 50 concerns also are impacting this debate. I thought I include a brief note here to shed light on what that might mean.

The article observes that “[w]hen military leaders push to do more with hackers, they usually meet some form of resistance from Pentagon lawyers.” By way of illustration, the article points to an instance in which CYBERCOM operators deleted ISIS propaganda off a server that happened to be located in Germany. The Germans apparently were notified of the operation in some fashion but not asked for advance consent, and they were not happy about it.

From a legal perspective, the issue this highlights is that operations abroad implicate the UN Charter and related claims about international law protection of sovereignty. So how does this become part of the Title 10/Title 50 debate? Intelligence agencies can more easily act in this setting when operating under Title 50 authority, as covert action status carries with it a statutory obligation to comply with the U.S. Constitution and U.S. statutes—but no more than that. Title 10, in contrast, carries with it no such implicit statutory shield against international law objections, and of course there is a general Defense Department policy of international law compliance. Thus CYBERCOM operating under Title 10 would run into the full thicket of international law concerns. There may be good and sufficient answers to those concerns in particular cases—so this should not be understood as an absolute bar—but it does make sense to say that the legal friction is greater in that setting (that is, operations with effects on servers in third countries and without consent from those countries) than it would be for an entity acting under color of Title 50.

### Link---Normal Means---AT: Title 10---1AR

#### The distinction between Title 10 and Title 50 is meaningless.

Andru Wall 11, Senior Associate with Alston & Bird LLP; former senior legal advisor for U.S. Special Operations Command Centra, 12/2/2011, “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action,” <https://www.soc.mil/528th/PDFs/Title10Title50.pdf>, cc

Read in concert with Title 10, Title 50 does not infringe upon the Secretary of Defense’s authorities to collect intelligence. Rather, Title 50 recognizes the authorities assigned to the Secretary of Defense under Title 10 over all DoD intelligence activities, and adds Title 50’s provisions regarding Congressional oversight to intelligence activities conducted primarily by DoD personnel in support of or in furtherance of tasking from the Director of National Intelligence (DNI) (as opposed to tasking from the Secretary of Defense).

Thus, Title 10 and Title 50 are mutually-reinforcing authorities, not mutually-exclusive authorities; these statutory authorities may even be exercised simultaneously by personnel under the command and control of the Secretary of Defense. Labeling some intelligence activities “Title 50” activities while labeling similar activities “Title 10” activities creates a distinction where the law does not. Importantly, the statutes make distinctions based on direction, control, and funding—not on nomenclature.

### Thumper---Ukraine---2AC

#### Ukraine thumps.

Colin Demarest 4/7, reporter at C4ISRNET, where he covers military networks, cyber and IT, 4/07/2022, “US Cyber Command reinforces Ukraine and allies amid Russian onslaught,” <https://www.c4isrnet.com/cyber/2022/04/07/us-cyber-command-reinforces-ukraine-and-allies-amid-russian-onslaught/>, cc

WASHINGTON — U.S. Cyber Command has played a pivotal role in shielding networks and critical infrastructure stateside and abroad in the run up to and during Russia’s attack on Ukraine, its leader told Congress this week.

Along with tasking teams with identifying cyber vulnerabilities and threats — operations that have since “bolstered the resilience of Ukraine” and others — the command has gleaned and shared intelligence, worked hand-in-glove with U.S. government and industry, and pursued extensive contingency planning, Gen. Paul Nakasone said April 5.

“In conjunction with interagency, private sector and allied partners, we are collaborating to mitigate threats to domestic and overseas systems,” he continued in written testimony provided to the Senate Armed Services Committee.

In Ukraine, specifically, Cyber Command has provided remote analytic support and conducted network defense activities, Nakasone testified. The general is also the director of the National Security Agency.

### Turn---Leaks---2AC

#### Amity between the NSA and CYBERCOM leads to leaks of sensitive material.

James Di Pane 19, Policy Analyst, Defense Policy, Center for National Defense, 5/02/2019, “Should Cyber Command and the NSA Have Separate Leadership? How to Decide,” <https://www.heritage.org/defense/report/should-cyber-command-and-the-nsa-have-separate-leadership-how-decide>, cc

The third concern is the increased potential for exposure of NSA tools and operations. Maintaining the secrecy of the NSA’s cyber tools is one of the highest priorities of the organization. Because the NSA shares its hacking tools with Cyber Command, the frequency of use for these tools has increased, leading to a correlating increased chance of release. This does not necessarily stem from the dual-hat relationship, but more from Cyber Command’s close relationship with the NSA for support.

### CMR D---2AC

#### CMR collapse is academic garbage.

Dunlap 17 Former Major General Charles J. Dunlap, a Duke Law Professor with a focus on security and civil-military relations after retiring from the Air Force. [Let’s Temper the Rhetoric About Civil-Military Relations, Dec 15, 2017, https://smallwarsjournal.com/jrnl/art/lets-temper-rhetoric-about-civil-military-relations]//BPS

The military is hardly as homogenous in its views as many narratives would have you believe. According to a poll from last fall, it is true that the military in general is more supportive of the commander-in-chief than the general public, but the officer corps is rather similar to the public in its opinion of the commander in chief. Furthermore, my bet is that some critics would be surprised to know that members of the military (30 percent) label white nationalists as posing a significant danger, “more than many international hot spots, like Syria (27 percent), Pakistan (25 percent), Afghanistan (22 percent) and Iraq (17 percent).” Regardless, there is nothing inherently evil or unprofessional about belonging to a political party. Personally, I’ve always been a registered independent, but I never questioned someone’s professionalism simply because in their private life chose to identify with a political party on voter rolls. In fact, one could easily argue that it is healthy for a democracy when the members of its armed forces to remain connected in a lawful way to political discourse. Of course, maintaining the appearance of non-partisanship can be complicated when, for example, a non-military spouse becomes active in partisan politics, but that is an issue not confined to the military, but to other professions in American society (see e.g., here and here). In any event, nobody should assume that simply because someone has not registered with a party or, for that matter, voted, that they have no opinion about political issues, to include partisan ones. Likewise, are we to assume that simply because someone registers a party membership they will, ipso facto, be partisan in the execution of their professional duties? That certainly is not what I’ve observed, and not just among military professionals. Judges are only one example of professional who may hold distinctly partisan views, but who nevertheless regularly set them aside (hopefully) and conduct themselves impartially in the courtroom and in their formal opinions. Military professionals in particular are routinely called upon to compartmentalize their personal views when performing their official duties so as to insulate themselves from inappropriate decision-making. For example, Roman Catholics comprise the largest faith group in the military, but they are required to operate in an environment where key tenets of their religion---such as opposition to gay marriage and abortion---cannot be allowed to compromise their official actions. Additionally, military leaders in combat especially must mentally sequester their personal feelings, such as their affection for their troops if that affection could compromise the paramount responsibility to the security of the nation as a whole. This is because the warfighting mission necessitates leaders sending them into situations where it is inevitable some will be killed or injured. When leaders find they are not able to handle the unavoidable sacrifice of their troops in order to protect the country, the best realize it’s time to leave the profession. This is precisely what happened to then Marine major Nate Fick. As he recorded his reason for leaving the Marine Corps in his magnificent memoir, One Bullet Away: The Making of a Marine Officer, Fick said: “Great Marine commanders, like all great warriors, are able to kill that which they love most---their men. It’s a fundamental law of warfare. Twice I had cheated it. I couldn’t tempt fate again.” Setting aside one’s political druthers is a vastly less demanding decision than the one Fick wrestled with, and most military professionals do so instinctively. An illustration: I deployed for Operation Desert Fox which was in the midst of Congressional efforts to impeach Bill Clinton. Despite the uncertainty of Clinton’s future, as well as his unpopularity in the military, the orders he gave to send servicemembers into harms’ way were obeyed without question (even as some say the operation was concocted to distract attention from the impeachment scandal). Claiming a “crisis” in civil-military relations as the title to Matt’s essay suggests is a perennial favorite among academics and pundits. Almost 25 years ago Dick Kohn virtually founded the “crisis” school of civil military relations with his eponymous essay Out of Control: The Crisis in Civil-Military Relations. The intellectual problem? The crisis never materialized. Instead, we’ve seen a military that has, despite all sorts of pressures through administrations of both parties, remained dutifully adherent to the Constitution.

#### Political influence thumps.

Risa Brooks 21, Allis Chalmers Associate Professor of Political Science at Marquette University; Jim Golby, Senior Fellow at the Clements Center for National Security at the University of Texas at Austin; and Heidi Urben an Adjunct Associate Professor in Georgetown University’s Security Studies Program, “Crisis of Command,” <https://www.foreignaffairs.com/articles/united-states/2021-04-09/national-security-crisis-command>, cc

Of course, senior military leaders do not always get everything they want, but they often get more than they should. Their power also extends beyond headline-grabbing decisions about overseas deployments or troop reductions. The military’s influence manifests hundreds of times a day through bureaucratic maneuvers inside the Pentagon, in policy discussions in the White House, and during testimony on Capitol Hill. These mundane interactions, perhaps more than anything else, steer decision-making away from civilians in the Office of the Secretary of Defense and toward uniformed personnel. Inside the Pentagon, for instance, military leaders often preempt the advice and analysis of civilian staff by sending their proposals straight to the secretary of defense, bypassing the byzantine clearance process that non-uniformed staffers must navigate.

There are signs of the erosion of civilian control outside the Pentagon, as well. Congress too rarely demands that the military bow to civilian authority, instead weighing in selectively and for partisan reasons. During the Obama administration, for example, some commentators and at least one member of Congress suggested that Martin Dempsey, the chairman of the Joint Chiefs of Staff, should resign in protest over the president’s management of the campaign to defeat the Islamic State, also known as ISIS. The goal was to use Dempsey’s role as the president’s chief military adviser as leverage in a partisan battle over Obama’s foreign policy. Under Trump, many Democrats cheered on the retired and active-duty generals who pushed back against the president’s decisions. These “adults in the room” included James Mattis (the secretary of defense), John Kelly (the secretary of homeland security and then White House chief of staff), and H. R. McMaster (Trump’s national security adviser). At the extreme, some of Trump’s opponents even urged senior military leaders to contemplate removing Trump from office. In August 2020, two well-known retired army officers, John Nagl and Paul Yingling, penned an open letter to Mark Milley, the chairman of the Joint Chiefs of Staff, telling him to do just that if the president refused to leave office after losing the 2020 election. Although these efforts may have comforted those concerned about Trump’s erratic policies, they undermined civilian control by suggesting that it was the military’s job to keep the executive in check. When politicians endorse military insubordination that serves their interests, they do long-term damage to the principle of civilian primacy.

### CMR D---1AR

#### The narrative is a partisan ruse.

Dunlap 17 Former Major General Charles J. Dunlap, a Duke Law Professor with a focus on security and civil-military relations after retiring from the Air Force. [Let’s Temper the Rhetoric About Civil-Military Relations, Dec 15, 2017, https://smallwarsjournal.com/jrnl/art/lets-temper-rhetoric-about-civil-military-relations]//BPS

Let’s pose the issue a little differently. Are “dire” fears about the military profession as a whole really supported by a study that shows that despite today’s extraordinarily divisive political environment, two-thirds of West Point cadets and National Defense University colonels had nonetheless not observed or shared any insulting, rude, or disdainful comments about elected leaders? The reality is that however regrettable such commentary may be, it’s occurred within the ranks throughout our history (and especially during the Revolution and the Civil War)…yet the Republic has not suffered “dire” consequences. In truth, in a democracy that treasures free speech, there is a limit to the wisdom of trying to suppress every untoward remark that someone in uniform might make about an elected leader. This may be one reason why Article 88 of the Uniform Code of Military Justice (which criminalizes “contemptuous language” by officers about certain elected officials) is so limited, and why the Manual for Courts-Martial counsels that “if not personally contemptuous, adverse criticism of one of the officials or legislatures named in the article in the course of a political discussion, even though emphatically expressed, may not be charged as a violation of the article.” Do we have issues that bear watching about civil-military relations? Absolutely! As I explained at the Army War College Strategy conference recently, I believe that technology---particularly social media, big data, and even neuroscience---could operate to change not only how military leaders relate to their subordinates and the public, but also to change society itself. The “civil” of civil-military relations may evolve into an entity that is markedly different from today, and this could---and probably will---impact civil-military relations. But all that is quite different from the perils Matt sees. To be crystal clear, we certainly do have work to do, but excitedly proclaiming that we are on the cusp of “dire consequences” unhelpfully overstates and, even worse, obfuscates the real issues. In fact, over-hyping issues in civil-military relations plays into partisan politics. How? Consider that journalist Ross Douthat observed in the New York Times recently that the US won a great victory over ISIS, but “nobody seemed to notice.” Douthat cites a number of reasons for the lack of attention, but most interesting is this: But this is also a press failure, a case where the media is not adequately reporting an important success because it does not fit into the narrative of Trumpian disaster in which our journalistic entities are all invested. In other words, conjuring up impending apocalypse in civil-military relations can become another weapon which, whether intended or not, may be used by critics invested in the “narrative of Trumpian disaster” to try to delegitimize an area in which the Administration has enjoyed, as Douhet points out, some undeniable success: national security. Addressing the perennial challenges of civil-military relations isn’t facilitated when they get wrapped up with political narratives about specific individuals.

### NC3 D---2AC

#### No NC3 impact.

Erica Lonergan 22, 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; and Keren Yarhi-Milo, the Arnold A. Saltzman Professor of War and Peace Studies in the political science department and the School of International and Public Affairs and the director of the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University, 4/21/2022, “CYBER SIGNALING AND NUCLEAR DETERRENCE: IMPLICATIONS FOR THE UKRAINE CRISIS,” <https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/>, edited for ableist language, cc

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~~ [destroy] 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.

### NC3 D---1AR

#### NC3s are disconnected from the Internet.

Futter ’16 [Andrew; 2016; International Politics Professor at the University of Leicester; “War Games Redux? Cyberthreats, US–Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control,” European Security 25(2), p. 171-172]

It is of course highly unlikely that either the USA or Russia has plans – or perhaps more importantly, the desire – to fully undermine the other’s nuclear command and control systems as a precursor to some type of disarming first strike, but the perception that nuclear forces and associated systems could be vulnerable or compromised is persuasive. Or as Hayes (2015) puts it, “The risks of cyber disablement entering into our nuclear forces are real”. While the growing possibility of “cyber disablement” should not be overstated (notions of a “cyber-Pearl Harbor” (Panetta 2012) or “cyber 9–11” (Charles 2013) have done little to help understand the nature of the challenge), cyberthreats are nevertheless an increasingly important component of the contemporary US–Russia strategic context. This is particularly the case when they are combined with other emerging military-technical developments and programmes. The net result, especially given the current downturn in US–Russian strategic relations, and the way cyber is exacerbating the impact of other problematic strategic dynamics, is that is seems highly unlikely that either the USA or Russia will make the requisite moves to de-alert nuclear forces that the new cyber challenges appear to necessitate, or for that matter to (re)embrace the “deep nuclear cuts” agenda any time soon.

Assessing the options for arms control and enhancing mutual security

Given the new challenges presented by cyber to both US and Russian nuclear forces and to US–Russia strategic stability, it is important to consider what might be done to help mitigate and guard against these threats, and thereby help minimise the risks of unintentional launches, miscalculation, and accidents, and perhaps create the conditions for greater stability, de-alerting, and further nuclear cuts. While there is unlikely to be a panacea or “magic bullet” that will reduce the risk of cyberattacks on US and Russian nuclear forces to zero – be they designed to launch nuclear weapons or compromise the systems that support them – there are a number of options that might be considered and pursued in order to address these different types of threats and vulnerabilities. None, of these however, will be easy.

The most obvious and immediate priority for both the USA and Russia is working (potentially together) to harden and better protect nuclear systems against possible cyberattack, intrusion, or cyber-induced accidents. In fact, in October 2013 it was announced that Russian nuclear command and control networks would be protected against cyber incursion and attacks by “special units” of the Strategic Missile Forces (Russia Today 2014). Other measures will include better network defences and firewalls, more sophisticated cryptographic codes, upgraded and better protected communications systems (including cables), extra redundancy, and better training and screening for the practitioners that operate these systems (see Ullman 2015). However, and while comprehensive reviews are underway to assess the vulnerabilities of current US and Russian nuclear systems to cyberattacks, it may well be that US and Russian C2 infrastructure becomes more vulnerable to cyber as it is modernised and old analogue systems are replaced with increasingly hi-tech digital platforms. As a result, and while nuclear weapons and command and control infrastructure are likely to be the best protected of all computer systems, and “air gapped”14 from the wider Internet – this does not mean they are invulnerable or will continue to be secure in the future, particularly as systems are modernised or become more complex (Fritz 2009). Or as Peggy Morse, ICBM systems director at Boeing, put it, “while its old it’s very secure” (quoted in Reed 2012).

### Terror D---2AC

#### Terrorism isn’t existential.

Walt 16 – Stephen M. Walt, international relations professor at Harvard University. [My Top 5 Foreign-Policy Unicorns — and Why I Want to Kill Them, 9-8-2016, https://foreignpolicy.com/2016/09/08/my-top-5-foreign-policy-unicorns-and-why-i-want-to-kill-them/]

3. The terrorist mastermind. A close cousin to the nuclear rogue is the terrorist mastermind, busily concocting elaborate and highly destructive plots to bring the world to its knees. People like Osama bin Laden and Islamic State leader Abu Bakr al-Baghdadi have made extravagant and dire threats, but the good news is that they’ve never come close to toppling a foreign government, winning millions of followers, or threatening our way of life. I don’t deny that some terrorist groups have devised and executed successful assaults — of which the 9/11 attacks were by far the most damaging — but a word like “mastermind” conjures up images of Dr. Evil-style villains who will inevitably outwit our feeble efforts to stop them and unleash fearsome destruction on an innocent world. In fact, as John Mueller and others keep reminding us, the vast majority of contemporary terrorists are incompetent misfits, and even the very best of them fall well short of evil genius. They can and do stage small-scale attacks that cause modest amounts of harm, but they have repeatedly shown themselves to be incapable of orchestrating complicated operations that could actually bring a stable country to its knees. There have been serious terrorist attacks in Boston; London; Paris; Brussels; Orlando, Florida; and several other places in recent years, for example — yet in each case, these societies proved resilient, and they are thriving again today. Or just look at New York City, which suffered the worst single attack ever and has since fully recovered. Terrorism is a problem, the lives lost to it are an unfortunate tragedy, and those who employ it are dangerous criminals. A few terrorists are moderately clever; most are not. None rises to the level of a “mastermind,” and none poses an existential threat. Reporters, pundits, and speechwriters should drop this term from their lexicon, because this particular animal doesn’t exist. Fortunately.

### Terror D---1AR

#### Security systems don’t work, BUT that doesn’t matter because terrorists are incompetent.

Mueller and Stewart, 18—Woody Hayes Senior Research Scientist, Mershon Center for International Security Studies, and adjunct professor of Political Science, at Ohio State University AND Professor of Civil Engineering and Director of the Centre for Infrastructure Performance and Reliability at The University of Newcastle (John and Mark, “Terrorism and Bathtubs: Comparing and Assessing the Risks,” Terrorism and Political Violence, October 29, 2018, dml) [ableist language modifications denoted by brackets]

There may also be something of a grand or ultimate deterrent at work, but it has little to do with security measures. Although one shouldn’t give most terrorists all that much credit for careful and especially for long-term thinking, that terrorism is such a rare phenomenon in the developed world may derive at least in part from the fact that terrorism simply doesn’t recommend itself as a course of practical political action because of the futility and fundamental absurdity of the enterprise. In general, in fact, it tends to be counterproductive.37 Maybe at least a few terrorists have figured that out and have given up early. That there is so little terrorism, then, is not because of the efficacy of security measures or because it is so difficult to pull off—lucrative targets are ubiquitous and headlinegrabbing mayhem is easy to commit. To a considerable degree, terrorism is rare because terrorists, unlike bathtubs, don’t exist. As Bruce Schneier puts it bluntly, “there isn’t much of a threat of terrorism to defend against.” 38

### Democracy D---2AC

#### Democracy solves nothing.

Renske Doorenspleet 19, Political Science and International Studies Professor at Warwick University, “Democracy and Interstate War,” Chapter 3 of *Rethinking the Value of Democracy: A Comparative Perspective*, Stras

There is actually more evidence for the idea that the liberal norms lead to more (not less!) violence. Bear Braumoeller (1997), for example, argued that liberal norms of conflict resolution vary because liberalism takes many forms. By examining survey results from the newly independent states of the former Soviet Union, he showed that liberalism in that region bears a stronger resemblance to nineteenth-century liberal nationalism than to the sort of universalist, Wilsonian liberalism described by democratic peace theorists. As a result, liberals in the region are more, not less, aggressive than non-liberals. Carol Fair and her colleagues (Fair et al. 2014) came to similar conclusions. They conducted surveys in Pakistan (with 6000 respondents) and found that strong supporters of democratic values are actually not less but more supportive of militant groups. Moreover, it seems that individuals’ attitudes towards war are shaped by core beliefs about revenge, which vary across countries. Democracies with a strong tradition to support ideas of revenge24 are significantly more likely to initiate conflicts (Stein 2015). We cannot state that people in democracies are not belligerent. These results challenge the conventional wisdom about the roots of militancy and the existence of universal democratic norms, which would encourage peace.

Some scholars have argued that not the liberal democratic norms, but market-oriented development creates the norms and values that explain the democratic peace (see, e.g., Mousseau 2000). When opportunities to come to a deal in the market are widespread, as in market-oriented developed countries, a culture of contracting emerges that encourages shared respect for individualism, negotiations, compromise, respect for the law and equality before the law. Constrained by voters, democratically elected leaders in market-oriented developed countries abide by these norms. In contrast, voters in democracies without developed market economies, and the leaders in nondemocracies, have other norms and values that encourage conflict.

Hence, there is not only a lack of statistical studies, but also most findings do not support the ideas of the so-called democratic norms argument. Moreover, it is not clear why the pacifist attitude of citizens is ‘only evident in cases of democratic adversary’, while this is not the case when there are conflicts with nondemocracies, colonial expansion or third-party interventions (Gates et al. 1996: 5–6). Finally, this kind of argument tends to be tautological, stating that ‘relations between democratic states are peaceful because they are informed by a common perception that democracies are peaceful’ (Gates et al. 1996: 5–6).25

### Democracy D---1AR

#### Norms are tautological and impossible to measure.

Doorenspleet 19 – Renske Doorenspleet, Politics Professor at the University of Warwick. [Rethinking the Value of Democracy: A Comparative Perspective, Palgrave Macmillan, p. 85-86]

There are only few statistical studies focusing on this argument of norms. Zeev Maoz and Bruce Russett (1993) defended this idea and stated that they found evidence, but their measure is very weak and lacks validity. They employed two measures of the prevalence of democratic norms. The first is through the concept of political stability, the persis¬tence of the political system in years. The second is through the amount of political violence within a state, which is measured by the number of deaths from political violence and extent of domestic conflict. In my view, those measures do not really measure 'democratic norms' but simply 'political stability and violence'. Other studies have focused on conflict management as proxy for democratic norms. William J. Dixon (1994), for example, discovered that democratic systems are better at conflict management. Democratic opponents are significandy more likely to reach peaceful settlements than other types of disputants. In addition, in disputes between democra¬cies, mediation is more likely to be pursued (Inman et al. 2014; see also Dixon 1993). Those scholars argued such outcomes supported the dem¬ocratic norms argument, but eventually they do not directly measure this concept. Moreover, the existence of democratic norms apparently did not stop the democracies to go war in the first place. Within this approach of democratic norms, other scholars stated that greater support for core liberal values leads to a rejection of destruc¬tive political activities and reduced support for violent politics. People in democracies are less aggressive, the argument goes, which could help understand the assumed existence of democratic peace. Analyses of public opinion surveys showed that American and British people are somewhat more inclined to use force against dictatorships than against democracies (Johns and Davies 2012), but the effect is very small, and it is unclear why this is the case. There is actually more evidence for the idea that the liberal norms lead to more (not less!) violence. Bear Braumoeller (1997), for example, argued that liberal norms of conflict resolution vary because liberalism takes many forms. By examining survey results from the newly independ¬ent states of the former Soviet Union, he showed that liberalism in that region bears a stronger resemblance to nineteenth-century liberal nation¬alism than to the sort of universalist, Wilsonian liberalism described by democratic peace theorists. As a result, liberals in the region are more, not less, aggressive than non-liberals. Carol Fair and her colleagues (Fair et al. 2014) came to similar conclusions. They conducted surveys in Pakistan (with 6000 respondents) and found that strong supporters of democratic values are actually not less but more supportive of militant groups. Moreover, it seems that individuals' attitudes towards war are shaped by core beliefs about revenge, which vary across countries. Democracies with a strong tradition to support ideas of revenge24 are significantly more likely to initiate conflicts (Stein 2015). We cannot state that people in democracies are not belligerent. These results challenge the conventional wisdom about the roots of militancy and the existence of universal democratic norms, which would encourage peace. Some scholars have argued that not the liberal democratic norms, but market-oriented development creates the norms and values that explain the democratic peace (see, e.g., Mousseau 2000). When opportunities to come to a deal in the market are widespread, as in market-oriented developed countries, a culture of contracting emerges that encourages shared respect for individualism, negotiations, compromise, respect for the law and equality before the law. Constrained by voters, democrat¬ically elected leaders in market-oriented developed countries abide by these norms. In contrast, voters in democracies without developed mar¬ket economies, and the leaders in nondemocracies, have other norms and values that encourage conflict. Hence, there is not only a lack of statistical studies, but also most findings do not support the ideas of the so-called democratic norms argument. Moreover, it is not clear why the pacifist attitude of citizens is 'only evident in cases of democratic adversary', while this is not the case when there are conflicts with nondemocracies, colonial expansion or third-party interventions (Gates et al. 1996: 5-6). Finally, this kind of argument tends to be tautological, stating that 'relations between democratic states are peaceful because they are informed by a common perception that democracies are peaceful' (Gates et al. 1996: 5-6).23

### Cyberwar D---2AC

#### Cyberattacks are bearable AND dwarfed by squirrel sabotage.

John Mueller 22, Adjunct Professor of Political Science, Ohio State University; Senior Fellow, Cato Institute, 3/22/2022, “The Cyber-​Delusion,” <https://www.cato.org/commentary/cyber-delusion>, cc

This contemporary approach to cyberthreats resembles the aftermath of 9/11, when almost all experts believed an even larger terrorist attack would soon take place. Then, as now, the threat is overblown. Although occasionally dramatic, cyberattacks have turned out to be a comparatively minor and manageable threat. Far too much discussion around the issue focuses on worst-​case scenarios, fails to contextualize the problem, and neglects to weigh the costs of cyberattacks against the enormous value of the Internet and artificial intelligence. Most commentary, moreover, does not fully appreciate the ability of the business sector—by far the most tempting of targets for malevolent hackers—to develop effective countermeasures.

Cyberwar

If a system is resilient, even successful, dramatic, and dastardly surprise attacks can be managed.

Over the past decade, the global obsession with digital threats has taken various forms, with a particular focus on the potential military implications of emerging cyber-​capabilities. To be sure, the military needs to worry about keeping its communications and command and control operations secure from hostile attackers. Any disruptions, however, are more likely to be instrumental or tactical than strategic.

Despite statements to the contrary, the U.S. military itself seems to have recognized this reality. When Panetta proclaimed in 2013 that cyber was “without question, the battlefield for the future,” political scientist Micah Zenko observed at the time that the Pentagon was spending less than one percent of its budget on cybersecurity, and an assessment from 2019 suggests it may be more like one-​tenth of one percent. If those funds prove adequate for the challenge, it would be something of a bargain.

Cyber also supposedly enhances a state’s ability to carry out such ancient endeavors as espionage, propaganda dissemination, and sabotage. Analysts have even coined a new term, “hybrid warfare,” that usually includes these three enterprises—although, since the term does not include direct armed conflict, it might more plausibly be called “denatured warfare.” Cyber’s contribution to these three areas, however, is relatively limited.

Should invading hackers engage in digital espionage against the United States, for instance, they are likely to find that most of what they come across is already well known, and that much of the rest is not worth knowing in the first place. Wikileaks’ 2010 publication of thousands of classified U.S. government documents demonstrated the degree to which governments worldwide have fallen victim to over-​classification. When Bill Keller, the editor in charge of poring over the documents at The New York Times, was asked whether the reporting team found anything they didn’t already know, he responded “no” without hesitation.

Much the same holds for concerns over the theft of intellectual property. Not only is this practice centuries old, but systematic stealing has often proved unwise because it distracts governments from homegrown innovation. Cyber-​propaganda efforts, in turn, are more likely to increase the overall amount of available information and disinformation—an age-​old problem in warfare—than to provide a decisive advantage.

The achievements of cyber-​sabotage have also been quite modest. The United States and Israel famously used a computer virus known as Stuxnet to hamper Iran’s progress toward developing a nuclear weapon. Although observers hailed the operation as a dangerous new development in modern conflict, the damage proved temporary. Iran quickly rebuilt its centrifuges, and the attack actually proved counterproductive, as it encouraged Tehran to accelerate its nuclear program. There have also been efforts by the United States to physically interfere with missile development in North Korea. Yet, much like the Iranians, Pyongyang eventually solved whatever the problem was, and the attacks had little long-​term effect on their program.

Cyber-​alarmists have also warned about hackers disabling major infrastructure such as power grids—potentially crippling entire countries. Grids do go down occasionally, but the culprits are typically squirrels and lightning. Regardless of the source, such disruptions are usually brief and bearable, and engineers are increasingly designing systems that are resilient to such threats. Estonia, for instance, the victim of a major and oft-​discussed cyberattack in 2007, is now the home of NATO’s Cooperative Cyber Defence Centre of Excellence.

### Cyberterror D---2AC

#### Cyberterrorists are bums.

John Mueller 22, Adjunct Professor of Political Science, Ohio State University; Senior Fellow, Cato Institute, 3/22/2022, “The Cyber-​Delusion,” <https://www.cato.org/commentary/cyber-delusion>, cc

Fears that terrorist groups could inflict damage through cyberspace have been around for many years. And although cyber played no direct role in the execution of the 9/11 terrorist, the event stirred anxiety about the issue. In 2002, for instance, The Washington Post published a lengthy front-​page article conveying the views of “government experts” that “terrorists are at the threshold of using the Internet as a direct instrument of bloodshed.”

To date, however, no terrorist group has launched a successful cyberattack. And even if it becomes possible for hackers to shed blood, shootings and bombings are likely to accomplish the same goal far more reliably. Still, cyber has undoubtedly proved to be a relatively convenient method for terrorist groups to recruit and communicate. Rather than creating a paradigm shift, however, this technique has simply replaced or embellished older methods. Even comparatively savvy groups such as the Islamic State (also known as ISIS) tend to comically fail when using the Internet to stir up violence and instruct potential sympathizers. In one case, an ISIS handler connected his eager American charge to a prospective collaborator who happened to be an FBI operative.

For the most part, any virtual terrorist army in the United States has, as terrorism expert Brian Jenkins puts it, remained exactly that: virtual. “Talking about jihad, boasting of what one will do, and offering diabolical schemes egging each other on is usually as far as it goes,” he noted. Indeed, the foolish willingness of would-​be terrorists to describe their aspirations and often-​childish fantasies on the Internet has often helped police seeking to track them down.

### Cybercrime D---2AC

#### Resilience measures check cybercrime.

John Mueller 22, Adjunct Professor of Political Science, Ohio State University; Senior Fellow, Cato Institute, 3/22/2022, “The Cyber-​Delusion,” <https://www.cato.org/commentary/cyber-delusion>, cc

Despite the overheated rhetoric about war, terrorism, election interference, and critical infrastructure, most cyberattacks target the private sector, seeking to steal or extort money from businesses and their customers. The record here, however, is rather encouraging, and it likely has broader relevance. To be sure, cybercriminals have stolen and extorted billions of dollars from businesses and individuals, but firms have done well at limiting the damage by closing software holes, maintaining backups, and safeguarding sensitive material.

A central issue for potential hackers is the profitability of their enterprise. A report by the cybersecurity firm Symantec estimates that 978 million people were affected by cybercrime in 2017, losing $172 billion in total. That number—regardless of how hackers divvy up the profits—is actually remarkably small compared to losses from other forms of illegal activity. Personal and property crimes in 2017, for instance, cost Americans $2.6 trillion.

Businesses are also learning to adapt. Andrew Odlyzko, former head of the University of Minnesota’s Digital Technology Center, points out that many firms have realized they can readily mitigate the most damaging effects of cybercrime through minor and incremental alterations to their business practices. Banks, for instance, increasingly require customers to verify large or suspicious transactions through voice calls or texts. And even though criminals routinely capture millions of credit card numbers through compromised databases, the overall damage is limited and often dominated by the cost of providing replacement cards. Businesses have also made it easy for consumers to recover from fraud.

### Elections D---2AC

#### No impact to election hacking.

John Mueller 22, Adjunct Professor of Political Science, Ohio State University; Senior Fellow, Cato Institute, 3/22/2022, “The Cyber-​Delusion,” <https://www.cato.org/commentary/cyber-delusion>, cc

Election interference also features prominently in alarmist discourse on cyberthreats. During the 2016 U.S. presidential election, for instance, the United States highlighted apparent attempts by Russian hackers to undermine Hillary Clinton’s campaign. Although Clinton still handily won the popular vote, many analysts argued that digital interlopers sought to undermine the integrity of U.S. elections and perhaps democracy itself.

These warnings are exaggerated and—coming from U.S. policymakers—arguably hypocritical. It is worth noting that the United States has intervened in foreign elections for decades. Moreover, the idea that elections and voters are easily manipulated is suspect. If extensive promotion could guarantee success, Americans would all be driving Edsels and drinking New Coke—legendary marketing failures in 1958 and 1985 by two of the most successful businesses in history: the Ford Motor Company and Coca-​Cola. In any capitalist society, people are regularly deluged by advertising and marketing campaigns. In all cases, those petitioned remain free to ignore the ads, and most become quite good at it. In fact, studies have shown that campaign information rarely changes many votes. As political scientist Diana Mutz points out, the impact of campaign advertising “is marginal at most.”

Political campaigns, as anyone who has suffered through one knows, are also rife with falsehoods: incumbents strategically distort their record, and challengers do the same in reverse. The 2016 Russian contribution to this flood of misinformation was tiny. On Facebook, where most of the manipulation supposedly took place, Moscow’s intervention totaled perhaps a fraction one percent of the content on the platform’s news feed. Much of this was also wasted because the people who embraced it were already committed to a particular party or lived in states that went solidly for one or the other candidate. Russia’s efforts, moreover, proved wildly counterproductive. Instead of weakening U.S. policy, Moscow generated bipartisan support for anti-​Russian sanctions when the two U.S. political parties could agree on little else.

## AT Cybercom DA

### 2AC---Resources Infinite

#### CYBERCOM’s budget is ballooning AND the aff is priced in.

Mark Pomerleau 3/14, reporter for DefenseScoop, covering information warfare and cyberspace, 3/14/2022, “Cyber Command prepares to gain significant budget control,” <https://www.fedscoop.com/cyber-command-budget-control-preparations-pom/>, cc

U.S. Cyber Command is preparing to wield much greater budget control over major cyber programs, shifting funds away from the Army and Air Force programs that currently procure systems on behalf of the command and its forces.

The fiscal 2022 National Defense Authorization Act gave the commander of Cybercom responsibility for direct control and management of planning, programming, budgeting and execution of the resources to maintain the cyber mission force, an authority known as enhanced budget control.

Previously, the commander only had oversight of about $600 million from an overall Department of Defense IT budget of around $40 billion.

“The individual that runs a combatant command that’s responsible for defending the nation from significant cyberattack, defending the Department of Defense information networks and providing cyber capabilities to the other warfighting [combatant commands] … he’s got $600 million out of that topline $40 billion to $50 billion budget,” Lt. Gen. Charles Moore, deputy commander of Cybercom, said during the command’s legal conference March 10. “We have a significant mismatch in terms of the actual money, the authorities and the responsibility. We’re just trying to bring that back into alignment.”

With these new authorities set to take effect in 2024, the command is now working on its program objective memorandum, or POM, which sets fiscal plans for future years.

“We’re having to build our POM starting in 2024 and, of course, acquisitions. [That’s a] big part of what you’re going to need, what your requirements are, how are you going to POM for those types of activities,” Moore said.

In trying to bring the budget back into alignment, Moore said Cyber Command will focus on a variety of things including headquarters, subordinate headquarters, the cyber mission force and the elements of the Joint Cyber Warfighting Architecture (JCWA), which guides the command’s acquisition priorities.

Under this new paradigm, funding for major acquisition programs that the services were directing on behalf of the command will shift to Cybercom, although the services’ program executive offices and program managers will continue to execute the programs, a spokesperson said.

The elements of the JCWA include systems for command and control of cyber forces and the larger cyber environment, big data, training and executing offensive operations, among others. The Air Force and Army primarily run these programs, providing the funding and acquisition personnel to deliver them on behalf of the command.

Under the new model, funding for those programs will transfer to Cyber Command.

### 2AC---No Link---Normal Means

#### The NSA can serve as an implementing agency for the plan.

DSCA 21, Defense Security Cooperation Agency, carries out all security cooperation, 10/01/2021 (carbon dated), “THE SECURITY COOPERATION ENTERPRISE,” <https://www.dsca.mil/50th-anniversary/the-security-cooperation-enterprise>, cc

The Military Departments (MILDEPs) advise the Secretary of Defense on all SC matters for their respective departments. The MILDEPs also execute foreign sales and training as Foreign Military Sales (FMS) “Implementing Agencies” (IAs):

Office of the Deputy Assistant Secretary of the Army for Defense Exports and Cooperation (DASA (DE&C)) provides policy oversight for international affairs functions, including FMS.

U.S. Army Security Assistance Command (USASAC) provides management oversight of Army SC programs.

Office of the Deputy Assistant Secretary of the Navy (International Programs) (Navy IPO) provides policy oversight of Navy, Marine Corps, and Coast Guard SC Programs.

Office of the Deputy Under Secretary of the Air Force, International Affairs (SAF/IA), provides policy oversight for all Air and Space Force SC programs.

Air Force Security Assistance Command (AFSAC) provides management oversight for all Air Force SC programs.

Other organizations which serve as IAs include the National Geospatial-Intelligence Agency (NGA), the Defense Logistics Agency (DLA), the Missile Defense Agency (MDA), and the National Security Agency (NSA).

### 2AC---UQ---Ukraine

#### Ukraine thumps.

Colin Demarest 4/7, reporter at C4ISRNET, where he covers military networks, cyber and IT, 4/07/2022, “US Cyber Command reinforces Ukraine and allies amid Russian onslaught,” <https://www.c4isrnet.com/cyber/2022/04/07/us-cyber-command-reinforces-ukraine-and-allies-amid-russian-onslaught/>, cc

WASHINGTON — U.S. Cyber Command has played a pivotal role in shielding networks and critical infrastructure stateside and abroad in the run up to and during Russia’s attack on Ukraine, its leader told Congress this week.

Along with tasking teams with identifying cyber vulnerabilities and threats — operations that have since “bolstered the resilience of Ukraine” and others — the command has gleaned and shared intelligence, worked hand-in-glove with U.S. government and industry, and pursued extensive contingency planning, Gen. Paul Nakasone said April 5.

“In conjunction with interagency, private sector and allied partners, we are collaborating to mitigate threats to domestic and overseas systems,” he continued in written testimony provided to the Senate Armed Services Committee.

In Ukraine, specifically, Cyber Command has provided remote analytic support and conducted network defense activities, Nakasone testified. The general is also the director of the National Security Agency.

### 2AC---Link UQ---Cybersecurity

#### The DOD’s Cyber Command is already cracking down on ransomware.

Jaspreet Gill 4/28, reporter covering emerging technology and defense networks at Breaking Defense, 4/28/2022, “CYBERCOM increasing intel collection in light of Russia-Ukraine conflict,” <https://breakingdefense.com/2022/04/cybercom-increasing-intel-collection-in-light-of-russia-ukraine-conflict/>, cc

CYBERCOM has also had a pivot in the last year when it comes to thinking about ransomware, Kennedy said.

“I think about a year and a half ago if you had asked me what the…responsibility of the Department of Defense in ransomware was, [it] was purely in support of [the Department of Justice] and that activity is primarily a [law enforcement] activity,” Kennedy said. “What we’re finding, though, in recent times is that ransomware is a national security imperative as well.”

Last year, Gen. Paul Nakasone, head of CYBERCOM and the NSA, said similarly that views on ransomware has changed, and that when it affects “critical infrastructure, it’s a national security issue.”

When it comes to intelligence collecting, Kennedy said partnerships with the FBI and CISA have been “critical” to sharing information with the industrial base and “maybe being some level of deterrence” when it comes to making the operating environment risky for adversaries.

CISA, along with the FBI, NSA and allied cybersecurity authorities earlier in April released a joint advisory in wake of increased threats by Russian cyber groups targeting critical infrastructure both within and outside the Ukraine region.

The advisory urged critical infrastructure network defenders to prepare for and mitigate potential cyber threats, including ransomware and cyber espionage, by hardening their cyber defenses.

### 2AC---T Title 50

#### The distinction between Title 10 and Title 50 is meaningless.

Andru Wall 11, Senior Associate with Alston & Bird LLP; former senior legal advisor for U.S. Special Operations Command Centra, 12/2/2011, “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action,” <https://www.soc.mil/528th/PDFs/Title10Title50.pdf>, cc

Read in concert with Title 10, Title 50 does not infringe upon the Secretary of Defense’s authorities to collect intelligence. Rather, Title 50 recognizes the authorities assigned to the Secretary of Defense under Title 10 over all DoD intelligence activities, and adds Title 50’s provisions regarding Congressional oversight to intelligence activities conducted primarily by DoD personnel in support of or in furtherance of tasking from the Director of National Intelligence (DNI) (as opposed to tasking from the Secretary of Defense).

Thus, Title 10 and Title 50 are mutually-reinforcing authorities, not mutually-exclusive authorities; these statutory authorities may even be exercised simultaneously by personnel under the command and control of the Secretary of Defense. Labeling some intelligence activities “Title 50” activities while labeling similar activities “Title 10” activities creates a distinction where the law does not. Importantly, the statutes make distinctions based on direction, control, and funding—not on nomenclature.

### 2AC---Cybercom Normal Means

#### CYBERCOM legally can’t execute security cooperation

Robert Chesney 18, the Charles I. Francis Professor in Law and Associate Dean for Academic Affairs at the University of Texas School of Law and serves as the Director of UT-Austin's interdisciplinary research center the Robert S. Strauss Center for International Security and Law, 4/12/2018, “Title 10 and Title 50 Issues When Computer Network Operations Impact Third Countries,”’ <https://www.lawfareblog.com/title-10-and-title-50-issues-when-computer-network-operations-impact-third-countries>, cc

Does Title 10 impose a legal barrier on U.S. Cyber Command conducting operations outside of the Pentagon’s own networks?

That’s the question raised earlier this week by this story from Chris Bing at Cyberscoop (an increasingly interesting site), which builds on recent congressional testimony from Admiral Rogers. The story depicts a “quiet but constant tug of war … between the intelligence community and the military over the future of government—backed hacking,” with the central issue concerning the allocation of lead responsibility for conducting computer network operations outside the government’s own systems in order to “strike back at foreign targets.” More specifically, the story depicts something of a turf war between NSA and an increasingly independent CYBERCOM (highlighting a number of key themes, including the inherent challenge of balancing intel collection equities against the interest in having disruptive effect on some targets; on that point, read all the way to the bottom for spot-on observations from Jamil Jaffer of George Mason).

Critically, the story suggests that Title 10 and Title 50 concerns also are impacting this debate. I thought I include a brief note here to shed light on what that might mean.

The article observes that “[w]hen military leaders push to do more with hackers, they usually meet some form of resistance from Pentagon lawyers.” By way of illustration, the article points to an instance in which CYBERCOM operators deleted ISIS propaganda off a server that happened to be located in Germany. The Germans apparently were notified of the operation in some fashion but not asked for advance consent, and they were not happy about it.

From a legal perspective, the issue this highlights is that operations abroad implicate the UN Charter and related claims about international law protection of sovereignty. So how does this become part of the Title 10/Title 50 debate? Intelligence agencies can more easily act in this setting when operating under Title 50 authority, as covert action status carries with it a statutory obligation to comply with the U.S. Constitution and U.S. statutes—but no more than that. Title 10, in contrast, carries with it no such implicit statutory shield against international law objections, and of course there is a general Defense Department policy of international law compliance. Thus CYBERCOM operating under Title 10 would run into the full thicket of international law concerns. There may be good and sufficient answers to those concerns in particular cases—so this should not be understood as an absolute bar—but it does make sense to say that the legal friction is greater in that setting (that is, operations with effects on servers in third countries and without consent from those countries) than it would be for an entity acting under color of Title 50.

### 2AC---Taiwan D

#### A confluence of historical evidence and economic factors prove Xi will not invade Taiwan.

Andrew Nathan 6/23, Class of 1919 Professor of Political Science at Columbia University, 6/23/2022, “Beijing Is Still Playing the Long Game on Taiwan,” <https://www.foreignaffairs.com/articles/china/2022-06-23/beijing-still-playing-long-game-taiwan?check_logged_in=1&utm_medium=promo_email&utm_source=lo_flows&utm_campaign=registered_user_welcome&utm_term=email_1&utm_content=20220625>, cc

But fears of an imminent Chinese attack are misplaced. For decades, China’s policy toward Taiwan has been characterized by strategic patience, as has its approach to other territorial claims and disputes—from India to the South China Sea. Far from spurring China to jettison this approach in favor of an imminent military assault on Taiwan, the war in Ukraine will reinforce Beijing’s commitment to playing the long game. The price Moscow has paid, both militarily and in the form of international isolation, is but a fraction of what China could expect if it were to attempt to take Taiwan by force. Better to wait patiently for Taiwan’s eventual surrender, as Beijing sees it, than to strike now and risk winning the island at too high a cost—or losing it forever.

IMPENDING ATTACK?

Fear that China will attack Taiwan had been growing well before Putin invaded Ukraine. As Robert Blackwill and Philip Zelikow observed in a 2021 report published by the Council on Foreign Relations, Taiwan is “becoming the most dangerous flash point in the world for a possible war that would involve the United States of America, China, and probably other major powers.” In addition to its historical and economic motives for controlling Taiwan, Beijing feels the need to prevent other powers from using the island as a base to pressure China militarily or subvert it politically. For its part, the United States has strong motives for insisting on what Washington has referred to since 1972 as the “peaceful resolution of the Taiwan issue”—which, given the anti-unification sentiments of the Taiwanese people, means an open-ended and perhaps permanent state of de facto autonomy for the island. Although there is much emotion on both sides—for China, nationalism; for the United States, commitment to democracy—what makes the Taiwan issue truly nonnegotiable are the two countries’ security interests.

In 1979, when the United States broke diplomatic relations with Taiwan to normalize relations with China, Beijing had a reasonable chance of winning over Taiwan without using force. Taiwan was diplomatically isolated, militarily weak, and increasingly economically dependent on the mainland. China encouraged this dependence by establishing a host of incentives for Taiwanese enterprises to do business on the mainland, by purchasing Taiwanese exports, and by sending Chinese tourists to the island. Beijing also invested in Taiwanese media with the aim of generating favorable news coverage and held exchanges with leaders of the anti-independence Kuomintang, or Nationalist Party.

But these efforts proved insufficient to stem the tide against unification in Taiwanese public opinion and politics. According to opinion polls, the share of Taiwanese voters favoring unification fell from 28 percent in 1999 to less than two percent in 2022. An overwhelming majority favor “maintaining the status quo,” which in the language of Taiwanese politics means sustaining autonomy without formally declaring independence. Since 2016, the anti-unification Democratic Progressive Party has controlled both the presidency and the legislature, and it looks well positioned to win the next set of national elections in 2024.

Fears of an imminent Chinese attack are misplaced.

These trends have prompted China to adopt a more threatening posture toward Taiwan. Beijing has stepped up measures to isolate the island diplomatically, slowed imports and the tourist trade, trained the Chinese military to conduct the complicated joint operations necessary for a cross-strait invasion, and conducted frequent probes of Taiwan’s air defense identification zone. China has also developed what the Pentagon calls “anti-access/area denial” capabilities—including long-range precision missiles, submarine-launched torpedoes, antiship ballistic missiles, cybertools, and space capabilities—designed to hold at bay a U.S. defense of Taiwan.

These moves have fed speculation that China is building up to a full-scale attack. In addition to Xi’s desire to secure his legacy, the shifting balance of power between China and the United States is often cited by U.S. analysts as a possible motivation for Xi. The scholars Michael Beckley and Hal Brands, for instance, have suggested that China may attack in the near term because it has reached the peak of its national strength—and China’s leaders know it. China is looking at a period of decline caused by a combination of unsustainable debt, rising labor costs, an aging population, declining productivity, and a critical water shortage. Meanwhile, the United States and Taiwan have recently started to readjust their military postures to counter the asymmetric threat China poses. The Biden administration is pulling Japan and South Korea together around a commitment to “stability in the Taiwan Strait,” and Western businesses are gradually moving their production sites out of China because of rising labor costs, lack of a level playing field in the Chinese market, and COVID-19 restrictions. As this reorientation gathers steam, the West’s economic incentives to avoid war with China will diminish. By this logic, Beijing has reason to strike before its adversaries are ready.

WAITING GAME

The facts on which such forecasts are based are not wrong, but they are incomplete. A fuller set of facts suggests that China is still pursuing a strategy of strategic patience when it comes to Taiwan. First, Chinese leaders—rightly or wrongly—seem confident that they can handle their own problems better than the West can handle its problems. They don’t deny the challenges that Beckley and Brands highlight, but they believe the West is in decline, hobbled by ill-managed and slow-growing economies, social divisions, and weak political leaders. However, Chinese strategists do not seem to believe that China has yet reached a favorable power balance with the West. As Yan Xuetong, dean of the Institute of International Relations at Tsinghua University, has argued, “China’s global reach still has its limits. Despite being a major power, China also thinks of itself as a developing country—and rightly so, considering that its GDP per capita remains far behind those of advanced economies.”

Beijing can afford to wait for power in the Western Pacific to tip decisively in its favor. When Washington comes to understand that the cost of defending Taiwan is beyond its means, and Taiwanese officials realize that Washington no longer has the appetite for a clash with China, Taiwan will pragmatically negotiate an arrangement that Beijing can accept. In the meantime, China needs only to deter Taipei and Washington from attempting to lock in formal Taiwanese independence. Beijing’s shows of force are not precursors of an imminent attack, therefore, but measures intended to buy time for history to take its course.

Second, contrary to the common portrayal of China as itching for war, Beijing has demonstrated strategic patience in pursuit of its other goals. A good example is Beijing’s behavior in the South China Sea, where China has built and militarized seven sand islands without triggering a war with the United States or rival territorial claimants. It did so by building only on landforms it already controlled, claiming all along that it wasn’t doing what it was doing. The rival territorial claimants were too weak to confront China, while the United States lacked a justification for doing so because it has no territorial claims where China was building. Beijing restricted access to but refrained from seizing a landform it contests with the sole U.S. treaty ally involved in these disputes—the Philippines—which in any case lacked an appetite to invoke its alliance with Washington by moving militarily to defend itself.

The conflict in Ukraine is reminding Xi that war is unpredictable and rule over a resisting population is costly.

China likewise changed the strategic status quo without triggering an armed conflict over the contested Senkaku Islands, known in China as the Diaoyu Islands, by escalating from an occasional maritime presence in Japanese waters to a permanent one, supplementing its naval forces with less confrontational coast guard, maritime militia, and fishing vessels. Beijing followed a similar playbook in the contested Ladakh region of India, where Chinese troops gradually advanced their positions and established a series of new lines of control with only one confirmed outbreak of shooting that was quickly contained.

China has invested in ostensibly civilian port projects across the Indian Ocean and beyond that could serve as foundations for future naval operations, raising some alarm but no counteraction. Beijing has also used its economic and diplomatic influence in Africa, Europe, Latin America, the Middle East, and Oceania and its norm-setting power in international institutions to incentivize governments to align with China’s interests, again generating some alarm but no effective resistance. Such diplomatic, economic, and military “gray zone tactics” illustrate that China’s strategic behavior is geared toward the long term rather than the short term, moving from no presence to sustained presence in a host of arenas without generating substantial pushback, much less armed conflict (with the exception of the fighting in Ladakh). That same strategic caution has so far been evident in China’s policy toward Taiwan, where Beijing has dialed up tension and deterred a Taiwanese drive for independence without precipitating a crisis.

Finally, the lesson Xi is likely drawing from Putin’s war in Ukraine is not that territorial aggression would go unpunished militarily by the West but that it would be both difficult and costly. There is no reason to believe that Xi is surrounded, as Putin seems to be, by yes men who will tell him that a war over Taiwan can be easily won. Even if he is, however, the grinding conflict in Ukraine is reminding him that war is unpredictable and rule over a resisting population is costly. The amphibious operation China would need to undertake to seize Taiwan would be far more difficult than the land invasion Russia has carried out in Ukraine. Xi has been reforming the Chinese military’s command structure and ramping up training for such an operation, but Chinese forces remain untested in actual combat operations. Meanwhile, the chances that the United States would intervene to defend Taiwan have increased as anti-Chinese sentiment has risen in the United States and Europe—and after U.S. President Joe Biden remarked last month that defending Taiwan is “the commitment we made.”

### 2AC---NC3 D

#### No NC3 impact.

Erica Lonergan 22, 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; and Keren Yarhi-Milo, the Arnold A. Saltzman Professor of War and Peace Studies in the political science department and the School of International and Public Affairs and the director of the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University, 4/21/2022, “CYBER SIGNALING AND NUCLEAR DETERRENCE: IMPLICATIONS FOR THE UKRAINE CRISIS,” <https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/>, edited for ableist language, cc

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~~ [destroy] 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.

### 1AR---NC3 D

#### NC3s are disconnected from the Internet.

Futter ’16 [Andrew; 2016; International Politics Professor at the University of Leicester; “War Games Redux? Cyberthreats, US–Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control,” European Security 25(2), p. 171-172]

It is of course highly unlikely that either the USA or Russia has plans – or perhaps more importantly, the desire – to fully undermine the other’s nuclear command and control systems as a precursor to some type of disarming first strike, but the perception that nuclear forces and associated systems could be vulnerable or compromised is persuasive. Or as Hayes (2015) puts it, “The risks of cyber disablement entering into our nuclear forces are real”. While the growing possibility of “cyber disablement” should not be overstated (notions of a “cyber-Pearl Harbor” (Panetta 2012) or “cyber 9–11” (Charles 2013) have done little to help understand the nature of the challenge), cyberthreats are nevertheless an increasingly important component of the contemporary US–Russia strategic context. This is particularly the case when they are combined with other emerging military-technical developments and programmes. The net result, especially given the current downturn in US–Russian strategic relations, and the way cyber is exacerbating the impact of other problematic strategic dynamics, is that is seems highly unlikely that either the USA or Russia will make the requisite moves to de-alert nuclear forces that the new cyber challenges appear to necessitate, or for that matter to (re)embrace the “deep nuclear cuts” agenda any time soon.

Assessing the options for arms control and enhancing mutual security

Given the new challenges presented by cyber to both US and Russian nuclear forces and to US–Russia strategic stability, it is important to consider what might be done to help mitigate and guard against these threats, and thereby help minimise the risks of unintentional launches, miscalculation, and accidents, and perhaps create the conditions for greater stability, de-alerting, and further nuclear cuts. While there is unlikely to be a panacea or “magic bullet” that will reduce the risk of cyberattacks on US and Russian nuclear forces to zero – be they designed to launch nuclear weapons or compromise the systems that support them – there are a number of options that might be considered and pursued in order to address these different types of threats and vulnerabilities. None, of these however, will be easy.

The most obvious and immediate priority for both the USA and Russia is working (potentially together) to harden and better protect nuclear systems against possible cyberattack, intrusion, or cyber-induced accidents. In fact, in October 2013 it was announced that Russian nuclear command and control networks would be protected against cyber incursion and attacks by “special units” of the Strategic Missile Forces (Russia Today 2014). Other measures will include better network defences and firewalls, more sophisticated cryptographic codes, upgraded and better protected communications systems (including cables), extra redundancy, and better training and screening for the practitioners that operate these systems (see Ullman 2015). However, and while comprehensive reviews are underway to assess the vulnerabilities of current US and Russian nuclear systems to cyberattacks, it may well be that US and Russian C2 infrastructure becomes more vulnerable to cyber as it is modernised and old analogue systems are replaced with increasingly hi-tech digital platforms. As a result, and while nuclear weapons and command and control infrastructure are likely to be the best protected of all computer systems, and “air gapped”14 from the wider Internet – this does not mean they are invulnerable or will continue to be secure in the future, particularly as systems are modernised or become more complex (Fritz 2009). Or as Peggy Morse, ICBM systems director at Boeing, put it, “while its old it’s very secure” (quoted in Reed 2012).

### 2AC---Elections D

#### No impact to election hacking.

John Mueller 22, Adjunct Professor of Political Science, Ohio State University; Senior Fellow, Cato Institute, 3/22/2022, “The Cyber-​Delusion,” <https://www.cato.org/commentary/cyber-delusion>, cc

Election interference also features prominently in alarmist discourse on cyberthreats. During the 2016 U.S. presidential election, for instance, the United States highlighted apparent attempts by Russian hackers to undermine Hillary Clinton’s campaign. Although Clinton still handily won the popular vote, many analysts argued that digital interlopers sought to undermine the integrity of U.S. elections and perhaps democracy itself.

These warnings are exaggerated and—coming from U.S. policymakers—arguably hypocritical. It is worth noting that the United States has intervened in foreign elections for decades. Moreover, the idea that elections and voters are easily manipulated is suspect. If extensive promotion could guarantee success, Americans would all be driving Edsels and drinking New Coke—legendary marketing failures in 1958 and 1985 by two of the most successful businesses in history: the Ford Motor Company and Coca-​Cola. In any capitalist society, people are regularly deluged by advertising and marketing campaigns. In all cases, those petitioned remain free to ignore the ads, and most become quite good at it. In fact, studies have shown that campaign information rarely changes many votes. As political scientist Diana Mutz points out, the impact of campaign advertising “is marginal at most.”

Political campaigns, as anyone who has suffered through one knows, are also rife with falsehoods: incumbents strategically distort their record, and challengers do the same in reverse. The 2016 Russian contribution to this flood of misinformation was tiny. On Facebook, where most of the manipulation supposedly took place, Moscow’s intervention totaled perhaps a fraction one percent of the content on the platform’s news feed. Much of this was also wasted because the people who embraced it were already committed to a particular party or lived in states that went solidly for one or the other candidate. Russia’s efforts, moreover, proved wildly counterproductive. Instead of weakening U.S. policy, Moscow generated bipartisan support for anti-​Russian sanctions when the two U.S. political parties could agree on little else.

### 2AC---Democracy D

#### Democracy solves nothing.

Renske Doorenspleet 19, Political Science and International Studies Professor at Warwick University, “Democracy and Interstate War,” Chapter 3 of *Rethinking the Value of Democracy: A Comparative Perspective*, Stras

There is actually more evidence for the idea that the liberal norms lead to more (not less!) violence. Bear Braumoeller (1997), for example, argued that liberal norms of conflict resolution vary because liberalism takes many forms. By examining survey results from the newly independent states of the former Soviet Union, he showed that liberalism in that region bears a stronger resemblance to nineteenth-century liberal nationalism than to the sort of universalist, Wilsonian liberalism described by democratic peace theorists. As a result, liberals in the region are more, not less, aggressive than non-liberals. Carol Fair and her colleagues (Fair et al. 2014) came to similar conclusions. They conducted surveys in Pakistan (with 6000 respondents) and found that strong supporters of democratic values are actually not less but more supportive of militant groups. Moreover, it seems that individuals’ attitudes towards war are shaped by core beliefs about revenge, which vary across countries. Democracies with a strong tradition to support ideas of revenge24 are significantly more likely to initiate conflicts (Stein 2015). We cannot state that people in democracies are not belligerent. These results challenge the conventional wisdom about the roots of militancy and the existence of universal democratic norms, which would encourage peace.

Some scholars have argued that not the liberal democratic norms, but market-oriented development creates the norms and values that explain the democratic peace (see, e.g., Mousseau 2000). When opportunities to come to a deal in the market are widespread, as in market-oriented developed countries, a culture of contracting emerges that encourages shared respect for individualism, negotiations, compromise, respect for the law and equality before the law. Constrained by voters, democratically elected leaders in market-oriented developed countries abide by these norms. In contrast, voters in democracies without developed market economies, and the leaders in nondemocracies, have other norms and values that encourage conflict.

Hence, there is not only a lack of statistical studies, but also most findings do not support the ideas of the so-called democratic norms argument. Moreover, it is not clear why the pacifist attitude of citizens is ‘only evident in cases of democratic adversary’, while this is not the case when there are conflicts with nondemocracies, colonial expansion or third-party interventions (Gates et al. 1996: 5–6). Finally, this kind of argument tends to be tautological, stating that ‘relations between democratic states are peaceful because they are informed by a common perception that democracies are peaceful’ (Gates et al. 1996: 5–6).25

### 1AR---Democracy D

#### Norms are tautological and impossible to measure.

Doorenspleet 19 – Renske Doorenspleet, Politics Professor at the University of Warwick. [Rethinking the Value of Democracy: A Comparative Perspective, Palgrave Macmillan, p. 85-86]

There are only few statistical studies focusing on this argument of norms. Zeev Maoz and Bruce Russett (1993) defended this idea and stated that they found evidence, but their measure is very weak and lacks validity. They employed two measures of the prevalence of democratic norms. The first is through the concept of political stability, the persis¬tence of the political system in years. The second is through the amount of political violence within a state, which is measured by the number of deaths from political violence and extent of domestic conflict. In my view, those measures do not really measure 'democratic norms' but simply 'political stability and violence'. Other studies have focused on conflict management as proxy for democratic norms. William J. Dixon (1994), for example, discovered that democratic systems are better at conflict management. Democratic opponents are significandy more likely to reach peaceful settlements than other types of disputants. In addition, in disputes between democra¬cies, mediation is more likely to be pursued (Inman et al. 2014; see also Dixon 1993). Those scholars argued such outcomes supported the dem¬ocratic norms argument, but eventually they do not directly measure this concept. Moreover, the existence of democratic norms apparently did not stop the democracies to go war in the first place. Within this approach of democratic norms, other scholars stated that greater support for core liberal values leads to a rejection of destruc¬tive political activities and reduced support for violent politics. People in democracies are less aggressive, the argument goes, which could help understand the assumed existence of democratic peace. Analyses of public opinion surveys showed that American and British people are somewhat more inclined to use force against dictatorships than against democracies (Johns and Davies 2012), but the effect is very small, and it is unclear why this is the case. There is actually more evidence for the idea that the liberal norms lead to more (not less!) violence. Bear Braumoeller (1997), for example, argued that liberal norms of conflict resolution vary because liberalism takes many forms. By examining survey results from the newly independ¬ent states of the former Soviet Union, he showed that liberalism in that region bears a stronger resemblance to nineteenth-century liberal nation¬alism than to the sort of universalist, Wilsonian liberalism described by democratic peace theorists. As a result, liberals in the region are more, not less, aggressive than non-liberals. Carol Fair and her colleagues (Fair et al. 2014) came to similar conclusions. They conducted surveys in Pakistan (with 6000 respondents) and found that strong supporters of democratic values are actually not less but more supportive of militant groups. Moreover, it seems that individuals' attitudes towards war are shaped by core beliefs about revenge, which vary across countries. Democracies with a strong tradition to support ideas of revenge24 are significantly more likely to initiate conflicts (Stein 2015). We cannot state that people in democracies are not belligerent. These results challenge the conventional wisdom about the roots of militancy and the existence of universal democratic norms, which would encourage peace. Some scholars have argued that not the liberal democratic norms, but market-oriented development creates the norms and values that explain the democratic peace (see, e.g., Mousseau 2000). When opportunities to come to a deal in the market are widespread, as in market-oriented developed countries, a culture of contracting emerges that encourages shared respect for individualism, negotiations, compromise, respect for the law and equality before the law. Constrained by voters, democrat¬ically elected leaders in market-oriented developed countries abide by these norms. In contrast, voters in democracies without developed mar¬ket economies, and the leaders in nondemocracies, have other norms and values that encourage conflict. Hence, there is not only a lack of statistical studies, but also most findings do not support the ideas of the so-called democratic norms argument. Moreover, it is not clear why the pacifist attitude of citizens is 'only evident in cases of democratic adversary', while this is not the case when there are conflicts with nondemocracies, colonial expansion or third-party interventions (Gates et al. 1996: 5-6). Finally, this kind of argument tends to be tautological, stating that 'relations between democratic states are peaceful because they are informed by a common perception that democracies are peaceful' (Gates et al. 1996: 5-6).23