[Nihar] and I negate Resolved: The benefits of the United States federal government’s use of offensive cyber operations, or OCOs, outweigh the harms.

The ASPI defines offensive cyber operations, or OCOs, as:

Operations to manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks.

# Sole Contention is preventing chaos in cyberspace

### Subpoint A is destroying cyber-alliances

**Brandon Valeriano 19** Brandon Valeriano (). 1-15-2019. "The Myth of the Cyber Offense: The Case for Restraint." Cato Institute. https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint. Accessed 11-6-2019.

Securing command of the commons in the face of increasing cyber operations by China and Russia requires a policy framework that accelerates cyber offense. Offensive cyber operations entail missions “intended to project power in and through foreign cyberspace.”[17](https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint#endnote-017) **In August 2018, Trump granted the military the initiative to launch offensive cyber operations with**what appears to be **little interagency consultation** or coordination.[18](https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint#endnote-018) Cyberspace became a domain for soldiers, not just networks of spies. The move **represent[ing] a dramatic shift from [past] the restraint**s on cyber operations imposed by the Obama administration.

#### 

**Smeets ‘19** Max Smeets (Cybersecurity postdoctoral fellow at Stanford University Center for International Security and Cooperation), 10-26-2019, "NATO Allies Need to Come to Terms With Offensive Cyber Operations," Lawfare, https://www.lawfareblog.com/nato-allies-need-come-terms-offensive-cyber-operations Accessed 10.26.2019 CB19THS)

It has now been widely discussed that the **U.S. Cyber Command has undergone a significant shift in strategic thinking away from deterrence toward persistent engagement** and defend forward. Following these recent changes in strategic thinking, **U.S. Cyber Command seeks to cause friction “**wherever the adversary maneuvers,” operating **“globally, continuously and seamlessly.”** In a similar vein, NSA director and Cyber Command head Gen. Paul Nakasone writes in an article for Joint Force Quarterly: “We must … maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries.” While one may expect adversaries to maneuver in allied networks, **the U.S. is currently the only NATO state that makes causing [conflict] friction in allied networks a necessary and explicit component of its strategy.** Other military cyber organizations could follow in the near future.

#### However, these offensive cyber operations degrade the trust and confidence of our allies

**Smeets 10**-14 (Max Smeets, Oct 14 2019. Lawfare “NATO Allies Need to Come to Terms With Offensive Cyber Operations” https://www.lawfareblog.com/nato-alliesneed-come-terms-offensive-cyber-operations Accessed 10.25.2019 CB19QLC)

**In** late **2016, U.S. Cyber Command operators wiped Islamic State propaganda material off a server located in Germany. [but] The German government was** notified in some fashion but **not asked for advance consent, causing much frustration.** While U.S. Cyber Command’s reported action may have violated Germany’s sovereignty, it didn’t explicitly violate the memorandum. It wasn’t an act of CND; it was a computer network attack (CNA), seeking to disrupt, deny, degrade or destroy. **This reveals an uneasy situation within cyber cooperation:** Allies do not agree on the appropriate procedures and boundaries for offensive cyber operations. More specifically, **there is no agreement on when military cyber organizations can gain access to systems and networks in allied territory to disrupt adversarial activity.** As I have argued previously, **this issue may end up causing significant loss in allies’ trust and confidence.** My proposed solution: NATO allies should establish memoranda of understanding on offensive cyber effects operations in systems or networks based in allied territory.

**Dunlap 12**, **Major General and Former Deputy Judge Advocate General**

(Lawless Cyberwar? Not If You Want to Win, [www.americanbar.org/groups/public\_services/law\_national\_security/patriot\_debates2/the\_book\_online/ch9/ch9\_ess2.html](http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch9/ch9_ess2.html))

**Rejection of legal limits [this] carries** other, **real-world consequences that are not in the United States’ cyber interests. An effective response to cyber threats is not an autarchic enterprise; it requires the cooperation of international allies**. Baker’s “**[but a] damn the law** and lawyers” **approach would [harm]**~~cripple~~ **our relations with the law-abiding nations whose cooperation we must have to address cyber threats.** We need to keep in mind that the vast majority of adverse cyber incidents are criminal matters, and the resolution of them frequently necessitates the involvement of foreign police and judicial authorities who, by definition, require partners who are themselves committed to faithfulness to the rule of law. **The importance of legal legitimacy cannot be overstated**. As outlined above, **few in uniform who have experienced the vicissitudes of war since 9/11 would underestimate the deleterious impact on coalition support that the mere perception of American lawlessness can have.**

**This destroys alliance cohesion which is key to effectively defend against catastrophic cyberattacks**

[**David Inserra Center for Foreign Policy Studies 17**](https://www.heritage.org/cybersecurity/report/cybersecurity-beyond-us-borders-engaging-allies-and-deterring-aggressors)

Cyberspace is a domain that has revolutionized the world. Massive amounts of data can be communicated from device to device from the other side of the room or the other side of the world. The number of services that are now available to the average consumer through a personal computer, smartphone, or other device are truly mindboggling. Banking, ride or apartment sharing, dissemination of information and media, video sharing and conferencing, social media, entertainment and gaming, buying and selling of goods, and countless other online activities are now second nature to most Americans, not to mention billions of individuals elsewhere. With such leaps in productivity and convenience has [allowed] come the opportunity for hackers and certain nation states to abuse this domain to steal, undermine, destroy, or manipulate [computer] systems and masses of data for their own purposes. **Since this domain is spread across the world, bad actors in cyberspace can accomplish their goals from thousands of miles away.** As a result, when considering cybersecurity policies, the U.S. cannot just think about its own laws, resources, and systems but must also consider what is occurring outside its territory. Indeed, **the U.S. must engage with its allies and partners to craft solutions that cross borders, while using traditional tools of national power to retaliate against nations that harbor or engage in malicious cyber activity. Only through such U.S. leadership will cyberspace continue to be a domain that is sufficiently secure to continue to promote prosperity and liberty**

**We need to cooperate with EU allies like Germany and asian allies like South Korea to create a unified defense,**

**Xie 18 fortinet elaborates that these**

[**https://www.fortinet.com/blog/business-and-technology/the-value-of-collaborative-threat-intelligence-sharing-.html**](https://www.fortinet.com/blog/business-and-technology/the-value-of-collaborative-threat-intelligence-sharing-.html)

This is where the value of the **cyber threat alliances are critical. It enables** cybersecurity providers to**sharing intelligence and cooperation in incident response.**Each of the CTA’s members may have access to different pieces of the intelligence puzzle, and the CTA helps bring them together to reveal the broader picture. This approach enables CTA members to **gain[ing] rapid access to information they otherwise would not have,** which in turn allows them to better protect their customers. **This sort of cooperative strategy allows cybersecurity companies to work together operationally during large-scale cyber incidents, such as WannaCry and NotPetya, or to address newly discovered vulnerabilities, such as Meltdown. This approach dramatically improves the efficiency and effectiveness of our response efforts.**

### Subpoint B is stopping the Cyber-plague

#### Using OCOs causes the uncontrollable spread of computer viruses

#### 

Mims 17 WSJ https://www.wsj.com/articles/how-cyberwarfare-makes-cold-wars-hotter-1500811201

**You can think of cyberweapons a[re] akin to biological weapons. They often spread beyond their original targets, and once they are stolen or used, their DNA— [or] the underlying code—can be endlessly repurposed.** Exploits stolen from the U.S. National Security Agency have subsequently been used in attacks such as WannaCry, which hit businesses in the U.S. and around the world. Microsoft has made this point and called for a “digital Geneva Convention.”

#### This leads to ~~happens because of in two ways~~

1. **~~Collateral Damage~~**

~~Rovner 17~~ [~~https://warontherocks.com/2017/08/are-cyber-weapons-too-dangerous-to-use/~~](https://warontherocks.com/2017/08/are-cyber-weapons-too-dangerous-to-use/)

~~Today, critics are asking the same question about cyberspace. Over the last two decades, states have developed increasingly sophisticated tools for conducting espionage and sabotage online. Cyber spying allows intelligence agencies to gain information without putting human sources in danger. Offensive cyber operations go further, offering the hope of destroying enemy capabilities without the need for military force. It’s easy to see why these tools are so seductive to policymakers. The best-known offensive cyber operation remains the Stuxnet attack on Iran’s nuclear facility at Natanz in 2009. The attack was clever and sophisticated. It caused uranium centrifuges to slowly fail by modulating their speed, all the while hiding the effects from Iranian engineers. The problem, however, was that~~**~~[when we used] the Stuxnet worm [against Iran’s nuclear reactors]~~** ~~did not die at Natanz. Instead,~~**~~it quickly spread outside Iran,~~** ~~ultimately~~ **~~infecting over 100,000 computers [around the world]~~ ~~in India, Indonesia, and elsewhere.~~** ~~That Stuxnet — a carefully designed cyber weapon that targeted a specific industrial control system at one plant~~ **~~— spread so far and so fast~~ ~~suggest[ing] that offensive cyber operations are difficult, if not impossible, to control~~~~.~~** ~~“We will rue Stuxnet’s cavalier deployment,” warned an observer in the Financial Times.~~ **~~Such concerns have increased this year, after reports that the WannaCry and NotPetya attacks, which spread worldwide with astonishing speed, used tools that might have been stolen from the National Security Agency.~~** ~~At first glance, the attacks appeared to be designed to force targets to pay to have their machines unlocked, but analysts quickly speculated that some other motive was involved. Indeed, some cybersecurity scholars believe the attacks herald a new era of online political warfare, as attackers use cyberspace as a domain for breaking up rival alliances and undermining public faith in political institutions. It’s not an accident that all these incidents allegedly began life as tools developed by the U.S. government at National Security Agency headquarters. Effective cyber capabilities are complex, and building them often requires enormous financial and organizational investment. For a variety of reasons, the United States is in the best position to develop and deploy these tools.~~ **~~This raises the question of whether it should try in the first place. If the United States cannot control its own creations, as critics fear, it~~ ~~[and] may inadvertently cause enormous collateral damage.~~**~~Organizations like the National Security Agency and U.S. Cyber Command benefit from espionage and offensive cyber operations, but~~ **~~they are likely to hit a lot of unintended targets.~~**

#### ~~2.~~ Cyberweapon proliferation

Hitchens 19 <https://breakingdefense.com/2019/05/this-code-wont-self-destruct-can-nsa-stop-china-copying-its-cyber-weapons/>

The fundamental problem? To copy any physical weapon in history, from copper swords to hypersonic missiles, you either have to steal the physical object and try to reverse-engineer how it was made — as the Soviets did with the B-29 — or steal the information that tells you how to make it — as the Soviets did with the A-bomb. But **to copy a cyber weapon, all you have to do is see it, because the weapon itself is made of information**. China copying the code the NSA used to attack them is less like what the Soviets copying the A-bomb or the B-29 and more like the Romans copying the Greek alphabet: Enemy see, enemy do.

**That makes copycat cyber weapons extremely hard to stop**. Even if **the code** is encrypted, even if it erases itself after its attack, it **has to be executed on the target’s computer in order to affect it. That means the information of which the weapon is made has to pass at some point through the enemy system. If** the targeted computer couldn’t understand the code, it couldn’t run it, so the attack wouldn’t work.

#### Our cyberweapons are stolen and used all over the world

The [ICRC](https://www.icrc.org/en/document/potential-human-cost-cyber-operations) reports in 2019

A third concern is the proliferation of cyber tools – an issue that in some respects raises concerns similar to those that may exist with regard to weapons proliferation or the proliferation of dual-use technology, although the specific nature of cyber tools must be taken into account. Cyber tools and methods can proliferate in a unique manner that is difficult to control. First, cyber space is a global domain: provided that the attacker can overcome the cyber security and defence measures in place, any network node and information residing on the network can be accessed from anywhere in the world. At the same time, **cyber tools can be repurposed or reengineered**. The combination of these two characteristics means that **when cyber tools have been used**, stolen, leaked or otherwise become available, **actors other than those who developed them** might be able to **find** them**, reverse engineer** them**, and reuse them for their own purposes.** Finally, the fact that cyber tools and methods can be repurposed and reused is one of the factors making rapid and reliable technical attribution of cyber attacks a challenging process.

#### This allows our enemies to gain easy access to them.

Lawson 19 <https://www.fifthdomain.com/thought-leadership/2019/10/23/what-will-be-the-effect-of-the-latest-us-cyberattack-on-iran/>

What’s more, Valeriano, Jensen, and Maness warn that though the United States is more successful in cyber coercion than other states, nonetheless **these [OCOs] operations come with significant risks. These include “unintended proliferation” of cyber capabilities to nation-state rivals and criminals alike, as well as potentially damaging our ability to [protect]  develop norms against aggressive use of cyberattacks against civilian critical infrastructures.**

#### Proliferation has already happened

Jai 19

<https://www.darkreading.com/attacks-breaches/chinese-group-built-advanced-trojan-by-reverse-engineering-nsa-attack-tool-/d/d-id/1335758>

"This is no coincidence - finding the exact same set of bugs in order to create an exploit that provides remote code execution capabilities is very unlikely," he says. At the same time, there are enough differences in Bemstour to indicate the exploit was re-engineered and built from scratch, rather than copied wholesale. That is what led Check Point to conclude that an NSA exploit was used in some way as a reference, he notes. During the analysis of Bemstour, Check Point researchers found evidence suggesting the **Chinese group [APT3] had closely monitored systems under its control that the NSA had managed to compromise. APT3** members then captured traffic related to those attacks—including information on how the NSA was moving laterally on the compromised networks—and then used that as a reference to **reverse-engineered the NSA's exploits**. This allowed them to build an exploit tool that looked and worked remarkably similar to the NSA's exploit, but with less effort and cost. Instead of purchasing from a third party or investing in its own in-house team, APT3 built its malware by collecting and using the NSA's own attack data. "The main takeaway is that we see evidence for the first time of a nation-state collecting and reusing foreign attack tools to recreate their own," Lechtik says. "We heard of that happening in theory; now we [have] facts that support it." Lechtik says it's unclear if other Chinese APT groups and state actors have adopted a similar approach. But from their point of view, the approach would make sense. "If they can catch a tool and repurpose it, they cut the costs on finding it themselves," he notes. "If we see they did it once, it would be likely they have done it on other instances and keep doing it today." The question of whether other countries are doing the same thing is harder to answer, he says. Pulling off something like what APT3 did requires the ability to deliberately monitor domestic systems, collect and analyze a lot of information all with the hope of finding one usable tool. That conclusion, by Check Point Software, is based on the security vendor's analysis of Bemstour after Symantec in May reported on APT3 using it in **[and used it to launch] attacks** on targets in multiple countries, including **Belgium, Hong Kong and the Philippines.**

#### ~~In another example~~

**~~Shane 19~~** [~~https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html~~](https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html)

**~~Since~~** ~~2017~~~~,~~ ~~when~~**~~the N.S.A. lost control of the tool, EternalBlue, it has~~**~~been picked up by state hackers in North Korea, Russia and, more recently, China, to~~ **~~[caused]~~** ~~cut a path of destruction around the world, leaving~~ **~~billions of dollars in damage.~~** ~~But over the past year, the cyberweapon has boomeranged back and is now showing up in the N.S.A.’s own backyard. It is not just in Baltimore. Security experts say EternalBlue attacks have reached a high, and cybercriminals are zeroing in on vulnerable American towns and cities, from Pennsylvania to Texas, paralyzing local governments and driving up costs. Today, Baltimore remains handicapped as city officials refuse to pay, though workarounds have restored some services. Without EternalBlue, the damage would not have been so vast, experts said. The tool exploits a vulnerability in unpatched software that allows hackers to spread their malware faster and farther than they otherwise could.~~ **~~North Korea was the first nation to co-opt the tool, for an attack in 2017 — called WannaCry — that~~ ~~paralyz[ing] the British health care system~~~~, German railroads~~ ~~and~~ ~~some~~ ~~200,000 organizations around the world.~~ ~~Next was Russia, which used the weapon in an attack — called NotPetya — that was aimed at Ukraine but spread across major companies doing business in the country. The assault cost FedEx more than $400 million and Merck, the pharmaceutical giant, $670 million. The damage didn’t stop there. In the past year, the same Russian hackers who targeted the 2016 American presidential election used EternalBlue to compromise hotel Wi-Fi networks. Iranian hackers have used it to spread ransomware and hack airlines in the Middle East, according to researchers at the security firms Symantec and FireEye.~~** ~~“It’s incredible that a tool which was used by intelligence services is now publicly available and so widely used,” said Vikram Thakur, Symantec’s director of security response.~~

### These two subpoints share two impacts

### 1st Impact: Preventing attacks on financial infrastructure

**Shuermann 18 Harvard Business Review.**

(Paul Mee is a partner at consulting firm Oliver Wyman and leads its cyber risk practice. Til Schumer manyn is a partner in Oliver Wyman’s financial services practice and was a senior vice president at the Federal Reserve Bank of New York during the financial crisis. September 14th, 2018. “How a Cyber Attack Could Cause the Next Financial Crisis.” Harvard Business Review. <https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis> DOA 10/25/19) GSH

How might a financial crisis triggered by a cyber attack unfold? A likely scenario would be **an attack by a rogue nation or terrorist group on financial institutions** or major infrastructure. Inside **North Korea,** for example, the Lazarus Group, also known as Hidden Cobra, routinely looks for ways to compromise banks and exploit crypto currencies. **An attack on a bank, investment fund, custodian firm, ATM network, the interbank messaging networks known as SWIFT, or the Federal Reserve itself would represent a direct hit on the financial services system.**Another possibility would be if a so-called hacktivist or “script kiddy” amateur were to use malicious programs to launch a cyber attack without due consideration of the consequences**[it]. Such an attack could [cause] have a chain reaction,** causing damage way beyond the original intent, because rules, battle norms, and principles that are conventional wisdom in most warfare situations but don’t exist in a meaningful way in the digital arena. For example, in 2016 a script kiddie sparked a broad denial-of-service attack impacting Twitter, Spotify, and other well-known internet services as amateurs joined in for mischief purposes. Whether a major cyber attack is deliberate or somewhat accidental, the damage could be substantial. **Most of the ATM networks across North America could freeze. Credit card and other [and banking and] payment systems could fail across entire nations, as happened to the VISA network in the UK in June. Online banking could become inaccessible: no cash, no payments, no reliable information about bank accounts. Banks could lose the ability to transact with one another during a critical period of uncertainty. There could be widespread panic, albeit temporary.** Such an outcome might not cause the sort of long-simmering financial crisis that sparked the Great Recession, because money would likely be restored to banks and payments providers once systems were back online. At the same time, it isn’t clear how a central bank, the traditional financial crisis firefighter, could respond to this type of crisis on short notice. After the problem is fixed and the crisis halted, a daunting task of recovery would loom. It would be even more difficult if data were corrupted, manipulated or rendered inaccessible.

**Which is they conclude that**

Ever since the forced bankruptcy of the investment bank Lehman Brothers triggered the financial crisis 10 years ago, regulators, risk managers, and central bankers around the globe have focused on shoring up banks’ ability to withstand financial shocks. **But the next [financial] crisis might not come from a financial shock at all. The more likely culprit: a cyber attack that causes disruptions to financial services capabilities, especially payments systems, around the world.**

**Criminals have always sought ways to infiltrate financial technology systems. Now, the financial system faces the added risk of becoming collateral damage in a wider attack on critical national infrastructure. Such an attack could shake confidence in the global financial services system, causing banks, businesses and consumers to be stymied, confused or panicked, which in turn could have a major negative impact on economic activity.**

**Cybercrime alone costs nations more than $1 trillion [each year and is] and is] globally,** far more than the record $300 billion of damage due to natural disasters in 2017, according to a recent analysis our firm performed. **We ranked cyber attacks as the [single] biggest threat facing the business world today — ahead of terrorism, asset bubbles, and other risks.**

#### ~~Most companies aren’t prepared~~

[**~~https://www.inc.com/adam-levin/more-than-70-percent-of-businesses-admit-theyre-unprepared-for-a-cyberattack.html~~**](https://www.inc.com/adam-levin/more-than-70-percent-of-businesses-admit-theyre-unprepared-for-a-cyberattack.html) **~~Levin 18~~**

**~~How Can 73 Percent of Companies Not Be Prepared for [cyberattacks] Hackers? Most organizations admit to having inadequate defenses, even as cyberattacks continue to intensify~~**

#### These attacks could collapse the global economy

**Kempe Atlantic Council 2014**, Fred Kempe and Axel Lehmann, “Risk Nexus: Beyond data breaches: global interconnections of cyber risk,” https://www.files.ethz.ch/isn/182163/Zurich\_Cyber\_Risk\_April\_2014.pdf kegs

Prior to the financial crisis, risks were assessed by financial institutions individually. For example, a bank with significant exposure to certain risks – such as those associated with a large portfolio of sub-prime mortgages – might have had to set aside a reserve and perhaps expect to have a bad quarter or two if the underlying risk led to a meltdown. There was little assessment by either regulators or the market participants themselves of the **complex interconnections among the financial risks of different institutions. The resulting shock started with those who [make the riskiest decisions, but soon cascaded to everyone, even those who had invested wisely and conservatively. Not only were the chances for [can cause] a cascading catastrophe** widely ignored, but many experts insisted at the time that the system was sufficiently diversified so that linkages between risks were impossible. The system’s very complexity allowed risk to be spread to those most willing and able to deal with it. But it was this complexity, magnified by attendant lack of transparency and limited understanding, which contributed to the ultimate crash of 2008. **A failure in one small part of the U.S. mortgage market thus could lead to a global recession**, the collapse of governments, a sovereign debt crisis requiring bailouts, and even fears for the future of the euro and European Union. Unfortunately, cybersecurity professionals often approach risks in a similar fashion, relying on a reductionist analysis of risks, while assuming that the risk posed to the system as a whole is merely the sum of all the point risks. They analyze cyber vulnerabilities looking at one technology, one organization or one nation at a time, paying little attention to how risk[s] might emerge from the interaction of those organizations or technologies. Just as sound, internally-focused risk management failed to protect companies from the collapse of the financial system, s**trong internal computer security controls won’t shield even the best-protected companies from a ‘cyber sub-prime’ failure.** The similarities between the financial and cyber risk management methodologies go well beyond simple analogy. In the financial crisis, banks, corporations, individuals and even nations became vulnerable because they were highly leveraged, taking on incredible financial debts. The same is true in cybersecurity, where modern economies and societies are perhaps even more heavily leveraged, but their leverage involves information technologies (IT), not borrowed dollars, yen or euros. Companies are feeling the pressure to increase their IT leverage for the same reason that banks and other companies once increased their financial leverage: to keep pace with rivals that are all doing the same. IT leverage has just as much complexity, lack of transparency with regard to the risks, and lack of understanding of the underlying fundamentals as financial leverage. Few people truly understand their own computers or the internet, or the cloud to which they connect, just as few before the crisis truly understood the financial system as a whole or the parts to which they were most directly exposed. **A significant chain of disruptions to an interconnected system that only a few, if any, fully understand, could bring it all crashing down.**

#### Because this results in a devastating recession

**IMF** , 04/05/**13,** (Former Associate Business Editor, The Huffington Post,) “Economic Shock Could Throw 900 Million People Into Poverty, IMF Study Warns,” *Huffington Post*, <https://www.huffpost.com/entry/global-poverty-900-million-economic-shock_n_3022420> dpet

Hundreds of millions of people worldwide are on the brink of poverty. A recent study by the International Monetary Fund warns that as many as **900 million people could fall back into poverty in the event of an economic shock like the Great Recession**. That figure is three times the size of the U.S. population. According to the World Bank, 1.2 billion people are currently living on less than $1.25 a day. While the report acknowledges that progress has been to made to reduce global poverty and strengthen the world economy following the financial crisis, the world is still in a vulnerable situation. Global unemployment, for example, is the highest it’s been in two decades with 40 percent of the world’s population out of work, according to the report. And things could get much worse in the event of a macroeconomic shock, of which the Europe and U.S. are dangerously close. The recent bailout of Cyprus threw the eurozone into chaos, igniting fears that the situation could lead to the next financial crisis. Here in the U.S., a series of automatic spending cuts know as the sequester could cost the economy hundreds of thousands of jobs. The cuts have already threatened the stability of safety nets designed to aid the nation’s poorest.. The U.S. continues to fail to sustain a robust job market, adding only 88,000 jobs in March.

**around the world**.

### The second impact is protecting developing nations from cybercrime

**~~Chernenko 18 CFR~~** [**~~https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms~~**](https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms) **~~February 23, 2018~~**

**~~Without [this] increased cooperation, the global digital economy is vulnerable to catastrophic cyberattack.~~** ~~The attacks of 2017, however, could be dwarfed by cyberattack campaigns in coming years. According to a Lloyd’s of London report, a major cyberattack on a cloud services provider such as Amazon could trigger economic losses of up to $53 billion, a figure on par with a catastrophic natural disaster such as Hurricane Sandy, which hit much of the eastern United States in 2012. The Russian Federal Security Service (FSB) estimates that~~ **~~cyberattacks [could]~~** ~~already~~ **~~cost the global economy~~**~~$300 billion annually, and Juniper Research recently predicted that figure will total~~ **~~$8 trillion over the next five years.~~**

#### 

#### Developing nations’s ICT, or information and communication technology infrastructures, are particularly vulnerable to criminal cyberattacks

**Lazarous UN** [**https://news.un.org/en/story/2011/12/397922-developing-countries-most-vulnerable-cyberattacks-un**](https://news.un.org/en/story/2011/12/397922-developing-countries-most-vulnerable-cyberattacks-un)

**“Cyberattacks have the potential for triggering inter-State and other conflicts which can put their entire ICT development process at considerable risk, [including mobile communications and the internet]. Developing countries, with relatively weak surveillance capacity are most vulnerable to such cyberattacks,” he said.** According to the UN International Telecommunication Union (ITU), there are six billion mobile cellular subscriptions worldwide and more than 2.3 billion people online, making ICTs a powerful tool to advance development. Developing countries are using ICTs to advance their development agenda, Mr. Kapambwe said, “**because of their relevance in transforming human activities and in presenting new opportunities for economic growth.** “Mobile phones and the Internet have had beneficial impacts on supporting the livelihoods of rural people, particularly farmers in Asia. In Africa, mobile phones are the most widely-used form of communications technology,” he said.

#### These ICT cyberattacks stunt their economic growth

**Todd 15** <https://www.one.org/international/blog/why-connecting-everyone-to-the-internet-could-help-end-extreme-poverty/>

The results of connectivity could be huge.**Internet connectivity could g**enerate $2.2 trillion of economic growth and more than 140 million new jobs. If everyone had access to the internet, the opportunities opened up to them could**lift 160 million people out of extreme poverty, the improvements in health care could help save the lives of 2.5 million people,** and 2.5 million HIV/AIDS patients could increase their life expectancy thanks to better monitoring and adherence to treatment.

**Thus we negate.**

# Frontlines

### Lay Rhetoric

Harms O/W benefits

Lay Strats: Ballot looks like/2 reasons one reason

### Cheese Frontline strats: We account, directionality, no warrant, not a turn

### 

### C1

OCOs destroy global cyber-security alliances

Valeriano and Smeets explain that the US is now recklessly launching OCOs in our ally’s networks without permission. For example, we attacked ISIS servers in Germany without the government’s consent which destroys their trust and confidence in us. Dunlap and Inserra explain that this shatters relations with our allies and prevents cooperation to stop cyberattacks. Xie find that intel sharing and incident response collaboration dramatically increases the world’s ability to defend against cyberattacks.

**Turns the link into their [x] impact - better able to prevent against isis attacks on things like power grids when we coordinate with allies- comes before conventional weighing mechanisms since it controls their link too**

o/w mag - global scope - every cyber attack around the world becomes more damaging - encompasses both impacts

o/w prob - our link has empirically happened -germany example gives 100% prob - alt solvency means they have low p of link uniqueness

### FL: Coop Now/Dont need allies

1. Coop could be much higher
   1. Ex HBR - US has not joined the EU-led Paris call b/c it would require us to follow peaceful norms
   2. That’s why we still see bad cyberattacks
2. Corrigan 19 - top diplomat says us could do more - joint deterrent effect is much stronger when everyone responds
3. Peters 19 - need new forums w/ allies

### FL: Makes Allies Feel Safer

1. Allies are less likely to follow us if we intrude their sovereignty - help o/w by mistrust

### FL: Alliances now

1. On the brink - trump relations are already poor just hanging on by a thread

### FL: Nato Turn

1. They don’t “turn” us - this functions as an independent DA to our arg but doesn’t affect our impacts
2. We control their internal link:
   1. **Success is contingent on cohesion but Turn: Fracture relations and cohesion - Smeets explicitly says Russia can exploit by operating in countries where the US does not have consent to launch OCOs through to hurt our relations w/ allies**
3. [Cockerill 19] Routine Cyberattacks remove norm of cyber restraint, increasing instability/violence
4. Independently Turn since it agresses russia
5. Lewis (bad?) - Shift away from defensive posture now
6. **Lewis - US is very secretive about OCOs with NATO - nobody knows whats going on -> conflict**
7. US unlikely to defend NATO - doesn’t like the commitment - thev just says US can but not will

## C2

### Extensions

Using OCOs causes the uncontrollable spread of computer viruses

2 ways:

1. Rovner- OCOs cause **collateral damage** - for example after we used stuxnet against iran it spread to 100k computers causing catastrophic global damage - concludes its uncontrollable
2. Hitchens ICRC - Cyberweps are guaranteed to be **reverse-engineered** and copied - all they have to do is see the attack to find the code - copycats are inevitable. This causes unintended cyber-proliferation - that’s Jai- China used our viruses successfully this year to launch cyberattacks against the phillipines.

O/W mag - 160 mill ppl, maybe:? prefer dev countries since they dont have any social safety net like social security,

O/W prob - empirically has happened - stuxnet China and wannacry examples prove it will happen again if we dont do anything

O/W TF -

**Turns every link in their case - our enemies get stronger which prevents deterrence and inc conflict**

### Frontlines

#### AT: Disclose vulns

1. Not all hacks are equally powerful - the ones we actually use are hidden
2. Vinik Politico - once we disclose they don’t work so concede solvency

#### AT: Other countries also have cyberweps

1. We have a history of really bad ones- wannacry, APT3
2. politico 15- us has most powerful cyberweps
3. It’s scalar

#### AT: Why hasnt happened yet?

The more OCOs we launch the more powerful our opponent’s cyberweapons get - more likely they can take down N9 and interbank exchanges and collapse the - It is a fallacy to say something wont happen just because it hasnt happened **yet**

#### AT: Not LT

1. Most financial market crashes are triggered by sudden short term events - eg. bear sterns in 2018; Bloom 11/ volatility shocks - sudden event cause market collapse, leads to chain reaction

#### AT: Not a big deal

1. Biz times 19 - up to 65% revenue lost

#### AT: Budapest agreement solves dev countries

* 1. Takes out their own impact
  2. Not enough - been around for 18 years and still attacks - need deeper coop

#### AT: No escalation

1. Deterrence fails against cybercriminals - too many of them to track

### Impact Section

The impact is preventing a financial crisis:

Shuermann and Kempe - attacks on interbank networks could cause a global chain reaction where all payment systems fail - that causes 1T in damage and collapses the global economy. IMF says that pushes 900 mil into poverty

Impact: is destroying dev countries

NSA Viruses like wannacry cause billions once they escape or are stolen - Lazarus and Tood find that cybercriminals then use these weps to destroy developing nation’s internet infrastructure which is critical for economic growth- that keeps 160 mil in poverty and costs 2.5 mil lives.

### FL Cards

Vinik Politico -

<https://www.politico.com/agenda/story/2015/12/defense-department-cyber-offense-strategy-000331>

As weapons, cyber capabilities differ in a few key ways from traditional weapons like missiles and bombs. First, they cause damage that’s less overt but more widespread than a physical attack—a cyber weapon could cripple a local economy by attacking a country’s financial or communication systems. Second, an attack can occur almost instantaneously against any target in the world. The Internet makes physical distance between enemies all but irrelevant, making it both easier for enemies to launch cyberattacks and harder for the government to monitor for them. Third, the use of a cyber capability is often a one-time deal: If the government has a piece of malicious software and uses it to exploit a flaw in an enemy’s code, it could render future uses of that capability ineffective, since the adversary could just patch it. It could also compromise intelligence-collection activities that use the same exploit.

Biz times 19

<https://www.businesstimes.com.sg/banking-finance/20-65-of-banks-quarterly-profit-at-risk-from-full-blown-direct-cyberattacks-mas>

This cost for this worst-case scenario jumps to as much as 65 per cent, if no contingencies have been made, said the regulator, as it raised scrutiny on the impact of cybersecurity on financial stability in Singapore. Deposits could also decline by 1-5 per cent.

https://www.politico.com/agenda/story/2015/12/defense-department-cyber-offense-strategy-000331

What's going on? The growth points to one of the most cutting-edge, but also obscure, realms of American military activity: its cyber strategy, and especially its strategy for cyber offense. The United States already has, most observers believe, the most powerful cyberattack capabilities in the world. Much less clear is just what its capacities actually are—and when the Department of Defense believes it should use them.

Peters 19 - need new forums

<https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/>

If the United States isn’t careful, it risks letting Russia and China win another matchup on cybercrime. It must be prepared for Russia to build on last year’s victory and start working now to expand the support it needs to effectively advance its own agenda on cybercrime. U.S. diplomats need to have a clear strategy and the resources needed to build allies in New York in this fight. And while the United States has remained committed to protecting the Budapest Convention, the government’s cybercrime agenda should be focused on not only expanding the number of parties to this treaty but also supporting new forums that can promote public and private global cooperation on cybercrime if those forums adhere to similar values. Yet U.S. President Donald Trump’s previous backtracking on the United States’ historic position against Russia’s approach to cybercrime undermined efforts to craft a consistent and coherent agenda. The United States has already lost clout and leverage at the United Nations, and it will continue to do so if its diplomats do not have the support and high-level backing from leaders in the Trump administration to effectively do their jobs. If they can’t, it will ultimately be everyday Americans who will be the victims.

Corrigan 19 <https://www.defenseone.com/politics/2019/04/top-cyber-diplomat-us-needs-allies-help-punish-cyberattacks/156510/>

Creating a unified international response around online attacks will help “establish the legitimacy” of norms for cyberspac **The U.S. could do a better job deterring cyberattacks if international allies were on board to punish the perpetrators, the nation’s top cyber diplomat said Tuesday.** In recent years, the U.S. and its allies have gotten less afraid of attributing cyberattacks to adversaries like Russia, Iran and North Korea, but their attempts to punish those online aggressions are far less united, according to Rob Strayer, the State Department’s deputy assistant secretary for cyber and international communications and information policy. To prevent those countries from launching attacks in the first place, the international community needs to make it clear that the costs of such actions outweigh the benefits. According to Strayer, that calculation is a lot easier when multiple countries are threatening retaliation.

**The most obvious benefit of this unified approach is that punishments are a lot stronger when they’re brought by multiple countries**, Strayer said. **If all of NATO slaps sanctions on Russia,** for example, its economy would suffer a lot more than if only the U.S. did so.

#### US has not joined the EU-led Paris call b/c it would put limits on our actions

HBR 19 <https://hbr.org/2019/09/why-companies-are-forming-cybersecurity-alliances>

There is evidence that such efforts have indeed begun to move the conversation forward for companies and nations. Last November, for example, President Emmanuel Macron of France launched the “Paris Call for Trust and Security in Cyberspace,” a symbolic declaration to improve cybersecurity practices and international standards for the internet. Sixty-seven countries, including the entire EU, have joined the pledge, along with 358 companies and 139 international and civil society organizations. (The list of signatories includes the World Economic Forum, where I am employed.) At the very least, the call represents an opening for companies and governments that care about security on a global scale to cooperate with a new set of allies.

That’s not to say cooperation will be easy, or perfect, in the short term. Currently, the most powerful nations are signaling an aversion to cooperation on many fronts, not just in tech. Among the signatories to the Paris call, for example, there are three countries noticeably absent: the U.S., China, and Russia. Although the United States generally supports multistakeholder internet governance, China and Russia have opted for a more isolationist and state-controlled approach. Russia, in fact, has announced plans to develop the capacity to entirely shut itself off from the global internet, similar to the “Great Firewall” of China.

**The U.S. is secretive about its OCOs to NATO.**

[Lewis, Center for Strategic and International Studies](https://ccdcoe.org/uploads/2018/10/TP_08_2015_0.pdf)

“The question of NATO and offensive cyber capabilities touches on a range of sensitive political issues that militate against any change in policy in the near term. **The US has always been overly secretive about its offensive cyber capabilities**, even after a flood of media leaks have made the most sensitive doctrine publicly available. **This secrecy has carried over into NATO, and is unhelpful in that it increases the likelihood of opponents miscalculating as they consider the risks of using force or coercion against NATO members or interests. A lack of public discourse on offensive cyber operations undercuts the legitimacy of NATO operations by failing to build public understanding, and leaves NATO open to charges of sinister plots**, since denial of offensive capabilities is not credible when two NATO members are world leaders in cyber operations.”

**A2: NSA got hacked? EternalBLue**

[**https://www.wired.com/story/nsa-zero-day-symantec-buckeye-china/**](https://www.wired.com/story/nsa-zero-day-symantec-buckeye-china/)

**Symantec found that by March 2016, the SMB zero-day had been obtained by the Chinese BuckEye group, which was using it in a broad spying campaign**. The BuckEye hackers seemed to have built their own hacking tool from the SMB vulnerability, and just as unexpectedly were using it on victim computers to install the same backdoor tool, called DoublePulsar, that the NSA had installed on its targets' machines. That suggests that the hackers hadn't merely chanced upon the same vulnerability in their research—what the security world calls a bug collision.; they seemed to have somehow obtained parts of the NSA's toolkit.

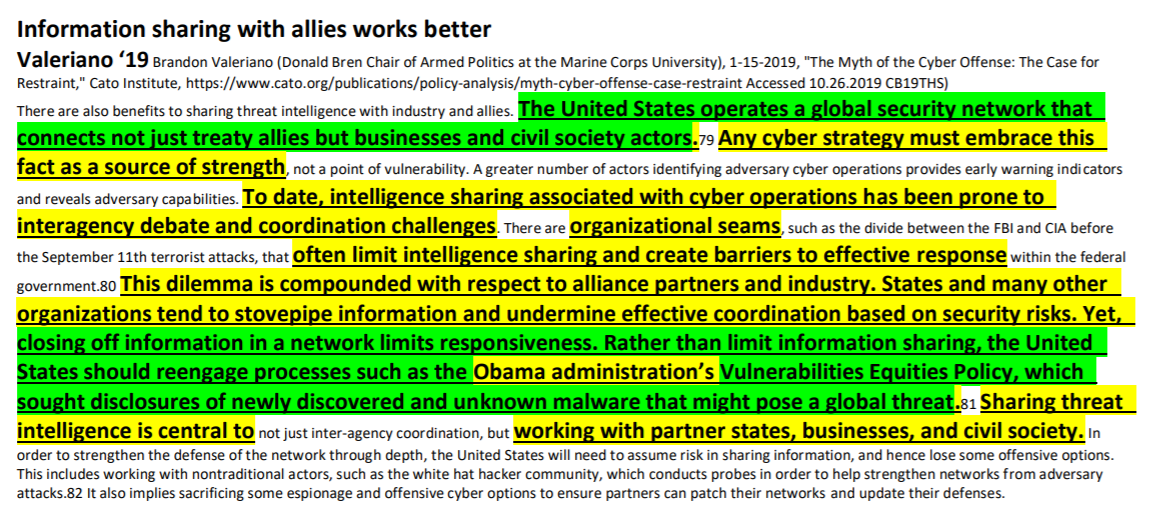
Symantec's researchers say they still don’t know how the BuckEye hackers got the NSA’s hacking secrets. But Symantec's Chien says **their theory is that the tools were found in victim networks, reverse-engineered,** and repurposed. "It doesn't look like they had the exploit executables,” says Jake Williams, a former NSA hacker and now founder of security firm Rendition Infosec, who reviewed Symantec's findings. **"But it's possible they were able to steal them [when they were] being thrown at targets by monitoring network communications**."

Starting a year after those stealthy intrusions began, however, the NSA's zero-day was hijacked in a far more public fashion. In April 2017, a still-mysterious group calling itself the **Shadow Brokers** dumped the NSA's EternalBlue, EternalRomance, EternalSynergy, and DoublePulsar tools into public view, part of a series of leaks from the group that had started the previous summer with a failed attempt to auction the stolen tools to the highest bidder. **It's still entirely unclear how the NSA's crown jewels ended up in the Shadow Brokers' hands, though theories include a rogue NSA insider selling the tools and hackers chancing upon an NSA "staging server," a machine used as a kind of remote outpost from which to launch operations.**

O/W Mag - global, lazarus and todd/ dev countries destroy their it like mobile phones and internet - 160

mil poverty 2.5 mil lives - they never terminalize or quantify their iran impacts

# Extra Cards



<https://www.darkreading.com/attacks-breaches/chinese-group-built-advanced-trojan-by-reverse-engineering-nsa-attack-tool-/d/d-id/1335758>

https://ccdcoe.org/uploads/2018/10/Art-10-Aladdins-Lamp.-The-Theft-and-Re-weaponization-of-Malicious-Code.pdf

We know for a fact that malware re-weaponization is possible because we often see it within academic research1 [2] [3] and in capture-the-flag (CTF) hacker competitions [4]. However, we have also seen reflections of it in real-world computer network operations by nation-states [5] [6]. Cyber actors and campaigns with names like DarkHotel, Lazarus, and TigerMilk have been seen throughout Asia, reusing attack code such as NetTraveler and Decafett in ways that also appear to incorporate false flags intended to cast blame on others during cyber operation

# OLD Contention 1 is destroying cyber-alliances

[**David Inserra Center for Foreign Policy Studies 17**](https://www.heritage.org/cybersecurity/report/cybersecurity-beyond-us-borders-engaging-allies-and-deterring-aggressors)

**Cyberspace** is a domain that has revolutionized the world. Massive amounts of data can be communicated from device to device from the other side of the room or the other side of the world. The number of services that are now available to the average consumer through a personal computer, smartphone, or other device are truly mindboggling. Banking, ride or apartment sharing, dissemination of information and media, video sharing and conferencing, social media, entertainment and gaming, buying and selling of goods, and countless other online activities are now second nature to most Americans, not to mention billions of individuals elsewhere. With such leaps in productivity and convenience **has [allowed]** come **the opportunity for hackers and certain nation states to abuse this domain to steal, undermine, destroy, or manipulate [computer] systems and masses of data** for their own purposes. Since this domain is spread across the world, **bad actors in cyberspace can accomplish their goals from thousands of miles away.** As a result, when considering cybersecurity policies, the U.S. cannot just think about its own laws, resources, and systems but must also consider what is occurring outside its territory. Indeed, **the U.S. must engage with its allies and partners to craft solutions that cross borders, while using traditional tools of national power to retaliate against nations that harbor or engage in malicious cyber activity. Only through such U.S. leadership will cyberspace continue to be a domain that is sufficiently secure to continue to promote prosperity and liberty.**

#### However, in order for us to successfully defend against cyberattacks, our allies must trust us in Cyberspace.

**Which is why Smeets 19** <https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies>

Much has been written about **[offensive] fundamental changes in U.S. cyber strategy.** U.S. Cyber Command’s vision of “persistent engagement” and the Department of Defense’s new strategy of “defend forward” have, in particular, led to numerous critical remarks about the risks of escalation between the U.S. and its main adversaries in cyberspace. These debates are worth continuing, including about what the change in strategy means for establishing norms in cyberspace. But commentators have so far ignored a key dimension: **The strategy’s main implications may not reside in how it changes the dynamics between the U.S. and its adversaries but, instead, in how it affects broader alliance relationships**, especially beyond the Five Eyes (Australia, Canada, the U.K., the U.S. and New Zealand). **U.S. Cyber Command’s mission to cause friction in adversaries’ freedom of maneuver in cyberspace** may end up causing significant friction in allies’ trust and confidence—and adversaries may be able to exploit that. In an article for Joint Force Quarterly (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.” 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 precedent 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, 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. 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, **[to] actively, seamlessly, and continuously disrupting [our] 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. I would add that there is also much uncertainty about where Cyber Command currently operates. This dimension, however, is crucially important for understanding the true implications of the United States’s change in cyber strategy. By operating in allied networks, Cyber Command is running the risk of causing the wrong type of friction.

#### 

#### Specifically, U.S. intrusions into allied networks destroy trust the most

**Smeets continues**, Max. "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis." 2019 11th International Conference on Cyber Conflict (CyCon). Vol. 900. IEEE, **2019**. <https://ccdcoe.org/uploads/2019/06/Art_09_NATO-Members-Organizational-Path.pdf>

<https://www.lawfareblog.com/nato-allies-need-come-terms-offensive-cyber-operations>

This reveals an uneasy situation within cyber cooperation: Allies do not agree on the appropriate procedures and boundaries for offensive cyber operations. More specifically, **there is no agreement on when military cyber organizations can gain access to systems and networks in allied territory to disrupt adversarial activity**. As I have argued previously, **this issue may end up causing significant loss in allies’ trust and confidence.** My proposed solution: NATO allies should establish memoranda of understanding on offensive cyber effects operations in systems or networks based in allied territory.

**In late 2016, U.S. Cyber Command operators wiped [isis] propaganda material off a server located in Germany. [but] The German government was** notified in some fashion but **not asked for advance consent, causing much frustration**. While U.S. Cyber Command’s reported action may have violated Germany’s sovereignty, it didn’t explicitly violate the memorandum. It wasn’t an act of CND; it was a computer network attack (CNA), seeking to disrupt, deny, degrade or destroy. This reveals an uneasy situation within cyber cooperation: Allies do not agree on the appropriate procedures and boundaries for offensive cyber operations. More specifically, there is no agreement on when military cyber organizations can gain access to systems and networks in allied territory to disrupt adversarial activity. As I have argued previously, this issue may end up causing significant loss in allies’ trust and confidence. My proposed solution: NATO allies should establish memoranda of understanding on offensive cyber effects operations in systems or networks based in allied territory.

Allied states may operate in each other’s systems or networks in at least three ways: as an observer, [gathering](https://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780190665012.001.0001/acprof-9780190665012) intelligence on adversarial activity in others’ networks; as a passerby, transiting through allied systems and networks to access a certain adversarial target; or as a disrupter, seeking to cause friction for an adversary’s operation within an ally’s network or system. The German case discussed above is the only publicly known case of a state acting as a disrupter in an allied network. But **we can expect that more of these cases will be publicly disclosed in the future.**

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

**Rovner 17** <https://warontherocks.com/2017/08/are-cyber-weapons-too-dangerous-to-use/>

**The more this happens, the more these operations risk eroding faith in cybersecurity.**Ordinary internet users may be less willing to log on. Businesses could be increasingly wary of operating online. Computer scientists and engineers may become less enthusiastic about volunteering their time and expertise to sustain the internet. And **if states believe their rivals are actively undermining cybersecurity for their own purposes, they will be less likely to cooperate on shared issues like cybercrime.**

#### ~~The very nature of these operations undermine alliance structures and international stability~~

~~David~~ **~~Mussington~~**~~, Center for International Governance Innovation, 4/8/~~**~~2019~~**~~, “Strategic Stability, Cyber Operations and International Security,”~~ [~~https://www.cigionline.org/articles/strategic-stability-cyber-operations-and-international-security~~](https://www.cigionline.org/articles/strategic-stability-cyber-operations-and-international-security) ~~(David Mussington is a senior fellow at the Centre for International Governance Innovation (CIGI), and professor of the practice and director, Center for Public Policy and Private Enterprise, University of Maryland, College Park. In 2010, David was senior adviser for cyber policy in the US Department of Defense, later serving on the Obama administration’s National Security Council staff as director for surface transportation security policy.) kegs~~

~~Strategic stability at the global level relies on the concept of deterrence — preventing aggression by threatening harsh punishment, or by imposing costs that exceed any benefits from attack. The anonymity granted to actors in cyberspace makes it tough to identify the culprit of a given attack with a high degree of certainty (the origin of a piece of malware is much less obvious than the origin of a missile strike), undermining the effectiveness of deterrence strategies and emboldening attackers (Solomon 2011).~~

~~While there has been some progress in improving the technical aspect of cyber attack attribution, political difficulties remain. After all, for a deterrence strategy to work, a state must retaliate once an attack is identified, and allies committed to collective defence must come to their aid. Despite traditional rhetoric, such assistance is never automatic, and the added problem of convincingly attributing cyber attacks adds another layer of uncertainty to the political calculus. Honoring commitments to allies can be costly, and states will be reluctant to bear this burden if there remain any doubts about the identity of the attacker. In this way, the cyber-attribution problem~~ **~~can undermine the cohesiveness of alliances and, by extension, international stability~~**~~.~~

### Impact is damaging coalition cohesion

**Major General Dunlap 12**, **Major General and Former Deputy Judge Advocate General**<http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare>

(Lawless Cyberwar? Not If You Want to Win,: While popular fiction and films depict cyberattacks as easy to mount—only a few computer keystrokes needed—in reality it takes significant digital snooping to identify potential entry points and susceptible nodes in a linked network of communications systems, radars and missiles like that operated by the Libyan government, and then to write and insert the proper poisonous codes. Obviously, if cyber weaponry is technically difficult for the world’s foremost military to use even against a third-world power such as Libya, one may reasonably infer that it is markedly more difficult to use against a sophisticated first-world power, even for a peer or near peer of that power. Rejection of legal limits carries other, real-world consequences that are not in the United States’ cyber interest**s. An effective response to cyber threats** is not an autarchic enterprise; it **requires the cooperation of international allies.** Baker’s “damn the law and lawyers” approach would [harm]cripple our relations with the law-abiding nations whose cooperation we must have to address cyber threats. We need to keep in mind that the vast majority of adverse cyber incidents are criminal matters, and the resolution of them frequently necessitates the involvement of foreign police and judicial authorities who, by definition, require partners who are themselves committed to faithfulness to the rule of law. The importance of legal legitimacy cannot be overstated. As outlined above, few in uniform who have experienced the vicissitudes of war since 9/11 would underestimate the deleterious impact on coalition support that the mere perception of American lawlessness can have.**An effective response to cyber threats** is not an autarchic enterprise; it **requires the cooperation of international allies.**

**which is why Lord et al 11, Vice President and Director of Studies at the Center for a New American Security**

(Kristin M., Travis Sharp is the Bacevich Fellow at the Center for a New American Security. Joseph S. Nye, Jr. is University Distinguished Service Professor at the Kennedy School of Government at Harvard University. Mike McConnell is Executive Vice President of Booz Allen Hamilton and former Director of National Intelligence and Director of the National Security Agency. Gary McGraw is Chief Technology Officer of Cigital, Inc., a software security consultancy, and author of eight books on software security. Nathaniel Fick is Chief Executive Officer of the Center for a New American Security. Thomas G. Mahnken is Jerome E. Levy Chair of Economic Geography and National Security at the U.S. Naval War College and a Visiting Scholar at the Johns Hopkins School of Advanced International Studies. Gregory J. Rattray is a Partner at Delta Risk LLC and Senior Vice President for Security at BITS, the technology policy division of The Financial Services Roundtable. Jason Healey is Director of the Cyber Statecraft Initiative at the Atlantic Council and Executive Director of the Cyber Conflict Studies Association. Martha Finnemore is Professor of Political Science and International Affairs at The George Washington University. David A. Gross is a Partner at Wiley Rein LLP and a former Ambassador and Coordinator for International Communications and Information Policy at the State Department. Nova J. Daly is a Public Policy Consultant at Wiley Rein LLP and former Deputy Assistant Secretary for Investment Security in the Office of International Affairs at the Treasury Department. M. Ethan Lucarelli is an Associate at Wiley Rein LLP. Roger H. Miksad is an Associate at Wiley Rein LLP. James A. Lewis is a Senior Fellow and Director of the Technology and Public Policy Program at the Center for Strategic and International Studies. Richard Fontaine is a Senior Fellow at the Center for a New American Security. Will Rogers is a Research Associate at the Center for a New American Security. Christopher M. Schroeder is an Internet entrepreneur, Chief Executive Officer of HealthCentral.com and a member of the Center for a New American Security’s board of advisors. Daniel E. Geer, Jr. is Chief Information Security Officer of In-Q-Tel, the independent investment firm that identifies innovative technologies in support of the missions of the U.S. intelligence community. Robert E. Kahn is President and Chief Executive Officer of the Corporation for National Research Initiatives and co-inventor of the TCP/IP protocol that is the foundation of the modern Internet. Peter Schwartz is Co-Founder and Chairman of Global Business Network and a member of the Center for a New American Security’s board of directors, “America’s Cyber Future Security and Prosperity in the Information Age volume I” June 2011, [http:// www.cnas.org/files/documents/publications/CNAS\_Cyber\_Volume%20I\_0.pdf](http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20I_0.pdf))

**The United States [must] should lead a broad**, multi-stakeholder **international cyber security coalition t**hat supplements U.S. freedom of action in cyberspace with global norms that will help protect its interests. The United States must play a greater leadership role within a range of existing and emerging international coalitions **if it wishes to shape the future of cyberspace** and how it is governed.35 Exercising leadership may, in some circumstances, require the United States to curtail some freedom of action internationally in order to shape the behavior of others. It does this already by adhering to existing norms and agreements, such as the Law of Armed Conflict and World Trade Organization. As long as such tradeoffs remain consistent with American interests and values, **this cooperative leadership model offers the best way for the United States to strengthen its cyber security**. Since the United States pursues competing interests and values in cyberspace, it must develop policies that balance those interests and values. An effective cyber security strategy requires American policymakers to balance competing interests and values in a way that defends the nation without subverting what it stands for.

**Mussington 19 - these alliances are key to cybersecurity**

<https://www.cigionline.org/articles/strategic-stability-cyber-operations-and-international-security>

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

**Xie 18 fortinet**

[**https://www.fortinet.com/blog/business-and-technology/the-value-of-collaborative-threat-intelligence-sharing-.html**](https://www.fortinet.com/blog/business-and-technology/the-value-of-collaborative-threat-intelligence-sharing-.html)

**This is where the value of the [cyber alliances] are critical. It enables cybersecurity providers to sharing intelligence and cooperation in incident response. Each of the CTA’s members may have access to different pieces of the intelligence puzzle, and the CTA helps bring them together to reveal the broader picture. This approach enables CTA members to gain rapid access to information they otherwise would not have, which in turn allows them to better protect their customers.**

**This sort of cooperative strategy allows cybersecurity companies to work together operationally during large-scale cyber incidents, such as WannaCry and NotPetya, or to address newly discovered vulnerabilities, such as Meltdown. This approach dramatically improves the efficiency and effectiveness of our response efforts.**

**Chernenko 18 CFR** [**https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms**](https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms) **February 23, 2018**

**Without [this] increased cooperation, the global digital economy is vulnerable to catastrophic cyberattack.** The attacks of 2017, however, could be dwarfed by cyberattack campaigns in coming years. According to a Lloyd’s of London report, a major cyberattack on a cloud services provider such as Amazon could trigger economic losses of up to $53 billion, a figure on par with a catastrophic natural disaster such as Hurricane Sandy, which hit much of the eastern United States in 2012. The Russian Federal Security Service (FSB) estimates that **cyberattacks [could]** already **cost the global economy**$300 billion annually, and Juniper Research recently predicted that figure will total **$8 trillion over the next five years.**

**Economic cyberattacks increase poverty**

[**https://www.livemint.com/opinion/columns/opinion-economic-growth-is-a-moral-obligation-to-the-poor-1552926519229.html**](https://www.livemint.com/opinion/columns/opinion-economic-growth-is-a-moral-obligation-to-the-poor-1552926519229.html)

But the job is far from complete. About 75 million Indians still live below the $1.90-a-day threshold in what is termed extreme poverty. Using a different figure by the World Bank of $3.20 a day for “lower middle income" countries like India, about one-third of all Indians (450 million) are poor and vulnerable to economic stress that could push them back into extreme poverty. According to a working paper by Pradeep Agarwal for the Institute of Economic Growth**, a single percentage point increase in [] GDP per capita reduces [] poverty by 0.78%.** In other words,a additional 1% increase in the GDP per capita can potentially lift about 3 million Indians out of poverty.