# CYBER NEG

# Cyber War Advantage Answers

## No Cyber Impacts

### 1nc – Russia Weak

#### Russia is using the full weight of its cyber capabilities now—we’re just not really seeing signs of it for multiple reasons

Seldin 22 [Jeff Seldin serves as VOA’s National Security Correspondent tracking developments in intelligence, counterterrorism, and cyber since March 2015, following a stint covering the Pentagon. 5-25-2022 Sanctions Frustrating Russian Ransomware Actors VOA https://www.voanews.com/a/sanctions-frustrating-russian-ransomware-actors-/6589241.html] SW 6-18-2022

U.S. and NATO officials on Wednesday also cautioned that it would be a mistake to think that just because there have been few signs of "catastrophic effects" that Russia has not tried to leverage its cyber capabilities to its advantage. "It has been happening and it's still happening," said Stefanie Metka, head of the Cyber Threat Analysis Branch at NATO. "There's a lot of cyber activity that's happening all the time and probably we won't know the full extent of it until we turn the computers back on." Said the NSA's Joyce: "If you look at Ukraine, they have been heavily targeted. What we've seen are a number of wiper viruses, seven or eight different or unique wiper viruses that have been thrown into the ecosystem of Ukraine and its near abroad." Wiper viruses are viruses that erase a computer's memory. These included a cyberattack against a satellite communications company, which hampered the ability of Ukraine's military to communicate and had spillover effects across Europe. But with help from the U.S. and other allies, Ukraine was able to mitigate the impact, Joyce said. "The Ukrainians have been under threat and under pressure for a number of years, and so they have continued to adapt and improve and develop their tradecraft to the point where they mount a good defense and, equally as important, they mount a great incident response," he said. Some cybersecurity experts say that ability to respond might be one of the biggest take-aways, so far, from the invasion. "Resiliency matters," said Dmitri Alperovitch, the founder of the Silverado Policy Accelerator and the former chief technology officer of cybersecurity firm CrowdStrike, at Wednesday's virtual forum. "The Ukrainians have gotten really, really good at rebuilding networks, quickly mitigating damage." Another key lesson, he said, is the limitations of cyber. "If you've got kinetic options, if you can create a crater somewhere, take out a substation, take out a communication system, that's what you're going to prefer to use," Alperovitch said. "That's what's easiest [to do] to get lasting damage."

### 1nc – SQ Deterrence Solves

#### Russia won’t launch major cyber attacks and no escalation – both sides believes in cyber MAD

Paul 22 [Kari Paul is a west coast based technology reporter for Guardian US 3-9-2022 ‘Catastrophic’ cyberwar between Ukraine and Russia hasn’t happened (yet), experts say Guardian https://www.theguardian.com/technology/2022/mar/09/catastrophic-cyber-war-ukraine-russia-hasnt-happened-yet-experts-say] SW 6-16-2022

Joe Biden pre-emptively warned Russia that the US is “prepared to respond” to any attacks on critical infrastructure, and others have warned for years of a “Cyber Pearl Harbor”. But thus far, experts say, it has been relatively quiet on the cyber warfront. “Though it would be foolhardy to rule it out in the future, we have not yet seen the completely destructive attacks on Ukraine infrastructure some anticipated,” said Glenn S Gerstell, former general counsel of the National Security Agency and Central Security Service. Fears of cyber warfare are stoked by a long history of international attacks coordinated out of Russia. The country was behind a large-scale attack on Ukraine’s power grid in 2015 in coordination with its annexation of Crimea. In 2017, Moscow unleashed on to Ukraine the data-wiping NotPetya virus, a destructive malware that ultimately spread globally. In addition, non-government Russian hackers have been linked to several brazen hacking schemes in past years, including the debilitating 2021 ransomware hack of the Colonial pipeline in the US. Coinciding with its invasion of Ukraine, Russia unleashed a number of smaller hacks – starting in January when more than 70 Ukrainian websites were defaced and separate cyber-attacks knocked out government websites including the ministry of foreign affairs and the education ministry. While these attacks have been “significant and unprecedented”, according to Aaron Turner of California cybersecurity firm Vectra, they have “not yet been catastrophic”. That is largely because no international power yet wants to be the one to cast the first stone in a cyber third world war, he said. “We have most likely reached a sort of detente, where both sides understand that catastrophic cyber-attacks will most likely result in mutually assured destruction of systems,” he added. National powers are also now better prepared to stave off attacks than they were previously, so it is possible some larger hacks have been quietly thwarted, experts said. The US has invested billions in cyber defense resources – both from private and public sources. Ukraine spent the past seven years in the wake of its power grid attack in 2015 steeling its infrastructure. “There has been a lot of thought and hard work put into preparing for an all-out assault on the cyber domain,” said Theresa Payton, cybersecurity expert and former White House chief information officer. “If we were to experience a hit to critical infrastructure, there are many playbooks in place to avoid sustained outages.

### 1nc – No Escalation

#### No scenario for cyber escalation.

Erica D. Borghard 19, Assistant Professor in the Army Cyber Institute at the United States Military Academy at West Point, and Shawn W. Lonergan, Assistant Professor of International Relations in the Department of Social Science at USMA, “Cyber Operations as Imperfect Tools of Escalation”, Strategic Studies Quarterly, Fall 2019, p. 123-124

However, there are important empirical reasons to suspect that the risks of cyber escalation may be exaggerated. Specifically, if cyberspace is in fact an environment that (perhaps even more so than others) generates severe escalation risks, why has cyber escalation not yet occurred? Most interactions between cyber rivals have been characterized by limited volleys that have not escalated beyond nuisance levels and have been largely contained below the use-of-force threshold.5 For example, in a survey of cyber incidents and responses between 2000 and 2014, Brandon Valeriano et al. find that “rivals tend to respond only to lower-level [cyber] incidents and the response tends to check the intrusion as opposed to seek escalation dominance. The majority of cyber escalation episodes are at a low severity threshold and are non-escalatory. These incidents are usually ‘tit-for- tat’ type responses within one step of the original incident.”6 Even in the two rare examples in which states employed kinetic force in response to adversary cyber operations—the US counter-ISIL drone campaign in 2015 and Israel’s airstrike against Hamas cyber operatives in 2019—the use of force was circumscribed and did not escalate the overall conflict (not to mention that force was used against nonstate adversaries with limited potential to meaningfully escalate in response to US or Israeli force).7

We posit that cyber escalation has not occurred because cyber operations are poor tools of escalation. In particular, we argue that this stems from key characteristics of offensive cyber capabilities that limit escalation through four mechanisms. First, retaliatory offensive cyber operations may not exist at the desired time of employment. Second, even under conditions where they may exist, their effects are uncertain and often relatively limited. Third, several attributes of offensive cyber operations generate important tradeoffs for decision-makers that may make them hesitant to employ capabilities in some circumstances. Finally, the alternative of cross-domain escalation—responding to a cyber incident with noncyber, kinetic instruments—is unlikely to be chosen except under rare circumstances, given the limited cost-generation potential of offensive cyber operations. In this article, we define cyber escalation and then explore the implications of the technical features and requirements for offensive cyber operations. We also consider potential alternative or critical responses to each of these logics. Finally, we evaluate the implications for US policy making.

### 1nc – Private Sector Solves

#### No systemic risk – big tech is patching up holes.

Chung ’21 [Ingrid; August 30; writer; National Review, “Big Tech Is Doing the Right Thing on Cybersecurity,” https://www.nationalreview.com/corner/big-tech-is-doing-the-right-thing-on-cybersecurity/; KP]

President Joe Biden recently met with Big Tech executives to discuss how to improve cybersecurity after recent cyberattacks in which government software contractor Solarwinds and oil pipeline Colonial Pipeline were targeted. Leading tech corporations, including IBM, Google, and Amazon, will all try to improve cybersecurity by investing in the training of personnel in this field and upgrading their respective encryption and security systems. Microsoft has also committed to investing $150 million in upgrades for cybersecurity systems of government agencies. Big Tech may not always do the right thing, but these plans to enhance cybersecurity are certainly something that we can all stand behind.

In recent years, as the Internet has become increasingly influential and indispensable, cybersecurity has, correspondingly, become an increasingly prominent threat to not only citizens’ privacy but also to national security. Former national-security adviser John Bolton explained the significance of cybersecurity to national defense in a recent National Review article, in which he characterized threats from cyberspace as “a multiplicity of hidden, ever-changing threats.” A recent report by the Heritage Foundation raised concern over espionage, trading of secrets, and the disruption of military commands and communication potentially being conducted in the cyber domain.

The effective regulation of cyberspace, a relatively new front for modern warfare characterized by its elusiveness and lack of boundaries, is sometimes challenging. Laxness in cybersecurity, however, has often led to catastrophic consequences. For instance, the WannaCry Ransomware Cyber Attack in 2017, in which files in affected computer systems were locked until ransom was paid for their decryption, affected approximately 200,000 computers in 150 countries and led to enormous financial costs. Victims of the cyber-extortion scheme included entities from government agencies such as the English National Health Service to major international corporates such as Boeing.

It is well established that both the state and leading tech corporations have a legitimate interest in enhancing cybersecurity. The government is responsible for engaging in national defense in the cyber domain and tech corporations are obligated to protect the privacy of their users, whose personal information is often entrusted to them.

Big Tech’s plans to cooperate with the government to improve cybersecurity through financial investments appears to be promising. While it may be difficult to predict the effectiveness of such investments, the fact that Big Tech and the government are placing the enhancement of cybersecurity close to the top of their agenda and are committing to coordinated efforts is good news. Big Tech, with its financial prowess derived from the sheer size of the industry, and a unique relationship with the use of cyberspace, is uniquely positioned to materially contribute to state-led efforts to secure cyberspace. Furthermore, investing in education on cybersecurity of employees may also be useful in raising awareness and amplifying the industry’s collective concern over capacity to combat cyberattacks in the long run.

### 2nc – Deterrence Solves

#### Status quo deterrence and norms are effective at preventing attacks

David **Lonsdale 17**, School of Law and Politics, University of Hull, Cottingham Road, Lonsdale, David J. “Warfighting for Cyber Deterrence: A Strategic and Moral Imperative.” Philosophy & Technology, Feb. 2017. CrossRef, doi:10.1007/s13347-017-0252-8.

3.4 The Failure of Cyber Deterrence? The potency of cyber deterrence is difficult to judge. This is partly because there exists no consensus on what constitutes an act of sufficient cyber aggression. Therefore, it is not entirely clear what is to be deterred. Where exactly the threshold for response should be will be discussed in section three of this paper. For now, we can state that low-level nuisance attacks are a daily occurrence. For example, U.S. military networks are probed and scanned millions of times each day (Work 2015, 1). Similarly, acts of cyber espionage are reasonably common. However, what is also evident is the lack of major cyber attacks. For a while, Stuxnet, Wiper, Shamoon and Bronze Soldier appeared to signal the rise of cyber attack as a potent new instrument of policy. However, medium to large-scale attacks have essentially dried-up. Indeed, reflecting the empirical evidence, and marking a shift in tone, in his September 2015 testimony to the Senate Armed Services Committee, Director of National Intelligence, James Clapper, talked down the possibility of an ‘electronic Pearl Harbor’. Instead, he focused on ongoing ‘low-to-moderate’ level threats (Clapper 2015, 2). What does this all tell us? Is deterrence working? If one considers low-to-moderate threats as deterrable, then the answer would seem to be no. From this perspective, and according to some policy makers, deterrence is already failing. In a 2015 Senate Armed Services Committee Hearing, Chairman John McCain was scathing in his assessment: ‘Our adversaries view our response ... as timid and ineffectual. Put simply, the problem is a lack of deterrence. The administration has not demonstrated to our adversaries that the consequence of continued cyber attacks against us outweigh the benefit.’ (Takala 2015) However, if we take the view that cyber deterrence should really concern itself only with large-scale attacks, the picture is more positive. Indeed, Valeriano and Maness (2015) have identified considerable levels of restraint in state cyber behaviour. This could be due to a lack of confidence in the strategic utility of cyber attack. It may also reflect the development of norms against aggressive forms of cyber behaviour and the efficacy of deterrence. Indeed, norms increasingly form part of ‘complex deterrence’, within which military and non-military elements operate together. In cyberspace, although a settled understanding of universal rules of behaviour is still lacking, norms appear to be crystalising around acceptable forms of intrusion rather than a blanket non-use position (Stevens 2012, 25). This may explain the continuance of lowlevel probes whilst large attacks have trailed off.

#### No large-scale cyberattacks---attribution deters AND complexity overwhelms despite technical advancements.

Miguel Alberto N. Gomez, 11-6-2018 - senior researcher at the Center for Security Studies at ETH Zurich; "In Cyberwar, There Are Some (Unspoken) Rules," Foreign Policy, https://foreignpolicy.com/2018/11/06/in-cyberwar-there-are-some-unspoken-rules-international-law-norms-north-korea-russia-iran-stuxnet/

Unlike conventional instruments, cyberoperations do not come with a return address. Technical evidence such as an IP address provides victims with a possible source but not necessarily the identity of the attacker. Furthermore, the presence of certain artifacts does not confirm the intent of the aggressor. Malicious code for use in espionage can just as well be employed as a first step for later, more damaging operations. Taken together, these factors would seem to encourage instability within cyberspace, as Wheeler argues. However, when viewed through the lens of preexisting strategic interactions and interests, the opposite may in fact be true.

Attribution becomes less of an obstacle when judgments are informed by tactical and strategic analysis. For instance, the appearance of individuals in unmarked uniforms carrying modern Russian weaponry in Ukraine were attributable to Russia, given the characteristics of these individuals as well as the surrounding context that preceded their appearance.

Different actors behave in a distinct manner that allows analysts—private threat assessment organizations and national intelligence services alike—to identify and classify individuals and groups. When analyzed alongside the prevailing political, economic, and military environment, both the identity and intent of the supposedly nonattributable actor usually become clearer. The intent of those deploying Stuxnet limited the pool of suspects to those with both the intent and the capabilities to execute this operation. Without the benefit of anonymity, aggressors are less inclined to engage in activities that significantly alter the current military balance for fear of provoking the opposite party.

For example, the long-running series of defacements and denial-of-service operations between India and Pakistan reflects this dynamic. Given the stable nature of this rivalry, both sides have opted for a tit-for-tat approach with respect to disruptive behavior. The defacement of an Indian website is met with the defacement of a corresponding Pakistani website in a matter of days with neither side opting for a more vigorous response to the provocations of the other.

The aftermath of Stuxnet prompted Iran to act more aggressively in cyberspace in the years following its discovery, but Tehran’s operations did not do much damage. Furthermore, with states reserving the right to respond with conventional military means to cyberthreats, the necessity for restraint becomes even greater.

Because decision-makers know the risks, cybercapable states routinely punch below their weight or decide to employ cyberoperations in a limited manner. A review of cyberoperations from 2006 to 2016 highlights that despite the advancements of numerous actors, operations capable of causing physical damage are limited. More recently, the announcement that the United States would deter Russia from interfering in its midterm elections by calling it out rather than using more aggressive means underlines this point.

This applies to the targeting of critical infrastructure, such as power grids and water treatment facilities, managed by industrial control systems that are demonstrated to be vulnerable to relatively simple exploits. When a state decides to target industrial controls, it does so with a specific intent that is informed by its strategic objectives. These objectives are discernible through its actions in other domains. These constraints even apply to perceived rogue states such as North Korea.

A review of North Korean cyberoperations from 2008 to 2014 illustrates that most of Pyongyang’s attacks caused low-level disruptions to private and nonmilitary systems of adversaries, which include the United States, Japan, and South Korea. In addition, these often coincided with significant historical, political, or military events. The same is true in the case of Iran. The nature and timing of these incidents is telling, as a similar pattern is observed with respect to the physical domain. North Korean behavior, barring its invasion of South Korea in 1950, has not been severe enough to invite a massive response. Provocations such as missile tests or the shelling of a South Korean-held island have invited international condemnation or a limited military response—but no more and with limited impact on North Korean behavior.

Although the 2014 Sony Pictures hack, which leaked confidential information and later involved physical threats against cinemas that screened The Interview, may appear to be a departure from this behavior, the operation did not disrupt the current strategic balance between North Korea and its adversary, in this case the United States. Nor did the U.S. government seem to think the hack merited a more vigorous response other than the recent complaint filed by the U.S. Justice Department. For the most part, the intent of the Sony hack appears to have been meant to signal the North Korean regime’s displeasure through a display of its prowess in cyberspace but no more. Even with the more recent WannaCry ransomware attack, its effects, while broad in scope, had no lasting strategic implications that might have resulted in escalation.

Countries that have invested significant resources in cyberspace don’t lack the ability to act more effectively within this domain. They are making a conscious decision to rely on less sophisticated operations based on their strategic calculus—the same calculus that leads a government such as North Korea’s to employ violent rhetoric and limited military operations to signal its displeasure without risking direct confrontation.

If critical industrial control systems are so easily compromised, one would expect governments to target these vulnerable systems more frequently rather than resort to mere disruption. While reports do suggest that North Korea has the capability to disrupt critical infrastructure such as power grids, acting on this is another matter altogether—much in the same way that having significant conventional military power does not merit its immediate use. There would be grave consequences.

Cybercriminals and script kiddies may see in these vulnerable systems an opportunity for profit or mischief. But attributional analysis that looks beyond technological features and includes tactical and strategic attributes can help distinguish between state-associated and independent criminal actors.

There is a vast body of experience in dealing with cases of cybercrime. While the corresponding institutions and legislation are far from perfect, they do offer a course of action if actors are classified under this category. Subjecting state-associated actors to this form of punishment, however, may not be as effective in deterring malicious behavior in this domain. Previous indictments against Chinese hackers appear to have had limited effect in deterring economic espionage. It is too early to tell if recent legal actions against North Korea, Russia, and China will have any noticeable effects in cyberspace.

Wheeler correctly presents cyberspace as a vulnerable domain that continues to lack a set of norms that regulates aggressive tendencies. But that doesn’t mean that state actors will immediately take the opportunity to fully exploit this situation to further their interests. They are acutely aware of the consequences of overly aggressive cyberoperations and therefore actively attempt to limit the impact of their activities by either narrowing the scope of their operations or resorting to techniques that do minimal damage and are easily contained.

Adequate health care, housing, education, and clean water and air are increasingly out of reach for large sections of the population, even in wealthy countries in North America and Europe, while transportation is becoming more difficult in the United States and many other countries due to irrationally high levels of dependency on the automobile and disinvestment in public transportation. Urban structures are more and more characterized by gentrification and segregation, with cities becoming the playthings of the well-to-do while marginalized populations are shunted aside. About half a million people, most of them children, are homeless on any given night in the United States.14 New York City is experiencing a major rat infestation, attributed to warming temperatures, mirroring trends around the world.15

In the United States and other high-income countries, life expectancy is in decline, with a remarkable resurgence of Victorian illnesses related to poverty and exploitation. In Britain, gout, scarlet fever, whooping cough, and even scurvy are now resurgent, along with tuberculosis. With inadequate enforcement of work health and safety regulations, black lung disease has returned with a vengeance in U.S. coal country.16 Overuse of antibiotics, particularly by capitalist agribusiness, is leading to an antibiotic-resistance crisis, with the dangerous growth of superbugs generating increasing numbers of deaths, which by mid–century could surpass annual cancer deaths, prompting the World Health Organization to declare a “global health emergency.”17 These dire conditions, arising from the workings of the system, are consistent with what Frederick Engels, in the Condition of the Working Class in England, called “social murder.”18

At the instigation of giant corporations, philanthrocapitalist foundations, and neoliberal governments, public education has been restructured around corporate-designed testing based on the implementation of robotic common-core standards. This is generating massive databases on the student population, much of which are now being surreptitiously marketed and sold.19 The corporatization and privatization of education is feeding the progressive subordination of children’s needs to the cash nexus of the commodity market. We are thus seeing a dramatic return of Thomas Gradgrind’s and Mr. M’Choakumchild’s crass utilitarian philosophy dramatized in Charles Dickens’s Hard Times: “Facts are alone wanted in life” and “You are never to fancy.”20 Having been reduced to intellectual dungeons, many of the poorest, most racially segregated schools in the United States are mere pipelines for prisons or the military.21

More than two million people in the United States are behind bars, a higher rate of incarceration than any other country in the world, constituting a new Jim Crow. The total population in prison is nearly equal to the number of people in Houston, Texas, the fourth largest U.S. city. African Americans and Latinos make up 56 percent of those incarcerated, while constituting only about 32 percent of the U.S. population. Nearly 50 percent of American adults, and a much higher percentage among African Americans and Native Americans, have an immediate family member who has spent or is currently spending time behind bars. Both black men and Native American men in the United States are nearly three times, Hispanic men nearly two times, more likely to die of police shootings than white men.22 Racial divides are now widening across the entire planet.

Violence against women and the expropriation of their unpaid labor, as well as the higher level of exploitation of their paid labor, are integral to the way in which power is organized in capitalist society—and how it seeks to divide rather than unify the population. More than a third of women worldwide have experienced physical/sexual violence. Women’s bodies, in particular, are objectified, reified, and commodified as part of the normal workings of monopoly-capitalist marketing.23

The mass media-propaganda system, part of the larger corporate matrix, is now merging into a social media-based propaganda system that is more porous and seemingly anarchic, but more universal and more than ever favoring money and power. Utilizing modern marketing and surveillance techniques, which now dominate all digital interactions, vested interests are able to tailor their messages, largely unchecked, to individuals and their social networks, creating concerns about “fake news” on all sides.24 Numerous business entities promising technological manipulation of voters in countries across the world have now surfaced, auctioning off their services to the highest bidders.25 The elimination of net neutrality in the United States means further concentration, centralization, and control over the entire Internet by monopolistic service providers.

Elections are increasingly prey to unregulated “dark money” emanating from the coffers of corporations and the billionaire class. Although presenting itself as the world’s leading democracy, the United States, as Paul Baran and Paul Sweezy stated in Monopoly Capital in 1966, “is democratic in form and plutocratic in content.”26 In the Trump administration, following a long-established tradition, 72 percent of those appointed to the cabinet have come from the higher corporate echelons, while others have been drawn from the military.27

War, engineered by the United States and other major powers at the apex of the system, has become perpetual in strategic oil regions such as the Middle East, and threatens to escalate into a global thermonuclear exchange. During the Obama administration, the United States was engaged in wars/bombings in seven different countries—Afghanistan, Iraq, Syria, Libya, Yemen, Somalia, and Pakistan.28 Torture and assassinations have been reinstituted by Washington as acceptable instruments of war against those now innumerable individuals, group networks, and whole societies that are branded as terrorist. A new Cold War and nuclear arms race is in the making between the United States and Russia, while Washington is seeking to place road blocks to the continued rise of China. The Trump administration has created a new space force as a separate branch of the military in an attempt to ensure U.S. dominance in the militarization of space. Sounding the alarm on the increasing dangers of a nuclear war and of climate destabilization, the distinguished Bulletin of Atomic Scientists moved its doomsday clock in 2018 to two minutes to midnight, the closest since 1953, when it marked the advent of thermonuclear weapons.29

Increasingly severe economic sanctions are being imposed by the United States on countries like Venezuela and Nicaragua, despite their democratic elections—or because of them. Trade and currency wars are being actively promoted by core states, while racist barriers against immigration continue to be erected in Europe and the United States as some 60 million refugees and internally displaced peoples flee devastated environments. Migrant populations worldwide have risen to 250 million, with those residing in high-income countries constituting more than 14 percent of the populations of those countries, up from less than 10 percent in 2000. Meanwhile, ruling circles and wealthy countries seek to wall off islands of power and privilege from the mass of humanity, who are to be left to their fate.30

More than three-quarters of a billion people, over 10 percent of the world population, are chronically malnourished.31 Food stress in the United States keeps climbing, leading to the rapid growth of cheap dollar stores selling poor quality and toxic food. Around forty million Americans, representing one out of eight households, including nearly thirteen million children, are food insecure.32 Subsistence farmers are being pushed off their lands by agribusiness, private capital, and sovereign wealth funds in a global depeasantization process that constitutes the greatest movement of people in history.33 Urban overcrowding and poverty across much of the globe is so severe that one can now reasonably refer to a “planet of slums.”34 Meanwhile, the world housing market is estimated to be worth up to $163 trillion (as compared to the value of gold mined over all recorded history, estimated at $7.5 trillion).35

The Anthropocene epoch, first ushered in by the Great Acceleration of the world economy immediately after the Second World War, has generated enormous rifts in planetary boundaries, extending from climate change to ocean acidification, to the sixth extinction, to disruption of the global nitrogen and phosphorus cycles, to the loss of freshwater, to the disappearance of forests, to widespread toxic-chemical and radioactive pollution.36 It is now estimated that 60 percent of the world’s wildlife vertebrate population (including mammals, reptiles, amphibians, birds, and fish) have been wiped out since 1970, while the worldwide abundance of invertebrates has declined by 45 percent in recent decades.37 What climatologist James Hansen calls the “species exterminations” resulting from accelerating climate change and rapidly shifting climate zones are only compounding this general process of biodiversity loss. Biologists expect that half of all species will be facing extinction by the end of the century.38

If present climate-change trends continue, the “global carbon budget” associated with a 2°C increase in average global temperature will be broken in sixteen years (while a 1.5°C increase in global average temperature—staying beneath which is the key to long-term stabilization of the climate—will be reached in a decade). Earth System scientists warn that the world is now perilously close to a Hothouse Earth, in which catastrophic climate change will be locked in and irreversible.39 The ecological, social, and economic costs to humanity of continuing to increase carbon emissions by 2.0 percent a year as in recent decades (rising in 2018 by 2.7 percent—3.4 percent in the United States), and failing to meet the minimal 3.0 percent annual reductions in emissions currently needed to avoid a catastrophic destabilization of the earth’s energy balance, are simply incalculable.40

Nevertheless, major energy corporations continue to lie about climate change, promoting and bankrolling climate denialism—while admitting the truth in their internal documents. These corporations are working to accelerate the extraction and production of fossil fuels, including the dirtiest, most greenhouse gas-generating varieties, reaping enormous profits in the process. The melting of the Arctic ice from global warming is seen by capital as a new El Dorado, opening up massive additional oil and gas reserves to be exploited without regard to the consequences for the earth’s climate. In response to scientific reports on climate change, Exxon Mobil declared that it intends to extract and sell all of the fossil-fuel reserves at its disposal.41 Energy corporations continue to intervene in climate negotiations to ensure that any agreements to limit carbon emissions are defanged. Capitalist countries across the board are putting the accumulation of wealth for a few above combatting climate destabilization, threatening the very future of humanity.

#### And, actors self-deter --- cyber is unique because defenders have the absolute defense of disconnecting. If attacks get strong enough, the internet itself becomes a bad deal for the defender, which also screws the attacker by denying lower-level cyber coercion and espionage

Jon **Lindsay and** Erik **Gartzke 14**, Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies, AND Erik Gartzke is Professor and Director of cPASS at the Department of Political Science @ UCSD, Lindsay, Jon R., and Erik Gartzke. “Coercion through Cyberspace: The Stability-Instability Paradox Revisited.” The Power to Hurt: Coercion in the Modern World, Oct. 2014.

Perhaps the simplest form of cross domain response to cyber threats is to forgo the use of the cyber domain altogether. While it is hard if not impossible to limit exposure to nuclear weapons and even a determined conventional assault, the risk of cyber attack can be completely eliminated by disconnection from digital networks. The internet is an artificial environment and connection to it is voluntary. Individuals, organizations, and states retain the ability to unplug completely, limit their online transactions, or erect various barriers to connection. Obviously disconnection is not very feasible commercially, socially, and militarily today, but this is more of an indicator of how positive the benefits of interconnection are compared to the perceived risks. If the risks were perceived as extreme, then firms and states could go back to making a living as they did before 1991 (when WWW went public). This is a cross-domain threat because it entails exiting the cyber domain altogether to leverage more traditional economic and military transactions. The threat of disconnection follows from the more general logic of international organizations, where contracts must be self-enforcing.44 On the internet as in institutions, ties among egoistic actors under anarchy must be mutually beneficial. If the internet is a bad deal for actors, they can throw up boundaries or exit cyberspace altogether. If repeated exposure to adversarial exploitation causes states to lose more than they gain from being online, then they can undermine the attacker’s very means for accessing the victim. The threat of voluntary disconnection is especially relevant for repeated interactions, or repeated exploitation, rather than a one-shot “bolt from the blue” cyber attack (which is better countered with cross-domain retaliation). The threat of disconnection is implicit in the voluntary nature of connection to the internet, and the potential loss of the ability to make future attacks exercises a deterrent effect on attacks in the present. An aggressor who does not want to lose the cyber adjuncts for espionage and disruption it has invested so much in developing will show restraint in their employment. This does not mean that coercion cannot take place online, but it is bounded by excess value. One implication is that the countries that can be most coerced on the internet will be those that have the most to lose by leaving it.

### 2nc – No Escalation

#### Cyber attacks are small, unlikely, and don’t escalate

**Blessing, 22** (Jason Blessing,fellow at the Foreign Policy Institute at the School of Advanced International Studies at Johns Hopkins University, a consulting fellow with the International Institute for Strategic Studies, and a US Institute of Peace–Minerva Peace and Security Scholar. Dr. Blessing has a PhD in political science (international relations and public policy). 4-25-2022, accessed on 6-16-2022, American Enterprise Institute - AEI, "The Russian Cyber Threat Is Here to Stay and NATO Needs to Understand It | American Enterprise Institute - AEI", https://www.aei.org/op-eds/the-russian-cyber-threat-is-here-to-stay-and-nato-needs-to-understand-it/)ao

Since the Russian invasion of Ukraine, the Biden administration has escalated warnings about likely Russian cyber-attacks on American infrastructure and business. More worrying still, cyber alarmists like Senate Intelligence Committee Chairman Mark Warner, D-Va., have suggested that cyber-attacks from the Kremlin could be acts of war that trigger NATO’s collective defense.

This sky-is-falling delusion, particularly from leaders with access to classified intelligence, is at best counterproductive and at worst dangerous.

Cyber-attacks are rarely acts of war, and treating them as if they are undermines NATO’s ability to deal with real threats short of cyber war.

NATO has only invoked Article 5 – which triggers a collective response – once and that was after the 9/11 attacks.

Cyber-attacks are unlikely to destroy buildings and kill thousands in an instant. While collective defense extends to cyberspace, few operations could realistically be a cause for war.

This would include cyber-attacks resulting in death or damage like traditional military operations or coordinated assaults that take the power grid or entire economic sectors offline. These scenarios are unlikely though: such attacks require far too much time, funding, manpower, and control. Instead, most attacks temporarily overwhelm servers with traffic, deny network access, hold computers hostage, and steal or delete data.

Even if allies wanted to trigger Article 5 over cyber operations, disagreements about the definitions of threats, origins of attacks, and pain thresholds in cyberspace can derail the process.

Collective retaliation requires a unanimous vote across NATO; building unity across these points is nearly impossible for most cyber activity. Unlike missile attacks or tanks in the streets, few “red lines” exist to distinguish cybercrime, cyber espionage, and cyber disruption from digital acts of war.

#### Cyber-attacks won’t escalate – fear of retaliation causing irreversible damages acts as deterrent against dangers in the cyber space

Fischer 19

a security professional, working in the German defense sector with focus on counter-UAS Solutions. He looks back on twelve years of service in the German military (Bundeswehr) as a military police officer. He graduated its Master’s program of International Security Studies concentrating on cyber security. The Concept of Deterrence and its Applicability in the Cyber Domain, The Quarterly Journal, https://connections-qj.org/article/concept-deterrence-and-its-applicability-cyber-domain

Cyberspace as the fifth domain is omnipresent, and all developed states increasingly realize that international relations and typical domains of statehood change in the face of global digitization. With the advent of game-changing technologies, traditional statecraft tools, such as deterrence, seem disregarded as outdated in the national security strategy building process. Advanced states, in particular, depend heavily on an open and safe cyber domain but, at the same time, suffer from manifold vulnerabilities. The recent past showed that sophisticated cyberattacks have the potential to disrupt governments, economies, and societies significantly and therefore pose a threat to core security interests. As a classical tool in international relations, deterrence can help bolster national security interests, even if the cyber domain requires some special considerations. Therefore, the article explains the basic mechanisms of deterrence in the nuclear age and contemporary international relations, cyberspace’s legal framework, and possible ways to apply deterrence in the cyber domain. It aims to urge global leaders to thoroughly consider deterrence in the cyber domain as a powerful asset and to provide policymakers with options for action. Speaking about deterrence in the 21st century feels like excavating remnants of a bygone era. With the advent of nuclear technologies and mainly during the Cold war, deterrence was a topic not only for politicians and academia but also shaped the daily lives of millions, no matter which side of the ‘blocks’ they belonged to. Since then, deterrence diminished its presence in the public perception together with the nuclear arsenals of the great powers. What remains is still of enormous potential but as a tool of statecraft rather than a placeholder. Especially states face the gradual change of the traditionally state-centered setting of the international system, particularly in habitual domains of statehood, like security. The classical understanding of war and conflict blurs and the traditional state structures seem to be overstrained to respond with the classical tools, as the new type of conflict is multilayered (political, military, and economic, among others), conducted mostly by non-military means like propaganda and political agitation and amongst diverse state and non-state actors.[[1]](https://connections-qj.org/article/concept-deterrence-and-its-applicability-cyber-domain" \l "_ftn1" \o "),[[2]](https://connections-qj.org/article/concept-deterrence-and-its-applicability-cyber-domain" \l "_ftn2" \o ") In the face of daily and continuing attacks on governments and their organs,[[3]](https://connections-qj.org/article/concept-deterrence-and-its-applicability-cyber-domain" \l "_ftn3" \o ") the question persists: What keeps an actor in the cyber domain from carrying out the same attacks over and over again, or even climbing up the escalation ladder and causing irreversible harm, if it serves his interests. There seems to be no respect, no fear of retaliation, and no serious technical barriers in the cyber domain – or in other words, no deterrence. This article will survey if the concept of deterrence is only effective if it is tied to nuclear weaponry and if it becomes useless in a no longer (purely) nuclear but cyber-dominated international system. The author claims that this is not the case! Even in the cyber age, deterrence can be a powerful tool of statecraft and could contribute to the protection of state’s national security interests. To prove this hypothesis, this article will scrutinize the concept of deterrence by looking into the past that generated manifold experiences on that topic, to finally project the findings into present times. Therefore, existing concepts of deterrence and special implications of the cyber arena, together with the legal framework of the ever more digitized international system, will be examined to finally find effective ways to apply deterrence in cyber space. The following assumptions and exclusions are considered common ground:

#### Cyber attacks stay small – their ev fearmongers

Valeriano and Maness 15 – co-authors of Cyber War versus Cyber Realities, AND \*Senior Lecturer in Social and Political Sciences at the University of Glasgow, AND \*\*Visiting Fellow of Security and Resilience Studies at Northeastern University (Brandon and Ryan C., The Coming Cyberpeace: The Normative Argument Against Cyberwarfare, Foreign Affairs, <https://www.foreignaffairs.com/articles/2015-05-13/coming-cyberpeace>)

The era of cyberconflict is upon us; at least, experts seem to accept that cyberattacks are the new normal. In fact, however, evidence suggests that cyberconflict is not as prevalent as many believe. Likewise, the severity of individual cyber events is not increasing, even if the frequency of overall attacks has risen. And an emerging norm against the use of severe state-based cybertactics contradicts fear-mongering news reports about a coming cyberapocalypse. The few isolated incidents of successful state-based cyberattacks do not a trend make. Rather, what we are seeing is cyberespionage and probes, not cyberwarfare. Meanwhile, the international consensus has stabilized around a number of limited acceptable uses of cybertechnology—one that prohibits any dangerous use of force. Despite fears of a boom in cyberwarfare, there have been no major or dangerous hacks between countries. The closest any states have come to such events occurred when Russia attacked Georgian news outlets and websites in 2008; when Russian forces shut down banking, government, and news websites in Estonia in 2007; when Iran attacked the Saudi Arabian oil firm Saudi Aramco with the Shamoon virus in 2012; and when the United States attempted to sabotage Iran’s nuclear power systems from 2007 to 2011 through the Stuxnet worm. The attack on Sony from North Korea is just the latest overhyped cyberattack to date, as the corporate giant has recovered its lost revenues from the attack and its networks are arguably more resilient as a result. Even these are more probes into vulnerabilities than full attacks. Russia’s aggressions show that Moscow is willing to use cyberwarfare for disruption and propaganda, but not to inflict injuries or lasting infrastructural damage. The Shamoon incident allowed Iran to punish Saudi Arabia for its alliance with the United States as Tehran faced increased sanctions; the attack destroyed files on Saudi Aramco’s computer network but failed to do any lasting damage. The Stuxnet incident also failed to create any lasting damage, as Tehran put more centrifuges online to compensate for virus-based losses and strengthened holes in their system. Further, these supposedly successful cases of cyberattacks are balanced by many more examples of unsuccessful ones. If the future of cyberconflict looks like today, the international community must reassess the severity of the threat. Cyberattacks have demonstrated themselves to be more smoke than fire. This is not to suggest that incidents are on the decline, however. Distributed denial-of-service attacks and infiltrations increase by the minute—every major organization is probed constantly, but only for weaknesses or new infiltration methods for potential use in the future. Probes and pokes do not destabilize states or change trends within international politics. Even common cyber actions have little effect on levels of cooperation and conflict between states.

#### No miscalc or escalation­- cyber-attacks will stay below the threshold of causing violence

Jon **Lindsay 15**, Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies., Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction.” International Security, vol. 39, no. 3, Jan. 2015, pp. 7–47.

Exaggerated fears about the ~~paralysis~~ [deactivation] of digital infrastructure and growing concerns over competitive advantage exacerbate the spiral of mistrust. Closer consideration of domestic factors within China and China’s strategic interac- tion with the United States reveals a more complicated yet less worrisome situation. This article argues that for every type of purported Chinese cyber threat, there are also serious Chinese vulnerabilities and Western strengths that reinforce the political status quo. Cyberwar between the United States and China, much like U.S.-China conventional war, is highly unlikely. Nevertheless, the economically driven proliferation of information technology enables numerous instances of friction to emerge below the threshold of violence. From a technical perspective, cyber operations are often thought to be inexpensive and effective, but there are underappreciated institutional costs involved in their employment. Moreover, even if actors can overcome the operational barriers associated with ambitious cyber penetrations, they still have incentives to moderate the intensity of their exploitation in order to preserve the benefits that make exploitation worthwhile in the first place. This logic culminates in a relentlessly irritating but indefinitely tolerable stability in the cyber domain. China and the United States can look forward to chronic and ambiguous intelligence-counterintelligence contests across their networks, even as the internet facilitates productive exchange between them.

## No Terminal Impacts

### 1nc – No Russia War Impact

#### No Russia war or miscalc.

Bruusgaard 17 Kristin Ven Bruusgaard is a Stanton Nuclear Security Fellow at CISAC, Stanford University and a Ph.D. student at King’s College London. [The Myth of Russia’s Lowered Nuclear Threshold, 9-22-2017, https://warontherocks.com/2017/09/the-myth-of-russias-lowered-nuclear-threshold/]//BPS

Yet the evidence for a lowered Russian nuclear threshold is getting weaker by the day. First, there is very little hard evidence that de-escalation is part of Russia’s nuclear doctrine. In fact, Russia’s doctrinal statements indicate an increased rather than a decreased nuclear threshold. Second, the idea of lowering the nuclear threshold logically flows from a lack of conventional capabilities, while in fact Russia’s conventional capabilities are rapidly improving. Third, it is difficult to understand why Russia would want to pursue military adventurism that would risk all-out confrontation with a technologically advanced and nuclear-armed adversary like NATO. While opportunistic, and possibly even reckless, the Putin regime does not appear to be suicidal. Make no mistake: Nuclear weapons remain essential to Russian national security, and the deterrent utility of the largest nuclear arsenal in the world remains significant. Nuclear weapons remain the single most important deterrent asset Russia has. Still, Russia today is less, not more likely to use nuclear weapons than it was 10 or 15 years ago. Advances in conventional and non-military capabilities have made Russia less reliant on using nuclear weapons to deal with security threats. Russia has a broader range of tools to signal her resolve to a potential adversary than she did a decade ago. Officially declared Russian doctrine over the past seven years confirms this increased range of options. This was not always the case. Seventeen years ago, Russian leaders were indeed contemplating a lower nuclear threshold. NATO’s intervention in Kosovo made it clear that Russia’s conventional capabilities seriously lagged behind the West’s, leaving a deep and lasting impression on the Russian political and military leadership. Nuclear weapons came to be seen as Russia’s only trump card in the face of massive Western conventional (particularly air) superiority. This viewpoint produced a seminal article by Russian military theorists V. I. Levshin, A. V. Nedelin and M. E. Sosnovsky, “On the use of nuclear weapons to de-escalate military conflict”. The article explained how the limited use of nuclear weapons early in a conflict could convince an adversary of the risks associated with continuing aggression, thereby de-escalating the situation. There were several indications of a lowered nuclear threshold in this period, from the purported de-escalation strike with nuclear weapons in the 1999 Zapad exercise to the open-ended wording of the 2000 Russian military doctrine, which said nuclear weapons could be used “in situations that are critical to the national security of the Russian Federation.” Still, even at the height of perceived Russian conventional backwardness, the theory of nuclear de-escalation was never doctrinally codified or officially endorsed. Russia watchers were actively contemplating this reduced nuclear threshold at the time, but in a benign security environment, Western policymakers paid little attention to this strategy shift. Over the next two decades, Russia’s prescriptive solutions to strategic challenges would change. Analysts still pondering the lowered Russian nuclear threshold pay too little attention to this shift, focus in part on outdated elements of Russian strategy. Since the early 2000s, Russia’s declaratory nuclear strategy has actually become more restrictive. The current Russian military doctrine, issued in 2014, states that nuclear weapons can be used “when the very existence of the state is under threat,” compared to the more expansive conditions laid out in 2000. Nonetheless, many nuclear hawks claim that a classified document outlining nuclear deterrence strategy, which Russia retains in addition to the openly declared military doctrine, must spell out the nuclear de-escalation theory. This may be so: We have yet to see any leaked or other information on this. An alternate interpretation of the lack of official confirmation of the de-escalation theory is that this is not, in fact, a dominant aspect of Russian warfighting strategy. It would be nonsensical for the secret and public documents to blatantly contradict one another. The nuclear de-escalation concept was also controversial inside Russia. A number of theorists questioned whether using or threatening to use nuclear weapons early on would produce the desired effect, i.e. a cessation of hostilities rather than compelling the adversary to escalate in kind. Both Russian officials and analysts emphasized that the 2000 doctrine, with its increased reliance on nuclear weapons, was intended for a transitional phase, until conventional forces and other capabilities could contribute to more effective and more credible deterrence consisting of a broader range of military and non-military options. Many observers wanted a less risky and less nuclear-focused deterrence strategy as soon as this would be viable. By the late 2000s, discussions of “Russian strategic deterrence” had overtaken deliberations about nuclear de-escalation, and by 2010, this concept was part of the official military doctrine. The Russian strategic deterrence concept depicted the seamless integration of nuclear, conventional, and non-military capabilities to influence the adversary in times of peace, conflict, and war. The backbone of strategic deterrence was, of course, nuclear weapons. But crucially, it also entailed a range of assets, precisely in order to avoid an unhealthy dependence on nuclear weapons to compensate for conventional inferiority. Non-nuclear deterrence involves both military and non-military assets that can convince an adversary that the costs of aggression against Russia would outweigh any benefit. These include precision strike capabilities, effective command, control, intelligence, and reconnaissance capabilities, effective strategic assets such as aerospace defense forces and special operations forces, information warfare capabilities, and non-military tools such as diplomatic, economic, and political instruments of influence. These non-nuclear tools would add to the combined credibility of Russian deterrence, particularly in deterring regional conflicts and emerging threats, such as color revolutions. Nuclear weapons were still central under the strategic deterrence concept, but rather than taking on an elevated role to compensate for a lack of conventional options, they shifted toward a more normalized role in deterring large-scale aggression. By 2014, official Russian strategy documents reflected this development; the main novelty in the 2014 military doctrine was its introduction of non-nuclear deterrence: “A complex of foreign policy, military and military-technical measures aimed at preventing aggression against the Russian Federation through non-nuclear means.” At the height of Western post-Crimea stress syndrome and nuclear paranoia, the timing of this publication is interesting. If ever there was a perfect time to cement the Western perception of a Russian “madman” nuclear strategy, this would be it. The Russians missed it, opting instead for a concept that increased, rather than decreased, the requirements for nuclear use. The more conspiracy-prone may claim this is a classic Russian diversionary tactic. The problem is that deterrence only works if your adversary actually understands what your intentions and capabilities are. Declared and non-declared nuclear doctrines that point in opposite directions not only seem absurd; they also confuse your adversary and make deterrence less effective. This is all the more reason to pay attention to the clear message in Russian official doctrine, now reflecting a deterrence concept that had been developing among Russian theorists for a decade. Russia has been piling significant effort and resources into developing cutting-edge conventional capabilities, which further undermines the idea of a lowered threshold. Seeing the holistic Russian approach to strategic deterrence is essential for understanding the role of nuclear weapons in that strategy. The comprehensive modernization of Russia’s conventional armed forces and the development of a broad set of non-traditional tools of statecraft have enabled Russia to rely less on nuclear weapons to influence adversaries. To predict when and how Russia may use nuclear weapons, that is, Russia’s nuclear threshold, we need to understand how and when Russia may use these other tools to achieve similar goals. The list of capabilities that give Russia increased flexibility in a potential conflict is long. The precision strike regime’s impact on Russian capabilities is by far the most significant leap providing enhanced conventional deterrence. Indeed, conventional precision strike capabilities may take over some of the tasks that Moscow previously assigned to nuclear weapons. Russian military theorists such as A. A. Protasov, V. A. Sobolevskii and V. V. Sukhorutchenko explain how conventional strategic assets could carry out demonstration strikes or strikes inflicting unacceptable damage on an enemy to force him into submission---precisely the kind of tasks nuclear weapons would carry out under a de-escalation doctrine. Although it is difficult to know whether Russian operational planning incorporates these changes, we do know that these capabilities are becoming available to Russia---should it want to use them. Examples of the non-military tools Russia has been developing include offensive cyber capabilities, used for denial of services attacks in Estonia in 2007 and Georgia in 2008, and most likely, for kinetic attacks against critical infrastructure in Ukraine. Russia’s improved information operations capabilities, as seen in the disinformation campaigns seen in several European countries, can erode the will of another state’s political leadership or population. According to Russian General Staff Chief Valeriy Gerasimov, the center of gravity in modern warfare is not the enemy troops, but the population’s willingness to fight. A combination of military and non-military pressure may be sufficient to sway this willingness without the use of nuclear weapons.

### 2nc – No Russia War Impact

#### Russia and the US will both avoid nuclear use

Schulze ’22 (Dr. Matthias is the deputy head of the security division at the German Institute for International and Security Affairs (SWP). He also runs percepticon.de blog and podcast on cybersecurity issues, 4-15, 22, Can Russia and the West Avoid a Major Cyber Escalation?, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/can-russia-and-west-avoid-major-cyber)

The central premise of our argument is that **Russia and NATO member states will want to avoid a direct military clash at nearly all costs (**Putin’s desire to protect his regime from imminent collapse might be an exception). If anything, the tragedies of the war in Ukraine reveal the enormous economic and human costs of conventional battles involving the Russian military behemoth. **Although the risk of an accidental or unwanted war between Russia and NATO is always present and has increased, both sides will want to reduce it**. That is how to interpret Russian President Vladimir Putin’s recent allusion to nuclear war: He rattled the atom in order not to have to use it. Similarly, President Joe Biden’s warning about the certainty of “World War 3” if Russia attacked NATO was a rhetorical device to reduce its chances. **Both sides have signaled that they wish to avoid an epochal war among them; they threaten it in order not to fight it.** This is conventional deterrence thinking at its finest. Familiar red lines are reinforced so that all sides can see them plainly amid the crisis.

#### A War Between the U.S. and Russia Won’t Happen

(Vikas **Shukla**, July 8th 20**15**, author, “Russia vs. U.S. Nuclear War Is Highly Unlikely,” http://www.valuewalk.com/2015/07/russia-vs-u-s-nuclear-war-unlikely/)

Russia and the U.S. are aggressively upgrading their nuclear arsenal as tensions between the two countries continue to mount. Washington is sending hundreds of howitzers, tanks and other lethal weapons to Eastern Europe amid Russia’s ‘nuclear rhetoric.” It has fueled worries that even an accidental escalation could lead to a nuclear war. Only 2% probability of a nuclear war between Russia and the U.S. A Gallup poll conducted last year found that 50% Americans believe the country was headed back to Cold War. While the mainstream public opinion is highly pessimistic, there is very little chance of a nuclear war between the two powers. Russian political analyst Fyodor Lukyanov recently told Vox that “a war is not something that’s impossible anymore.” Even if the two countries engage in a conflict, could it lead to a nuclear war? Political analyst Jay Ulfelder, who runs the Dart-Throwing Chimp blog, conducted a survey. He asked people on the online political science expert communities two questions: What are the odds of a Russia vs U.S. war before 2020; and if such a conflict occurred, whether it would turn into a nuclear war. He collected responses and ran them through statistical analysis. Ulfelder found that only 11% people said there was a probability of war between the two countries. Conditional on war, there was 18% probability that one or both sides will resort to nuclear weapons. Ulfelder translated these figures into a single number: 2% probability of a nuclear war between the U.S. and Russia. Difference between mainstream public and expert opinion The results of his survey are in line with that of a survey by Teaching, Research, and International Policy (TRIP). TRIP asked scholars, “How likely is a war between the United States and Russia over the next decade? Please use the 0–10 scale with 10 indicating that war will definitely occur.” They received responses from 2,040 scholars. On a scale of 0-10, the average perceived risk of war with Russia was 2.55. Their opinions were dramatically different from the mainstream public opinion. On the occasion of the U.S. Independence Day, Russian President Vladimir Putin said in a message of greetings to President Obama that even though some disagreements exist between the U.S. and Russia, they could peacefully resolve the issues through dialogue. Putin said relations between Moscow and Washington were “a crucial factor for international stability.”

#### Accidental Nuclear War is Improbable

Starr 15 – Contributor that Write for the Bulletin @ the Atomic Scientists

(Steven Starr, Robin Collins, Robert Green, Emie Regehr, et al September 29th 2015, contributers that write for the bulletin for the atomic scientists, “New terminology to help prevent accidental nuclear war,” http://thebulletin.org/new-terminology-help-prevent-accidental-nuclear-war8773)

Since the advent of US and Russian nuclear-armed ballistic missiles and early warning systems, the danger has always existed that a false warning of attack—believed to be true—could cause either nation to inadvertently launch a responsive “retaliatory” strike with its own nuclear forces. Fear of a disarming nuclear strike, especially during a crisis, creates immense pressure to use-or-lose nuclear forces if an attack is detected. Because launch-ready ballistic missiles allow either side to launch a counter-strike before nuclear detonations confirm whether or not the perceived “nuclear attack” is real, the launch of a retaliatory strike would in reality be a preemptive nuclear first-strike, should the warning prove to be false—resulting in accidental nuclear war. This pressure applies to any nation that might develop the ability to launch before detonation; as a result, what the United States and Russia decide to do could conceivably act as a role model for others—depending, of course, on the unique circumstances of each country. Consequently, there have been many calls to eliminate, or at least “de-alert,” these launch-ready forces—that is, to institute changes to the weapons systems that will prevent an overly hasty launch. This approach would make it physically impossible to start a nuclear war by accident, in response to a false warning of attack. Unfortunately, there has not been much enthusiasm in either the United States or Russia for de-alerting or eliminating high-alert nuclear forces. Yet the recent, escalating tensions between the United States and Russia have increased the need for both nations to address the dangers posed by their launch-ready strategic nuclear weapons. Almost all US and most Russian silo-based intercontinental ballistic missiles (ICBMs)—as well as some of their submarine-launched ballistic missiles—remain at launch-ready status, capable of rapid launch within a maximum of 15 minutes after receiving a warning. These weapons are armed with strategic nuclear warheads, and the detonation of even one such warhead could kill hundreds of thousands of people. There is another way to reduce the risk of accidental nuclear war: Russia and the United States could each independently adopt a policy of not launching their nuclear-armed missiles before confirmation of a nuclear detonation on their respective territories. Such a policy would make it impossible to launch a responsive or reflexive nuclear strike based upon a false warning of attack. To help them reach such commitments, the diplomatic world should address a factor that has spawned confusion and controversy: nuclear terminology.

### 1nc – No Nuclear Hack Impact

#### No NC3 hacking.

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).

### 2nc – No Nuclear Hack Impact

#### It's false – totally disconnected from the internet.

Caylor ’16 [Matt; 2-1-16; Command and Staff College; “The Cyber Threat to Nuclear Deterrence,” War on the Rocks, <http://warontherocks.com/2016/02/the-cyber-threat-to-nuclear-deterrence/>]

The perception that cyber threats will ultimately undermine the relevance or effectiveness of nuclear deterrence is flawed in at least three keys areas. First among these is the perception that nuclear weapons or their command and control systems are similar to a heavily defended corporate network. The critical error in this analogy is that there is an expectation of IP-based availability that simply does not exist in the case of American nuclear weapons — they are not online. Even with physical access, the proprietary nature of their control system design and redundancy of the National Command and Control System (NCCS) makes the possibility of successfully implementing an exploit against either a weapon or communications system incredibly remote. Also, whereas the cyber domain is characterized by significant levels of risk due to a combination of bias toward automated safeguards and the liability of single human failures, nuclear weapon safety and surety are predicated on balanced elements of stringent human interaction and control. From two-person integrity in physical inspections and loading, to the rigorous mechanisms and authority required for weapons release, human beings serve as a multi-factor safeguard while retaining the ultimate role to protect the integrity of nuclear deterrence against cyber threats.

To a large degree, the potential vulnerabilities caused by wireless communications and physical intrusions into areas holding nuclear material are already mitigated via secure communications that are not linked to the outside and multiple layers of physical security systems. While there has been a great deal of publicity surrounding the Y-12 break-in of 2012, the truth is that the three people involved never got near any nuclear material or technology.

Without state-level resourcing in the billions of dollars, the technical sophistication required to pursue a Stuxnet-like attack against nuclear weapons is most likely beyond the capability of even the most gifted group of hackers. For all intents, this excludes terrorist organizations and cyber criminals from the field of threats and restricts it to those nations that already possess nuclear weapons. Nuclear-weapon states, however, have the full-spectrum cyber threat capability referenced in the Defense Science Board report and would most likely be influenced by an understanding of the elements of classic nuclear deterrence strategy. In the case of first strike, no cyber weapon could be expected to perform at a rate higher than any conventional anti-nuclear capability (i.e., not 100 percent effective). Therefore, an adversary’s nuclear threat would be perceived to endure, thereby negating and dissuading the effort to use and employ a cyber weapon against an adversary’s nuclear force. Additionally, just as missile defense systems have been historically controversial due to perceived destabilizing effects, it is reasonable to conclude that these nuclear-weapon states would view the attempt to deploy a cyber capability against their nuclear stockpiles from a similar perspective.

Finally, the very existence of nuclear weapons is often enough to alter the risk analysis of an adversary. With virtually no chance of remote or unauthorized detonation (which would be the desired results of a sabotage event), the most probable cyber threat to any nuclear stockpile is that of espionage. Attempted cyber intrusions at the U.S. National Nuclear Security Agency (NNSA) and its efforts to bolster cybersecurity initiatives provide clear evidence that this is already underway. However, theft of design information or even more robust intelligence on the location of stored nuclear weapons cannot eliminate the potential destruction that even a handful of nuclear weapons can bring to an adversary. Knowledge alone, particularly the imperfect knowledge that cyber espionage is likely to offer, is incapable of drastically altering an adversary’s risk calculus. In fact, quite the opposite is true. An adversary with greater understanding of the nuclear capabilities of a rival is forced to consider courses of action to prevent escalation, potentially increasing the credibility of a state’s nuclear deterrence.

Despite the growing sophistication in cyber capabilities and the willingness to use them for espionage or in concert with kinetic attack, the strategic value of nuclear weapons has not been diminished. The insulated architecture combined with a robust and redundant command-and-control system makes the existence of any viable cyber threat of exploitation extremely low. With the list of capable adversaries limited by both funding and motivation, it is highly unlikely that any nation will possess, or even attempt to develop, a cyber weapon sufficient to undermine the credibility of nuclear weapons. In both psychological and physical terms, the threat of the megabyte will never possess the ability to overshadow the destructive force of the megaton. Although the employment of cyberspace for military effect has brought new challenges to the international community, the role of nuclear weapons and their associated deterrence against open and unconstrained global aggression are as relevant now as they were in the Cold War.

#### No nuclear hacking---US C2 is rigorously firewalled and isolated from other channels, making access impossible---two-person integrity and multi-layered safeguards prevent miscalc---that’s Caylor

#### Hacking impossible. Nukes aren’t online.

Fung 16, MSc, international relations. Reporter focusing on telecommunications, media, and competition. Citing Maj. General Jack Weinstein. (Brian, 5-26-2016, "The real reason America controls its nukes with ancient floppy disks", *Washington Post*, https://www.washingtonpost.com/news/the-switch/wp/2016/05/26/the-real-reason-america-controls-its-nukes-with-ancient-floppy-disks/)

As it happens, a similar logic underpins the U.S. military’s continued use of floppy disks. The fact that America’s nuclear forces are disconnected from digital networks actually acts as a buffer against hackers. As Maj. General Jack Weinstein told CBS’s “60 Minutes” in 2014: Jack Weinstein: I'll tell you, those older systems provide us some -- I will say huge safety when it comes to some cyber issues that we currently have in the world. Lesley Stahl: Now, explain that. Weinstein: A few years ago we did a complete analysis of our entire network. Cyber engineers found out that the system is extremely safe and extremely secure on the way it's developed. Stahl: Meaning that you're not up on the Internet kind of thing? Weinstein: We're not up on the Internet. Stahl: So did the cyber people recommend you keep it the way it is? Weinstein: For right now, yes. In other words, the rise of hackers and cyberwarfare is exactly why even technologically obsolete systems can still serve a valuable purpose.

### 1nc – No Grid Impact

#### No grids impact

Borghard and Lonergan 19 -- Erica Boghard, Assistant Professor at the Army Cyber Institute at the United States Military Academy at West Point and a research fellow at the Saltzman Institute of War and Peace Studies at Columbia University, PhD in political science from Columbia University, Shawn Lonergan, Research affiliate of the Army Cyber Institute at the United States Military Academy at West Point and a cyber officer in the US Army Reserve currently assigned to 75th Innovation Command, PhD in political science from Columbia University, 2019 (“Cyber Operations as Imperfect Tools of Escalation”, *Strategic Studies Quarterly*, Fall Issue 2019, Available Online through University of Southern California Libraries, Accessed 01-17-2021)

Third, these limitations become even more salient when we consider how strategic interactions are likely to play out over time during repeated crisis interactions. Because the virtual domain is changeable in a way that the physical world is not, actions taken by defenders in the context of a crisis can radically and unpredictably alter an attacker’s ability to deliver and sustain effects against a target over time.30 Access and capabilities are neither guaranteed nor indefinite—they have a shelf life.31 Footholds into a target’s network that were time intensive to develop can unexpectedly disappear as vulnerabilities in a network are patched. Exploits may have a short shelf life as revealing information about them enables targets to identify indicators of compromise (IOCs) and use these to prevent further damage from specific malware strains or quarantine malicious traffic using known malware signatures. An example of the latter is the US Cyber Command initiative, beginning in 2018, to share information about adversary malware by uploading samples to VirusTotal.32 Therefore, a target can “transition from vulnerability (to a particular attack) to invulnerability in, literally, minutes.”33 Third-party disclosure about software vulnerabilities by governments or private actors can also unintentionally precipitate the loss of access as exposure about vulnerability information enables network defenders to take measures to remedy them.34 For instance, the disclosures that began in 2016 by the group Shadow Brokers of purportedly pilfered US National Security Agency exploits and zero days ostensibly put US government accesses at risk.35 Put simply, a vulnerability upon which an access relies may in theory be only one update or disclosure away from being patched.

Thus, in the context of an ongoing crisis interaction between an attacker and defender, the former’s operational tempo is likely to be interrupted by the latter’s behavior, forcing the attacker to devote additional time to find or acquire new vulnerabilities and exploits in the midst of an offensive operation or campaign. As Inglis notes, to succeed in an offensive cyber campaign that unfolds over time, attackers must be able to sustain “the efficacy of tools under varying conditions caused by the defender’s response and the natural variability and dynamism of cyberspace.”36 The ability to build or acquire new accesses and capabilities “in real time” during a crisis is highly limited.37 Indeed, General Paul Nakasone remarked in a January 2019 interview on the radical difference in shelf life between conventional and cyber capabilities:

Compare the air and cyberspace domains. Weapons like JDAMs [ Joint Direct Attack Munitions] are an important armament for air operations. How long are those JDAMs good for? Perhaps 5, 10, or 15 years, sometimes longer given the adversary. When we buy a capability or tool for cyberspace . . . we rarely get a prolonged use we can measure in years. Our capabilities rarely last 6 months, let alone 6 years. This is a big difference in two important domains of future conflict.38

Therefore, as a 2013 Defense Science Board report notes, “offensive cyber will always be a fragile capability” when pitted against network defenders who are “continuously improving network defensive tools and techniques.”39

Each side can take defensive measures to blunt the impact and effectiveness of the other’s access and capabilities—particularly as information about them is revealed. Consequently, strategic accesses and capabilities are likely to become more vulnerable and less reliable over time, shrinking the set of cyber escalatory response options for all parties. This cycle is likely to generate temporal breaks in the pace of adversarial engagements in cyberspace, where states must regroup and develop or rebuild accesses and capabilities during an ongoing interaction. These pauses are likely to diffuse the pressure that typically accompanies—even defines—crisis situations, creating breathing space and, by extension, room for decisionmakers to deliberate alternative courses of action, for domestic political tensions to cool down, for intent to be communicated to adversaries, and for de-escalation pathways to be determined.

### 2nc – No Grids Impact

#### No grid impact---it’s overhyped.

Freedberg 14 (Sydney J, “Cyberwar: What People Keep Missing About The Threat,” Jan 6, <http://breakingdefense.com/2014/01/cyberwar-what-people-keep-missing-about-the-threat/>, CMR)

**Cites:**

--Peter W. Singer – former director of the Center for 21st Century Security and Intelligence and a senior fellow in the Foreign Policy program

--Allan A. Friedman – Research Scientist at the Cyber Security Policy Research Institute at George Washington University's School of Engineering

**Singer and Friedman** also **do a valuable service** in **beating back the hype** **about “Cyber Pearl Harbors”** **and “Cyber 9/11s” or the US suffering countless millions of “attacks.”** **Those alarmist statistics lump together everything from a virus easily stopped by** someone’s **firewall** to credit card theft **to the loss of secret schematics for the F-35** stealth fighter. **Those “attacks” vary from trivial, to significant losses** for one particular business, to actual matters of national security, **but none of them does as much damage as a good old-fashioned bomb**, they argue. **Even if hackers shut down the** national **electrical grid for weeks** on end, bad as that would be, **it wouldn’t be as bad as a single nuclear explosion**. “**It’s** a lot **like ‘Shark Week**,’” Singer said about the overhyped dangers. “**Squirrels have taken down the power grid more times than the zero times hackers have**.” There’s lots of talk about how the attacker always has the advantage in cyberspace, he told an audience at Brookings this afternoon, but “**a true cyber offense, an effective one**, a Stuxnet style [attack] **is** something **quite difficult**.”

#### Cyber attacks won’t take down the grid

Victoria Craig 16, Analyst at Fox Business, Citing the Senior Manager of Industrial Control Systems at Mandiant, “The U.S. Power Grid is 'Vulnerable,' But Don't Panic Just Yet”, http://www.foxbusiness.com/features/2016/02/02/u-s-power-grid-is-vulnerable-but-dont-panic-just-yet.html

The idea of the nation's power grids becoming the next battleground for cyber warriors could make hacking into consumers’ credit card accounts and personal information seem like child’s play. While U.S. power companies are likely targeted by foreign governments and others in increasingly sophisticated breaches, actually shutting off the lights and causing chaos is far more complicated than many pundits make it seem. Dan Scali, senior manager of industrial control systems at Mandiant, a cybersecurity consulting arm of FireEye ([FEYE](http://www.foxbusiness.com/quote.html?stockTicker=FEYE)), explained that while cyber criminals may gain access to power and utility data systems, it doesn’t necessarily mean the result will be a power outage and a total takedown of power grid control systems. In other words, the power grid is controlled by more than just a panel of digital buttons. “Losing the control system is bad from the perspective that it takes you out of your normal mode of operations of being able to control everything from one command center, but it doesn’t mean you’ve lost control or all the lights go out [in the city],” Scali explained. While many of the systems have been modernized to include digitized control panels, if a hacker were to infiltrate the system, a utility worker could still have the ability to manually control the machines by flipping a switch, pushing a button, or tripping a breaker. As the world saw with the recent attack in Ukraine, which caused a blackout for 80,000 customers of the nation’s western utility, the biggest problem may be ensuring the power grid’s control systems are not vulnerable to cyber break ins. The January attack in Ukraine was likely caused by a corrupted Microsoft Word attachment that allowed remote control over the computer, according to the U.S. Department of Homeland Security. Scali said there was no evidence from the incident in Ukraine that the hacker’s malware was able to physically shut down the power. “It wiped out machines, deleted all the files. Kill disk malware made it impossible to remotely control things. It caused chaos on the business network, and the area where control system operations sat. But the attacker, we believe, would have had to actually used the control system to cause load shedding, which caused the power to go out, or trip breakers to cause the actual problem. Malware itself didn’t turn the power out,” Scali said. He said what most likely happened in that incident was the hacker stole user credentials and logged into the system remotely. The bottom line: Yes, a similar event could happen in the U.S. And corporate America is concerned. A recent survey released in January on the state of information security, conducted by consulting firm Pricewaterhouse Coopers, showed cybersecurity as one of the biggest concerns among the top brass at U.S. power and utilities firms. Part of the problem, Brad Bauch, security and cyber sector leader at PwC said, is the interconnectedness of the industry’s tools. “Utilities want to be able to get information out of [their] systems to more efficiently operate them, and also share that information with customers so they have more real-time information into their usage,” he explained. While allowing access to their own consumption data allows the companies to give their customers more of what they want, it also opens up a host of access points for hackers, making the systems more vulnerable than they otherwise would be. But to say that the power grid is susceptible to cyber hackers is a bit of an oversimplification.

#### Squirrels are a bigger threat to our national grids than cyber-attacks

Rogue ’16 a strategist at the cybersecurity firm of Tenable Network Security, “Squirrels are bigger threat than hackers to US power grid” (C. Thomas, January 6, 2016) https://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0106/Opinion-Squirrels-are-bigger-threat-than-hackers-to-US-power-grid

The cyberwar drumbeaters have been stoking fears for decades about the potential of cyberattacks causing devastating physical damage. A litany of anonymous government officials quoted in articles regularly warn about coming digital strikes on power plants, gas pipelines, or water treatment plants. The perpetrators, they say, will be rogue nation hackers executing malicious code to pull off some kind of "cyber armageddon." But until recently no such attacks have ever been confirmed and nothing approaching the kind of physical destruction the doomsayers foretell has taken place. And even though two recently reported incidents – one at [a small New York dam](http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559) and another involving [a Ukrainian power plant](https://www.washingtonpost.com/world/national-security/russian-hackers-suspected-in-attack-that-blacked-out-parts-of-ukraine/2016/01/05/4056a4dc-b3de-11e5-a842-0feb51d1d124_story.html) – may qualify as real cyberattacks on critical infrastructure, recent history suggests we should all be wary of pointing to these incidents as signs that cyberwar is somehow imminent. Every time stories in the media emerge about computer attacks that cause physical damage – usually supported by anonymous sources – eventually more reasonable people investigate those claims and disprove theories involving destructive cyberattacks. Recommended: [Experts separate fact from hype in reports of Iranian hacking](https://www.csmonitor.com/World/Passcode/2015/1224/Experts-separate-fact-from-hype-in-reports-of-Iranian-hacking) One of the most commonly cited – yet erroneous – cyberevents involves several blackouts that affected Brazil between 2005 and 2007. The story goes that blackouts were the work of hackers. Even "60 Minutes" repeated that claim. Brazil's National Agency for Electric Energy, however, concluded that sooty insulators [caused the power outages](http://www.wired.com/2009/11/brazil_blackout/). [PHOTOS OF THE DAY](https://www.csmonitor.com/Photo-Galleries/Photos-of-the-Day) [Photos of the day 05/05](https://www.csmonitor.com/Photo-Galleries/Photos-of-the-Day-Archives/2017/Photos-of-the-day-05-05) Then there was the [2008 explosion of the Baku-Tbilisi-Ceyhan (BTC) pipeline](http://www.sueddeutsche.de/digital/tuerkei-ermittler-schliessen-cyberangriff-bei-pipeline-explosion-aus-1.2529345) in Turkey. No less than four unnamed sources claimed it was a cyberattack despite the fact that the pipeline owner said the valves involved in the blast weren't attached to any network. Ever since [Stuxnet](http://www.csmonitor.com/World/Security-Watch/2014/0225/Exclusive-New-thesis-on-how-Stuxnet-infiltrated-Iran-nuclear-facility), the computer worm discovered in 2010 [that damaged the Iranian nuclear program](http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/), many experts have warned a that torrent of other computer attacks on critical infrastructure would follow. They had a smoking gun the following year when [Russian hackers broke into a small Illinois water facility](http://www.wired.com/2011/11/water-pump-hack-mystery-solved/). While the plant's control systems were accessed by someone in Russia, that someone was the contractor for the water facility who happened to be on vacation in Russia at the time. Even though Stuxnet is the only confirmed cyberattack leading to physical damage, a German incident is often lumped into the category of hacks that lead to property destruction. [Many news articles](https://www.rt.com/news/216379-germany-steel-plant-hack/) and German government reports suggested that cyberattackers caused ["massive damage"](http://www.bbc.com/news/technology-30575104) at an unnamed steel plant by causing the blast furnace to malfunction. And, again, no one has gone on the record confirming this story and the steel plant remains unnamed. While this event has not been conclusively disproven, there are enough missing facts to raise considerable doubt. But over the Christmas and New Year's holiday, news stories about two more incidents are once again stirring up the cyberwar hawks. The first event occurred at the Bowman Avenue Dam near Rye, N.Y., which is about 20 miles north of Manhattan. It actually occurred in 2013 but unnamed officials (surprise) speaking to The Wall Street Journal attributed some kind of breach of the dam's computers to Iranian hackers. While the facts about what actually transpired at the dam are few, the incident did cause [the Department of Homeland Security to investigate](http://www.myrye.com/my_weblog/2015/12/rye-city-statement-on-bowman-avenue-dam.html). But exactly what DHS discovered, the extent of the so-called "attack," or how the incident was attributed to Iran remains unknown. What's more, the dam has no electrical generation capability and its only electronically controlled item is a flood control sluice gate, which dam officials say has never been fully operational. More facts are available surrounding the [Christmas Day attack in Ukraine](http://www.securitylab.ru/news/477942.php) in which the regional power company blamed malware for turning off substations. Normally, such claims would be met with deserved skepticism from cybersecurity pros. In this case, however, a sample of the malware has been found, which to people who research such things is considered [pretty damning evidence](https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered). But there's still debate as whether the introduction of the malware into the power company's systems was the work of a nation state, cybercriminals, or simply a random infection that occurs in all kinds of systems daily. So despite all the hype, fear, uncertainty, and doubt, we still don't have confirmed, indisputable cases of someone causing a power outage, or other major infrastructure damage, as a result of a cyberattack. In fact, according to a former deputy director of the National Security Agency, the biggest threat to the US power grid isn't a cyberattack at all. [It's a squirrel.](https://twitter.com/CyberSquirrel1/status/679345894421086209) Yes, [squirrels](http://cybersquirrel1.com/) and other animals cause hundreds of power outages every year and yet the only confirmed infrastructure cyberattack that has resulted in physical damage that is publicly known is Stuxnet. Perhaps we should focus less on cyberattacks and more attention to these furry adversaries.

# NATO Advantage Answers

\*\*\* Use cards from NATO Bad impact file

### 1nc – Alt Cause

#### Democratic backsliding is an alt cause to unity.

Hamilton & Binnendijk ’22 (Daniel S. Hamilton is President, Transatlantic Leadership Network Senior nonresident Fellow, Brookings, Senior Fellow, Foreign Policy Institute, Johns Hopkins University SAIS; Former U.S. Deputy Assistant Secretary of State. Hans Binnendijk is a Distinguished Fellow, Atlantic Council Former Senior Director for Defense Policy, U.S. National Security Council “One Plus Four: Charting NATO’s Future in an Age of Disruption,” NATO Task Force Report, Transatlantic Leadership Network, February 16, 2022, https://www.transatlantic.org/wp-content/uploads/2022/02/NATO-TF-SC-final-feb-16-2022.pdf)-mikee

The foundation for NATO’s next Strategic Concept must be renewed Alliance cohesion rooted in a common commitment to shared values. Today, those values are under assault from external and internal challengers. Waning attention to NATO’s core values has resulted in some allies prioritizing unilateral national decisions over collective Alliance interests, or using their position to block Alliance activities as a way to gain leverage in bilateral disputes. Some allies are themselves manipulating information and distorting data, undermining democratic processes and the rule of law, even threatening each other. 4 This is why a mutual affirmation of NATO’s democratic foundation must begin with humility. Our achievements do not always match our aspirations. Nonetheless, those aspirations matter – and they are enshrined in the North Atlantic Treaty. The preamble to the 1949 North Atlantic Treaty that established NATO declares that the signatories “are determined to safeguard the freedom, common heritage and civilization of their peoples, founded on the principles of democracy, individual liberty and the rule of law.”8 Article II states, “The Parties will contribute toward the further development of peaceful and friendly international relations by strengthening their free institutions.”9 Democratic deficits exacerbate mutual doubts, which can gnaw at allied commitments to collective defense and mutual security. These points of disunity can be used by strategic competitors to destabilize individual allies or NATO as a whole. Countries with weak protections for democracy, individual liberty and the rule of law are vulnerable to subversion, corruption, mis- and dis-information. Malign influences within allied states could mean that non-NATO countries could influence NATO decision-making. Regaining cohesion in decision-making is premised on reinforcing NATO's core values. Deficits in internal values can become external threats. Celeste Wallander has called democratic fragility “the alliance’s Achilles’ heel.” The 2020 NATO Experts Group report warns that “a drift toward NATO disunity must be seen as a strategic rather than merely a tactical or optical problem.”10 In recent years, much strategic discussion has focused on competition among states of “great power.” It is becoming clear, however, that this competition extends beyond traditional measures of power; it centers increasingly on forms of governance. Adversaries big and small are selling autocracy as “efficient.” They tout their own systems and use a broad array of tools to amplify fissures and undermine confidence within democracies. When they can’t do that successfully, they use diplomatic and other means of coercion. They support illiberal democracies. Others are beginning to follow their model. This puts democratic resilience at the heart of the new international system and international competition.

### 2nc – Alt Causes

#### Energy supply risks are uniquely wedge issues between and controversial debates about diversification guarantee disunity

Eugene Rumer, Richard Sokolsky, 4-11-2022, "Putin’s War Against Ukraine and the Balance of Power in Europe," Carnegie Endowment for International Peace, https://carnegieendowment.org/2022/04/11/putin-s-war-against-ukraine-and-balance-of-power-in-europe-pub-86832

Notwithstanding the allies’ early show of unity in the wake of the Russian attack on Ukraine, **some of their differences and challenges to a more robust NATO posture have not disappeared entirely**. These include the **varying interests and priorities of the EU’s and NATO’s diverse members,** as well as likely disagreements over which threats and challenges should be privileged in resource allocation decisions (among issues ranging from the Russian threat, China, climate change, pandemics, immigration, borders, refugees, or diversification of energy supplies). **It would be prudent to not take for granted that Europe will forge** the **political unity** and raise the billions of euros it will require to create a first-class military that might substitute for or provide a substantial addition to NATO’s military kit.¶ Moreover, the unanimity with which Europe came together to impose sanctions on Russia and help Ukraine is likely due to the fact that Ukraine is *not* a NATO member, and demonstrations of solidarity with it do not involve defense commitments through NATO’s Article 5. **In the event of a Russian attack against a NATO member country, the specter of an all-out war with Russia may lead some allies to demonstrate less resolve and more caution and hesitation**. ¶ One headline is likely to become a trend line: Putin has [confirmed](https://www.armscontrol.org/act/2022-03/news/putin-orders-russian-nuclear-weapons-higher-alert) that nuclear weapons are useful for a wide range of deterrence and coercive purposes to go along with what will still be formidable conventional capabilities in a short-war scenario, such as a quick land grab in the Baltic region. Several implications flow from this development.¶ First, notwithstanding rhetoric about defending every inch of NATO territory and the alliance’s impressive show of resolve, NATO may be unable or unwilling to conduct an Article 5 intervention against a Russian attack. The alliance may choose instead to form a coalition of willing NATO countries to defend vulnerable countries on its eastern flank. ¶ Second, against the backdrop of renewed Russian nuclear threats and an unreconstructed Putin determined to achieve his long-standing geopolitical ambitions in Europe, NATO will need to rethink its conventional and nuclear doctrine and capabilities. Three key questions, fraught with political and geostrategic consequences, will need to be confronted:¶ First, should the alliance try to muster the political unity and massive resources that would be required to shift from a trip-wire posture to provide deterrence and reassurance to a war-fighting posture?¶ Second, will NATO need to rethink the balance between conventional and nuclear capabilities in its military doctrine?¶ Finally, does the alliance need to do a fundamental rethink of its nuclear doctrine and declaratory policy—specifically, whether, how, and under what circumstances it should threaten or actually use nuclear weapons against Russian forces on the battlefield or against Russian territory?¶ Finally, the risks of inadvertent escalation could increase significantly if Russia relied more on its nonstrategic nuclear forces. To mitigate these risks, the United States and NATO will need to restore and upgrade military communications and deconfliction procedures with the Russian military and resume dialogue on stabilizing arms control and confidence-building measures as soon as possible.¶ Amid all the uncertainty, one thing is certain: the NATO alliance cannot afford to be trapped by institutional inertia, path dependent choices, or an assumption that a weakened Russia will stay Putin’s hand. To the contrary, Putin is likely to double down on his reckless gamble in Ukraine rather than stand down.

### 1nc – No Econ Impact

#### No econ impact

**Walt 20** [Stephen M. Walt is the Robert and Renée Belfer professor of international relations at Harvard University. “Will a Global Depression Trigger Another World War?”, May 13th, https://foreignpolicy.com/2020/05/13/coronavirus-pandemic-depression-economy-world-war/]

On balance, however, I do not think that even the extraordinary economic conditions we are witnessing today are going to have much impact on the likelihood of war. Why? First of all, if depressions were a powerful cause of war, there would be a lot more of the latter. To take one example, the United States has suffered 40 or more recessions since the country was founded, yet it has fought perhaps 20 interstate wars, most of them unrelated to the state of the economy. To paraphrase the economist Paul Samuelson’s famous quip about the stock market, if recessions were a powerful cause of war, they would have predicted “nine out of the last five (or fewer).”

Second, states do not start wars unless they believe they will win a quick and relatively cheap victory. As John Mearsheimer showed in his classic book Conventional Deterrence, national leaders avoid war when they are convinced it will be long, bloody, costly, and uncertain. To choose war, political leaders have to convince themselves they can either win a quick, cheap, and decisive victory or achieve some limited objective at low cost. Europe went to war in 1914 with each side believing it would win a rapid and easy victory, and Nazi Germany developed the strategy of blitzkrieg in order to subdue its foes as quickly and cheaply as possible. Iraq attacked Iran in 1980 because Saddam believed the Islamic Republic was in disarray and would be easy to defeat, and George W. Bush invaded Iraq in 2003 convinced the war would be short, successful, and pay for itself.

The fact that each of these leaders miscalculated badly does not alter the main point: No matter what a country’s economic condition might be, its leaders will not go to war unless they think they can do so quickly, cheaply, and with a reasonable probability of success.

Third, and most important, the primary motivation for most wars is the desire for security, not economic gain. For this reason, the odds of war increase when states believe the long-term balance of power may be shifting against them, when they are convinced that adversaries are unalterably hostile and cannot be accommodated, and when they are confident they can reverse the unfavorable trends and establish a secure position if they act now. The historian A.J.P. Taylor once observed that “every war between Great Powers [between 1848 and 1918] … started as a preventive war, not as a war of conquest,” and that remains true of most wars fought since then.

The bottom line: Economic conditions (i.e., a depression) may affect the broader political environment in which decisions for war or peace are made, but they are only one factor among many and rarely the most significant. Even if the COVID-19 pandemic has large, lasting, and negative effects on the world economy—as seems quite likely—it is not likely to affect the probability of war very much, especially in the short term.

### 2nc – No Econ Impact

#### Decline doesn’t cause war

Christopher Clary, former International Affairs Fellow in India at the Council on Foreign Relations, Postdoctoral Fellow at the Watson Institute at Brown University, Adjunct Staff Member @ RAND Corporation, Security Studies Program, MIT, country director for South Asian affairs in the Office of the Secretary of Defense, former Research Fellow, the Harvard Kennedy School's Belfer Center for Science and International Affairs, former research associate in the Department of National Security Affairs at the Naval Postgraduate School, BA from Wichita State University and an MA from the U.S. Naval Postgraduate School, 2015, Economic Stress and International Cooperation: Evidence from International Rivalries,” Massachusetts Institute of Technology Political Science Department Research Paper No. 2015

Economic crises lead to conciliatory behavior through five primary channels. (1) Economic crises lead to austerity pressures, which in turn incent leaders to search for ways to cut defense expenditures. (2) Economic crises also encourage strategic reassessment, so that leaders can argue to their peers and their publics that defense spending can be arrested without endangering the state. This can lead to threat deflation, where elites attempt to downplay the seriousness of the threat posed by a former rival. (3) If a state faces multiple threats, economic crises provoke elites to consider threat prioritization, a process that is postponed during periods of economic normalcy. (4) Economic crises increase the political and economic benefit from international economic cooperation. Leaders seek foreign aid, enhanced trade, and increased investment from abroad during periods of economic trouble. This search is made easier if tensions are reduced with historic rivals. (5) Finally, during crises, elites are more prone to select leaders who are perceived as capable of resolving economic difficulties, permitting the emergence of leaders who hold heterodox foreign policy views. Collectively, these mechanisms make it much more likely that a leader will prefer conciliatory policies compared to during periods of economic normalcy. This section reviews this causal logic in greater detail, while also providing historical examples that these mechanisms recur in practice.

#### No impact to economic decline – prefer new data

Daniel **Drezner 14**, Professor of IR at Tufts, “The System Worked: Global Economic Governance during the Great Recession”, World Politics, Volume 66. Number 1, January 2014, pp. 123-164

The final significant outcome addresses a dog that hasn't barked: the effect of the Great Recession on cross-border conflict and violence. During the initial stages of the crisis, multiple analysts asserted that the financial crisis would lead states to increase their use of force as a tool for staying in power.42 They voiced genuine concern that the global economic downturn would lead to an increase in conflict—whether through greater internal repression, diversionary wars, arms races, or a ratcheting up of great power conflict. Violence in the Middle East, border disputes in the South China Sea, and even the disruptions of the Occupy movement fueled impressions of a surge in global public disorder. **The aggregate data suggest otherwise**, however. The Institute for Economics and Peace has concluded that "the average level of peacefulness in 2012 is approximately the same as it was in 2007."43 Interstate violence in particular has declined since the start of the financial crisis, as have military expenditures in most sampled countries. Other studies confirm that the Great Recession has not triggered any increase in violent conflict, as Lotta Themner and Peter Wallensteen conclude: "[T]he pattern is one of relative stability when we consider the trend for the past five years."44 The secular decline in violence that started with the end of the Cold War has not been reversed. Rogers Brubaker observes that "the crisis has not to date generated the surge in protectionist nationalism or ethnic exclusion that might have been expected."43

### 1nc – No Populism Impact

#### Polarization won’t cause war

Niall Ferguson 16, Senior Fellow at Stanford University’s Hoover Institution, Senior Fellow of the Center for European Studies at Harvard University, and Visiting Professor at Tsinghua University in Beijing, Autumn 2016, “Populism as a Backlash against Globalization - Historical Perspectives,” <https://www.cirsd.org/en/horizons/horizons-autumn-2016--issue-no-8/populism-as-a-backlash-against-globalization>

Such comparisons between the United States today and Germany in the 1930s are becoming commonplace. As a professional historian, I would like to offer what seems to me a better analogy. Our Tranquil Times Journalists are fond of saying that we are living in a time of “unprecedented” instability. In reality, as numerous studies have shown, our time is a period of remarkable stability in terms of conflict. In fact, viewed globally, there has been a small uptick in organized lethal violence since the misnamed Arab Spring. But even allowing for the horrors of the Syrian civil war, the world is an order of magnitude less dangerous than it was in the 1970s and 1980s, and a haven of peace and tranquility compared with the period between 1914 and 1945. This point matters because the defining feature of interwar fascism was its militarism. Fascists wore uniforms. They marched in enormous and well-drilled parades and they planned wars. That is not what we see today. So why do so many commentators feel that we are living through “unprecedented instability?” The answer, aside from plain ignorance of history, is that political populism has become a global phenomenon, and established politicians and political parties are struggling even to understand it, much less resist it. Yet populism is not such a mysterious thing, if one only has some historical knowledge. The important point is not to make the mistake of confusing it with fascism, which it resembles in only a few respects. Rather like a television chef, I shall describe a recipe for populism, based on historical experience. It is a simple recipe, with just five ingredients. Five Ingredients for A Populist Backlash The first of these ingredients is a rise in immigration. In the past 45 years, the percentage of the population of the United States that is foreign-born has risen from below 5 percent in 1970 to over 13 percent in 2014—almost as high as the rates achieved between 1860 and 1910, which ranged between 13 percent and an all-time high of 14.7 percent in 1890. So when people say, as they often do, that “the United States is a land based on immigration,” they are indulging in selective recollection. There was a period, between 1910 and 1970, when immigration drastically declined. It is only in relatively recent times that we have seen immigration reach levels comparable with those of a century ago, in what has justly been called the first age of globalization. Ingredient number two is an increase in inequality. Drawing on the work done on income distribution by Thomas Piketty and Emmanuel Saez, we can see that we have recently regained the heights of inequality that were last seen in the pre-World War I period. The share of income going to the top one percent of earners is back up from below 8 percent of total income in 1970 to above 20 percent of total income. The peak before the financial crisis, in 2007, was almost exactly the same as the peak on the eve of the Great Depression in 1928. Ingredient number three is the perception of corruption. For populism to thrive, people have to start believing that the political establishment is no longer clean. Recent Gallup data on public approval of institutions in the United States show, among other things, notable drops in the standing of all institutions save the military and small businesses. Just 9 percent of Americans have “a great deal” or “quite a lot” of confidence in the U.S. Congress—a remarkable figure. It is striking to see which other institutions are down near the bottom of the league. Big business is second-lowest, with just 21 percent of the public expressing confidence in it. Newspapers, television news, and the criminal justice system fare only slightly better. What is even more remarkable is the list of institutions that have fallen furthest in recent times: the U.S. Supreme Court now has just a 36 percent approval rating, down from a historical average of 44 percent, while the Presidency has dropped from 43 percent to 36 percent approval. The financial crisis appears to have convinced many Americans—and not without good reason—that there is an unhealthy and likely corrupt relationship between political institutions, big business, and the media. The fourth ingredient necessary for a populist backlash is a major financial crisis. The three biggest financial crises in modern history—if one uses the U.S. equity market index as the measure—were the crises of 1873, 1929, and 2008. Each was followed by a prolonged period of depressed economic performance, though these varied in their depth and duration. In the most recent of these crises, the peak of the U.S. stock market was October 2007. With the onset of the financial crisis, we essentially replayed for about a year the events of 1929 and 1930. However, beginning in mid to late 2009, we bounced out of the crisis, thanks to a combination of monetary, fiscal, and Chinese stimulus, whereas the Great Depression was characterized by a deep and prolonged decline in stock prices, as well as much higher unemployment rates and lower growth. The first of these historical crises is the least known: the post-1873 “great depression,” as contemporaries called it. What happened after 1873 was nothing as dramatic as 1929; it was more of a slow burn. The United States and, indeed, the world economy went from a financial crisis—which was driven by excessively loose monetary policy and real estate speculation, amongst other things—into a protracted period of deflation. Economic activity was much less impaired than in the 1930s. Yet the sustained decline in prices inflicted considerable pain, especially on indebted farmers, who complained (in reference to the then prevailing gold standard) that they were being “crucified on a cross of gold.” We have come a long way since those days; gold is no longer a key component of the monetary base, and farmers are no longer a major part of the workforce. Nevertheless, in my view, the period after 1873 is much more like our own time, both economically and politically, than the period after 1929. There is still one missing ingredient to be added. If one were cooking, this would be the moment when flames would leap from the pan. The flammable ingredient is, of course, the demagogue, for populist demagogues react vituperatively and explosively against all of the aforementioned four ingredients. Kearney’s Cause Now, my argument is not intended to dismiss or downplay those elements of Donald Trump’s campaign for President of the United States that have been implicitly, if not explicitly, racist. Nor do I treat lightly the various signals he has given of indifference to, or at least ignorance of, the U.S. Constitution. My point is that these demerits do not by themselves qualify Trump for comparison with Mussolini, much less with Hitler. Rather, I want to argue that Trump has much more in common with the demagogues of the earlier, lesser depression of the late nineteenth century, and that it is to that period that we should look for historical analogies and insights. The best illustration of my case is the now forgotten figure of Denis Kearney, leader of the Workingmen’s Party of California and the author of the slogan “The Chinese Must Go!” Himself an Irish immigrant to the United States—as opposed to the son of a Scottish immigrant and grandson of a German, which is what Donald Trump is—Kearney was part of a movement of nativist parties and “Anti-Coolie” clubs that sought to end Chinese immigration into the United States. The report of the Joint Special Committee to Investigate Chinese Immigration in 1877 gives a flavor of the times. “The Pacific coast must in time become either Mongolian or American,” was the committee’s view. The report argued that the Chinese brought with them the habits of despotic government, a tendency to lie in court, a weakness for tax evasion and “insufficient brainspace […] to furnish [the] motive power for self-government.” Moreover, Chinese women were “bought and sold for prostitution and treated worse than dogs,” while the Chinese were “cruel and indifferent to their sick.” Giving such inferior beings citizenship, the committee’s report declared, “would practically destroy republican institutions on the Pacific coast.” The realities were, it scarcely needs to be said, very different. According to the “Six Companies” of Chinese in San Francisco—corporate bodies that represented the Chinese population of the city—there was compelling evidence that Chinese immigration was a boon to California. Not only did the Chinese provide labor for the state’s rapidly developing railroads and farms; they also tended to improve the neighborhoods in which they settled. Moreover, there was no evidence of a disproportionate Chinese role in gambling and prostitution. In fact, statistics showed that the Irish were more of a charge on the city’s hospital and almshouse than the Chinese. Nevertheless, a powerful coalition of “laboring men and artisans,” small businessmen and “grangers” (the term used to describe those who aimed to shift the burden of taxation onto big business and the rich) rallied to Kearney’s cause. As one shrewd contemporary observer noted, part of his appeal was that he was attacking not just the Chinese, but also the big steamship and railroad companies that profited from employing Chinese labor, not to mention the corrupt two-party establishment that ran San Francisco politics: Neither Democrats nor Republicans had done, nor seemed likely to do, anything to remove these evils or to improve the lot of the people. They were only seeking (so men thought) places or the chance of jobs for themselves, and could always be bought by a powerful corporation. Working men must help themselves; there must be new methods and a new departure […] The old parties, though both denouncing Chinese immigration in every convention they held, and professing to legislate against it, had failed to check it […] Everything, in short, was ripe for a demagogue. Fate was kind to the Californians in sending them a demagogue of a mean type, noisy and confident, but with neither political foresight nor constructive talent. Kearney may have lacked foresight and “constructive talent,” but there is no gainsaying what he and his ilk were able to achieve. Beginning with the Page Law (1875) prohibiting the immigration of Asian women for “lewd or immoral purposes,” American legislators scarcely rested until Chinese immigration to the United States had been stopped altogether. The Chinese Exclusion Act (1882) suspended immigration of Chinese for 10 years, introduced “certificates of registration” for departing laborers (effectively re-entry permits), required Chinese officials to vet travelers from Asia, and, for the first time in American history, created an offense of illegal immigration, with the possibility of deportation as a part of the penalty. The Foran Act (1885) banned all contract laborers from immigrating to America. Legislation passed in the Scott Act (1888) banned all Chinese from travel to the United States except “teachers, students, merchants, or travelers for pleasure.” In all, between 1875 and 1924, more than a dozen pieces of legislation served to restrict and finally end altogether Chinese immigration. No one should therefore underestimate the power of populism. For all his coarseness and bombast, Denis Kearney and his allies effectively sealed the American border along the Pacific coast of the United States; indeed, one cartoon of the time depicted them constructing a wall across the San Francisco harbor. In the 1850s and 1860s, as many as 40 percent of all Chinese emigrants had travelled beyond Asia, though the numbers arriving in the United States had in fact been relatively small (between 1870 and 1880, a total of 138,941 Chinese immigrants came, just 4.3 percent of the total, a share dwarfed by the vast European exodus across the Atlantic in the same period). What exclusion did ensure in the late nineteenth was that Chinese immigration would not grow, as it surely would have, but instead dwindled and then ceased. Ironies Populism, then, is not just a form of political entertainment. One sometimes hears it said of Donald Trump: “Ah, he says wild things on the campaign trail, but when he is president it will be fine.” History suggests otherwise. It suggests that men who threaten to restrict immigration—as well as to impose tariffs and to discourage capital export, as populists generally do—mean what they say. Indeed, populists are under a special compulsion to enact what they pledge in the campaign trail, for their followers are fickle to begin with. In the case of Trump, most have already defected from the Republican Party establishment. If he fails to deliver, they can defect from him, too. Of course, populists are bound eventually to disappoint their supporters. For populism is a toxic brew as well as an intoxicating one. Populists nearly always make life miserable for whichever minorities they chose to scapegoat, but they seldom make life much better for the people whose ire they whip up. Whatever the demagogues may promise—and they always promise “jam today”—populism tends to have significantly more economic costs than benefits. Restricting immigration, imposing tariffs on imported goods, penalizing firms for investing abroad: such measures, if adopted by an American government in 2017, would be almost certain to reduce growth and employment, rather than the reverse. That has certainly been the Latin American experience—and few regions of the world have run the populist experiment more often. The foreign dimension brings us to a final irony. Despite their habitual insistence on narrow national self-interest, populists are nearly always part of a global phenomenon. Globalization had been making enormous strides prior to 1873, with world trade, migration, and international capital flows growing at unprecedented rates. But the crisis of that year generated a populist backlash against globalization that was itself global in its scope. Then, just as now, the principal targets of the demagogues were immigration, free trade, and high finance. Just as the United States excluded immigrants and raised tariffs, so did European countries by adopting similar discriminatory measures. In Bismarck’s Germany, populism was often antisemitic—as it was in the France of the Dreyfus Affair—while in late Victorian Britain it was anti-Irish. Tariffs went up almost everywhere except in Britain. Populism today has a similarly global quality. In June, the British vote to leave the European Union was hailed by populists right across the European continent as well as by Donald Trump in the United States and, implicitly, by Vladimir Putin in Russia. Yielding to the Complicators Let me conclude with a note of qualified optimism. Because populism is not fascism, populist victories should not be construed as harbingers of war—if anything, the opposite is true. In the 1870s and 1880s, populists did achieve significant reductions in globalization: not only immigration restrictions, but also higher tariffs. But they did not form many national governments, and they did not subvert any constitutions. Nor were populists much interested in starting wars; if anything, they lent towards isolationism and viewed imperialism as just another big business racket. In most countries, the populist high tide was in the 1880s. What came next—in many ways as a reaction to populism, but also as an alternative set of policy solutions to the same public grievances—was Progressivism in the United States and socialism in Europe. Perhaps something similar will also happen in our time. Perhaps that is something to look forward to. Nevertheless, we would do well to remember that World War I broke out during the progressive not the populist era. The world today is, as I observed at the outset, in much less turmoil than one might infer from television news. Nevertheless, the economic and social consequences of globalization and the most recent financial crisis sowed the seeds for the populist backlash that we now see. Populists are not fascists. They prefer trade wars to actual wars; administrative border walls to more defensible fortifications. The maladies they seek to cure are not imaginary: uncontrolled rising immigration, widening inequality, free trade with “unfree” countries, and political cronyism are all things that a substantial section of the electorate have some reason to dislike. The problem with populism is that its remedies are wrong and, in fact, counterproductive. What we most have to fear—as was true of Brexit—is not therefore Armageddon, but something more prosaic: an attempt to reverse certain aspects of globalization, followed by disappointment when the snake oil does not really cure the patient’s ills, followed by the emergence of a new and ostensibly more progressive set of remedies for our current malaise. The “terrible simplifiers” may have their day then. But they will end up yielding power to well-intentioned complicators, those more congenial to educated elites, but probably every a bit as dangerous, if not more so.

### 1nc – No Democracy Impact

#### Democratic peace is statistically disproven---it’s conflict driving

Dr. Daina Chiba 21, Associate Professor of Political Science in the Department of Government and Public Administration at the University of Macau, Ph.D. in Political Science from Rice University, LL.M in Jurisprudence and International Relations from Hitotsubashi University, and Dr. Erik Gartzke, Professor of Political Science at the University of California, San Diego, PhD in Political Science from the University of Iowa, “Make Two Democracies and Call Me in the Morning: Endogenous Regime Type and the Democratic Peace”, 2/19/2021, https://dainachiba.github.io/research/make2dem/Make2Dem.pdf

The democratic peace—the observation that democracies are less likely to fight each other than are other pairings of states—is one of the most widely acknowledged empirical regularities in international relations. Prominent scholars have even characterized the relationship as an empirical law (Levy 1988; Gleditsch 1992). The discovery of a special peace in liberal dyads stimulated enormous scholarly debate and led to, or reinforced, a number of policy initiatives by various governments and international organizations. Although a broad consensus has emerged among researchers regarding the empirical correlation between joint democracy and peace, disagreement remains as to its logical foundations. Numerous theories have been proposed to account for how democracy produces peace, if only dyadically (e.g., Russett 1993; Rummel 1996; Doyle 1997; Schultz 2001).

At the same time, peace appears likely to foster or maintain democracy (Thompson 1996; James, Solberg, andWolfson 1999). A vast swath of research in political science and economics proposes explanations for the origins of liberal government involving variables such as economic development (Lipset 1959; Burkhart and Lewis-Beck 1994; Przeworski et al. 2000; Acemoglu and Robinson 2006; Epstein et al. 2006) and inequality (Boix 2003), political interests (Downs 1957; Bueno de Mesquita et al. 2003), power hierarchies (Moore 1966; Lake 2009), third party inducements (Pevehouse 2005) or impositions (Peceny 1995; Meernik 1996), geography (Gleditsch 2002b), and natural resource endowments (Ross 2001), to list just a few examples. Each of these putative causes of democracy is also associated with various explanations for international conflict. Indeed, some as yet poorly defined set of canonical factors may contribute both to democracy and to peace, making it look as if the two variables are directly related, even if possibly they are not.

We seek to contribute to this literature, not by proposing yet another theory to explain how democracy vanquishes war, but by estimating the causal effect of joint democracy on the probability of militarized disputes using a quasi-experimental research design. We begin by noting that some of the common causes of democracy and peace may be unobservable, generating an endogenous relationship between the two. Theories of democracy and explanations for peace are at a formative state; it is not possible to utilize detailed, validated and widely accepted models of each of these processes to assess their interaction. Indeed, to a remarkable degree democracy and peace each remain poorly understood and weakly accounted for empirically, despite their central roles in international politics. We address the risk of spurious correlation by applying an instrumental variables approach. Having taken into account possible endogeneity between democracy and peace, we find that joint democracy does not have an independent pacifying effect on interstate conflict. Instead, our findings show that democratic countries are more likely to attack other democracies than are non-democracies. Our results call into question the large body of theory that has been proposed to account for the apparent pacifism of democratic dyads.

### 1nc – No Disease Impact

#### No disease impact

Ord ’20 [Dr. Toby; 2020; Senior Research Fellow in Philosophy at Oxford University, DPhil in Philosophy from the University of Oxford; Hachette Books, “The Precipice: Existential Risk and the Future of Humanity,” p. 124-126]

Are we safe now from events like this? Or are we more vulnerable? Could a pandemic threaten humanity’s future?10 The Black Death was not the only biological disaster to scar human history. It was not even the only great bubonic plague. In 541 CE the Plague of Justinian struck the Byzantine Empire. Over three years it took the lives of roughly 3 percent of the world’s people.11 When Europeans reached the Americas in 1492, the two populations exposed each other to completely novel diseases. Over thousands of years each population had built up resistance to their own set of diseases, but were extremely susceptible to the others. The American peoples got by far the worse end of exchange, through diseases such as measles, influenza and especially smallpox. During the next hundred years a combination of invasion and disease took an immense toll—one whose scale may never be known, due to great uncertainty about the size of the pre-existing population. We can’t rule out the loss of more than 90 percent of the population of the Americas during that century, though the number could also be much lower.12 And it is very difficult to tease out how much of this should be attributed to war and occupation, rather than disease. As a rough upper bound, the Columbian exchange may have killed as many as 10 percent of the world’s people.13 Centuries later, the world had become so interconnected that a truly global pandemic was possible. Near the end of the First World War, a devastating strain of influenza (known as the 1918 flu or Spanish Flu) spread to six continents, and even remote Pacific islands. At least a third of the world’s population were infected and 3 to 6 percent were killed.14 This death toll outstripped that of the First World War, and possibly both World Wars combined. Yet even events like these fall short of being a threat to humanity’s longterm potential.15 [FOONOTE] In addition to this historical evidence, there are some deeper biological observations and theories suggesting that pathogens are unlikely to lead to the extinction of their hosts. These include the empirical anti-correlation between infectiousness and lethality, the extreme rarity of diseases that kill more than 75% of those infected, the observed tendency of pandemics to become less virulent as they progress and the theory of optimal virulence. However, there is no watertight case against pathogens leading to the extinction of their hosts. [END FOOTNOTE] In the great bubonic plagues we saw civilization in the affected areas falter, but recover. The regional 25 to 50 percent death rate was not enough to precipitate a continent-wide collapse of civilization. It changed the relative fortunes of empires, and may have altered the course of history substantially, but if anything, it gives us reason to believe that human civilization is likely to make it through future events with similar death rates, even if they were global in scale. The 1918 flu pandemic was remarkable in having very little apparent effect on the world’s development despite its global reach. It looks like it was lost in the wake of the First World War, which despite a smaller death toll, seems to have had a much larger effect on the course of history.16 It is less clear what lesson to draw from the Columbian exchange due to our lack of good records and its mix of causes. Pandemics were clearly a part of what led to a regional collapse of civilization, but we don’t know whether this would have occurred had it not been for the accompanying violence and imperial rule. The strongest case against existential risk from natural pandemics is the fossil record argument from Chapter 3. Extinction risk from natural causes above 0.1 percent per century is incompatible with the evidence of how long humanity and similar species have lasted. But this argument only works where the risk to humanity now is similar or lower than the longterm levels. For most risks this is clearly true, but not for pandemics. We have done many things to exacerbate the risk: some that could make pandemics more likely to occur, and some that could increase their damage. Thus even “natural” pandemics should be seen as a partly anthropogenic risk.

# Solvency Answers

### 1nc – No Solvency

#### Inconsistent data standards and lack of transparency in attribution makes cyber-operation useless. The US can’t cooperate with allies in NATO if they don’t understand or trust the intel.

Porter & Jordan ’19 (Christopher Porter is the chief intelligence strategist of cybersecurity company FireEye and a nonresident senior fellow at the Atlantic Council; Klara Jordan is director of the Cyber Statecraft Initiative at the Atlantic Council’s Scowcroft Center for Strategy and Security; Don’t Let Cyber Attribution Debates Tear Apart the NATO Alliance; <https://www.lawfareblog.com/dont-let-cyber-attribution-debates-tear-apart-nato-alliance>)-mikee

The alliance has a track record of collective action and cooperative security measures. For example, Operation Active Endeavour helped to deter, disrupt and protect against terrorist activity in the Mediterranean in the aftermath of the 9/11 terrorist attacks, in solidarity with the United States. For the seventh time, the Atlantic Council’s Cyber Statecraft Initiative will be among the organizations privileged to organize an event on the sidelines of the Feb. 15–17 Munich Security Conference. This year in particular, the Atlantic Council’s event, “Defending Human Dignity: Limiting Malicious Cyber Activity Through Diplomacy,” will complement the topics high on the agenda of the main conference, such as transatlantic collaboration, the consequences of a resurgence of great power competition and the future of arms control. In the United States, the greatest failures of response and deterrence to foreign aggression in cyberspace have not been caused by a lack of intelligence, capability or imagination. Rather, U.S. policy has been serviceable in theory but impotent in practice because of an inability to translate technical findings and intelligence into public support for sufficiently tough responses ordered by elected political leaders. North Korea’s repeated operations targeting U.S. companies and critical infrastructure have been met with public skepticism over their culpability, limiting the strength of retaliatory options needed to deter further events. Chinese cyber economic espionage continued for years despite widespread knowledge of China’s activities because political leaders found it difficult to confront Beijing without undermining U.S. companies in return. Russian information operations did not sow enough doubt to mislead experts, but they succeeded in exacerbating the partisan polarization of an already-divided electorate and its leaders. That inability to translate the findings of cyber experts into public sentiment and therefore political action has sidelined America’s cyberwarriors, by far the most technologically advanced and well-resourced in the world. Imagine the political response of an ally that is asked to burden-share in response to cyber aggression but is probably much closer to any resulting kinetic fight than the United States. Now imagine the response of that ally when it’s being asked to take causus belli on faith: The United States is presenting attribution for a cyberattack elsewhere in the world, but perhaps is depending on the ally lacking critical details due to classification, and is presenting that information alongside a request for help that might well put the ally in the crosshairs of its own cyberattack or lethal action. How can allies with different capabilities to collect, analyze and understand intelligence be part of a consensus on using sovereign cyber effects to support a NATO operation? How can a commander achieve a common operational picture to authorize the use of sovereign effects in a NATO operation if all the allies are not on the same page with respect to critical attribution and other technical information needed for a use of effect in an operation? We all know what a tank looks like on a shared satellite image, but if you ask three cyber experts to interpret the attribution for a set of indicators, you are likely to get at least four answers. For most U.S. allies in Europe and elsewhere, there is simply a dearth of technical know-how within the government when it comes to cyber attribution and operations. This is already a challenge for the United States, with a massive defense budget, Silicon Valley innovation and an educated workforce to pull into government service. But for many U.S. allies, tech-savvy public servants will have long fled for the private sector, nongovernmental organizations (NGOs) and academia before reaching ministerial positions. To its credit, the U.S. National Cyber Strategy does propose capacity-building measures to support allies. This means building up law enforcement, intelligence, and military operational and investigative capability. But even with successful capacity-building programs, many nations could, in a crisis, end up in the same place the United States is—with good options stuck on the shelf while political leaders and their electorates lack a critical mass of informed voters to trust, understand and act on expert findings. For countries weighing whether to risk their own blood and treasure in support of an ally’s cyber attribution findings, this hurdle could well prove insurmountable if not addressed well before a crisis emerges. Many such countries will no doubt recall being burned when placing too much confidence in U.S. technical and human sources without an ability to evaluate the evidence for themselves, as with the Iraq weapons of mass destruction findings.

### 1nc – Cooperation Fails

#### NATO’s is too divided – operationally, and politically, can’t coordinate

Oscar Jonsson in 2021

scholar of strategy, emerging technology and Russia who is founder of Phronesis Analysis and Researcher at Swedish Defence University; FROM EASTERN FLANK TO WESTERN ELECTIONS: RUSSIAN OPERATIONS AGAINST THE EU AND NATO; The Center for European Policy Analysis; https://cepa.org/the-evolution-of-russian-hybrid-warfare-eu-nato/

While hybrid warfare is naturally a wide effort, the Russian way goes beyond a Western all-of-government approach to include organized crime, cyber privateers, and intelligence services with a global reach and impressive coordination. According to one estimate, there are at least six presidential administration departments and a series of presidential councils in Russia that are involved in the active measures campaign.6 This shows both the variety of Russia’s hybrid warfare and its impressive machinery for exercising control. It poses a particular challenge for the EU and NATO, which are carefully bound by their respective mandates divided into different domains. Moreover, different sectors within the EU and NATO have a hard time cooperating even in the best of circumstances, not to mention against an actor that uses everything from licit and illicit finance, hackers, media outlets, and intelligence services.¶ The information domain is the most important venue for hybrid warfare. The revolution in information and communications technology has been one of the most profound societal changes in a long time. Today, a large part of how we understand the world, power, and legitimacy is mediated through social media.7 Therefore, “the process of collecting and organizing information is now a tremendous source of economic, political and cultural power.”8 This shift is, naturally, no secret to Russian strategists who have done their utmost to update their disinformation toolbox.¶ Russia’s vulnerabilities in the information domain have been exposed on several occasions in the past. For example, Chechen separatists successfully used the internet in a propaganda war with the Russians during the Second Chechen War, Russia’s image took a beating in the global media when it invaded Georgia in August 2008, and the Russian leadership was caught unaware by the pro-democracy Arab Spring in the Middle East and North Africa and the massive anti-government protests these uprisings inspired following the Russian elections in 2011. However, each failure was followed by adaptation and innovation: after the Chechen wars, Russia increased internet restrictions and surveillance; after the Georgian war, Russia’s state-controlled television network, RT, extended its global reach to include Arabic, Spanish, and French audiences; and, after the Arab Spring, Russia expanded censorship of social media9 (such as a new treason law that targets human rights activists and limits freedom on the internet).10¶ Russia’s countermeasures were not limited to defense. Its offensive toolbox was enhanced as well. Following the Arab Spring and the concomitant protests in Russia, the first reports referring to the Internet Research Agency (IRA), the St. Petersburg-based troll farm, emerged.11 The Russian leadership used the IRA to conduct an offensive against its domestic opponents (e.g., Russian opposition leader Alexei Navalny as early as 2013), but also international opponents (e.g., the United States’ 2016 presidential election).12¶ While targeting the United States, Russia’s strategy included running fake social media accounts pretending to be everything from alt-right voices to Black Lives Matter activists. The goal was to increase polarization and violence. Evidence of Russian meddling in the 2020 U.S. elections is now also emerging. A number of reports have described the use of fake Instagram accounts to discredit then U.S. presidential candidate Joseph R. Biden, Jr.13¶ Moreover, the Russian disinformation machinery has sought to amplify the voices of QAnon, a conspiracy theory collective that believes that former U.S. President Donald J. Trump is the guardian against a coup and that Hillary Clinton and her allies are running sex-trafficking rings.14¶ The Russian disinformation machine often maintains a high degree of coherence across channels and regions in terms of key messages, but not always in delivery. This is to a large degree the result of coordination from the top by Dmitry Peskov, Russian President Vladimir Putin’s press secretary. Peskov’s weekly meetings with representatives of pro-Kremlin media outlets are combined with guidelines for social media farms and foreign embassies.15 This is what allows for a high degree of coherence (although never flawless) between the different arms of the Kremlin machinery.¶ Another less noticed, but no less effective, way of pushing Russian narratives against the EU and NATO is evident in the Western Balkans. The Western Balkans are today at the front line between the EU and NATO on the one hand and Russia on the other. The states of the Western Balkans are on a steady, but slow, path to integration with the EU and NATO. Up until 2014, the Russian leadership did not seem to care too much about this, but after Russia invaded Ukraine that year its ambitions grew in the region. Montenegro, in particular, concluded association negotiations with NATO in May 2016 and joined the Alliance in June 2017. Coincidentally, Montenegro experienced an increase in cyberattacks both in terms of sophistication, but also in numbers, from 22 in 2012 to more than 400 in 2017.16¶ Russian leaders wanted to make an example of Montenegro for states pondering NATO membership. Around the time of the Montenegrin parliamentary elections on October 16, 2016, pro-NATO and pro-EU political parties as well as civil society groups and electoral monitors were targeted by large-scale distributed denial-of-service (DDoS) attacks. The cyberattacks were traced to APT28, also known as Fancy Bear, a hacking group with ties to Russia’s military intelligence service, GRU.17 There was also a coup attempt ahead of the elections that sought to topple the government and assassinate then-Prime Minister Milo Đukanović. The coup plotters were identified as GRU officers Eduard Shirokov (nom de guerre Shishmakov) and Vladimir Popov.18 They were indicted in 2017 along with 12 other people with Russian, Serbian, and Montenegrin citizenship.19¶ The cyberattacks, intelligence operations, and subversion in Montenegro should be seen in conjunction with Russia’s larger information offensive against the Western Balkans. A key instrument in that offensive has been Sputnik Serbia (Srbija), which has focused on providing pro-Russian, anti-EU, and anti-NATO narratives. Sputnik has been successful as it allows for free reproduction of its articles, which results in these articles being widely published by outlets with few resources.20 In other words, Russian disinformation is successful not so much because of illegal methods, but rather because it exploits opportunities presented by the structural transformation, or crisis, in the media.¶ It is hard to assess the aggregated impact of this disinformation in the international domain, but some examples can be illustrating. For example, 42% of Serbians see Russia as their best partner and 14% the EU. This is the case even while Russian trade and aid to Serbia is just a fraction of that of the EU.21¶ The case of Montenegro provides a vivid example of the combination of offline and online tools used by Russia, and the Russian leadership’s broader desire to undermine NATO and EU membership. By themselves, the cyberattacks or the information efforts might seem like minor nuisances, but the combination of these different tools is what makes them potent and gives them synergies.

### 1nc – Deterrence Fails

#### Cyber deterrence fails- attribution, ubiquity of tech, and unenforceable threats of retaliation

Katrina Manson May 2, 2022

Nobody Knows Where the Red Line Is for Cyberwarfare; Bloomberg; https://www.bloomberg.com/news/articles/2022-05-02/russia-cyberattacks-raise-questions-about-hacking-red-lines

The Department of Defense is preparing a new cyber strategy this year that’s likely to include a more prominent role for deterrence. U.S. officials and policy experts have been debating whether it’s better to dissuade attacks with the promise of retaliation in cyberspace or elsewhere, or to try to prevent them by taking offensive cyber measures that cut off rivals’ ability to carry them out. The Biden administration’s strategy will be based on integrated deterrence—the concept that attacks can be prevented by threats of economic penalties or other responses that rely on various levers of U.S. power.¶ Lawmakers from both parties and experts from outside government are pushing for their own vision of deterrence. A two-year, congressionally mandated bipartisan effort that concluded last year, the Cyberspace Solarium Commission, favors a variation of the theme “layered cyber deterrence,” which combines a focus on hardening technical defenses against attacks with the promotion of international norms against, say, cyberattacks targeting civilian infrastructure.¶ Read More: How Nations Attack Without Bullets or Bombs¶ Goldstein’s faith that the threat of catastrophic response could prevent state-sponsored cyberattacks makes him an outlier. Deciding when to respond would be fraught, because determining who has carried out any breach can be tricky. The best hackers often mask their identities. Russian hackers, for instance, have left bread crumbs suggesting they’re North Korean or Iranian, cybersecurity experts have said. Officials say they’ve become better in recent years at determining responsibility for attacks.¶ Unlike nuclear weapons, which haven’t been used since World War II, the tools of cyberwarfare are widely available and used regularly for attacks of varying seriousness. “Redlines are notoriously difficult to define in cyberspace,” Emily Goldman, a cyber strategist at U.S. Cyber Command, wrote in a 2022 paper for the journal The Cyber Defense Review. She argued that sanctions, criminal indictments, and other deterrent measures have proven ineffective: “More of the same will not produce different results.”¶ General Paul Nakasone, the leader of the U.S.’s 6,000-person military Cyber Command and one of the speakers at Goldstein’s event, has dismissed the nuclear parallels. “Cyber deterrence is not nuclear deterrence,” he told Congress in April. For the past several years he’s overseen an increase in the Pentagon’s continuous offensive cyber operations outside U.S. borders, under a strategy he’s described as “defending forward.”¶ The U.S. began changing its approach when Russian interference in the 2016 presidential election led U.S. leaders to overcome their reluctance for counteroffensive cyberattacks, according to Jonathan Reiber, who authored the government’s 2015 cyber strategy when he was the chief strategy officer for cyber policy at the Department of Defense. In 2018, Congress changed the legal definition of offensive cyber operations, classifying them as traditional military activity. That same year the Trump administration issued a classified policy memo that some U.S. lawmakers said essentially delegated authority to the Defense Department to conduct them without the White House signing off.¶ Nakasone told Congress that both the legal change and the policy memo have been “very helpful.” The Biden administration is reviewing the memo, and proponents of the “defend forward” strategy worry it could decide to restrict Cyber Command’s ability to act effectively.¶ One problem with using the threat of cyberattacks as a deterrent is that cyber superiority is inherently ephemeral, according to Nakasone. While a nuclear arsenal’s power is persistent, cyberweapons rely on exploiting vulnerabilities in code, which can be patched and disappear as quickly as they’re found. So, unlike nuclear weapons, Nakasone’s cyber arsenal and access routes must change all the time. The U.S.’s ability to find and exploit such vulnerabilities is significant, but its ability to carry out attacks on specific targets may ebb and flow.¶ Some academics argue that “defending forward” is a euphemism for the U.S. waging its own attacks. In a paper for the Atlantic Council in March, cyber coercion expert Jenny Jun argued that the strategy leaves “much room for misjudgment and misinterpretation” about how the U.S. will respond and that instead of being a deterrent, it could encourage adversaries to strike first rather than wait to be compromised themselves.

### 2nc – No Deterrence

#### No cyber deterrence- attribution and diffuse technology make failure inevitable

Emilio Iasiello in 2018

chief threat analyst for a global cyber intelligence firm, supporting federal and¶ commercial entities to manage cyber risks, understand their threat environment, and help prioritize their¶ investments against those threats impacting their business or mission; Is Cyber Deterrence an Illusory¶ Course of Action?; ASPJ Africa & Francophonie; https://www.airuniversity.af.edu/Portals/10/ASPJ\_French/journals\_E/Volume-09\_Issue-1/iasiello\_e.pdf

With the U.S. government (USG) acknowledgement of the seriousness¶ of cyber threats, particularly against its critical infrastructures, as well¶ as the Department of Defense (DoD) officially labeling cyberspace as¶ a war fighting domain, security experts, policymakers, and think tank¶ researchers have resurrected a potential Cold War strategy to implement against the¶ new threats fermenting in cyberspace.1¶ It is argued that the same principles that successfully contributed to nuclear deterrence with the Soviet Union can be applied to¶ cyberspace and the hostile actors that operate within. However compelling, similar¶ strategies are not transferrable and the key factors that made nuclear deterrence a¶ viable solution do not carry the same value in cyberspace. While only a handful of¶ states have demonstrated the capability to develop nuclear weapons, more than 140¶ nations have or are developing cyber weapons, and more than thirty countries are¶ creating military cyber units, according to some estimates. Moreover, this threat actor¶ landscape does not consist of nation states alone. Included are cyber criminals, hackers, and hacktivists of varying levels of sophistication and resources willing to use¶ their capabilities to support nefarious objectives.2¶ There are advocates favoring the implementation of a cyber deterrence strategy¶ to mitigate the volume of hostile cyber activity against public and private sector interests. However, too many factors—including attribution challenges and sustainability against this vast threat actor landscape—inhibit cyber deterrence options from¶ achieving their desired outcome in the near term. What’s more, other deterrent strategies such as those employed against nuclear weapon use, terrorism, and rogue state¶ behavior are not suitable models for the cyber realm. Despite some commonalities,¶ the cyber domain lacks the transparency and actor visibility required to develop deterrence measures. Despite these hindrances, nation states should seek to develop, ¶ refine, and implement national level cybersecurity strategies that focus on cyber defense improvements and enforce accountability to measure their successes. While¶ there will always be sophisticated actors able to thwart the most robust cybersecurity¶ defenses, the success of hostile activity against networks are the result of poor cybersecurity practices such as unpatched systems and users not well trained in information assurance principles. Cybersecurity is an ongoing effort that needs to be relentlessly monitored and adapted to a constantly changing threat environment.

#### Deterrence by denial fails - doesn’t stop the incentives for cyber attacks

Taddeo 18 [Mariarosaria Taddeo, Oxford Internet Institute, University of Oxford; “The Limits of Deterrence Theory in Cyberspace,” Philos. Technol; <https://link.springer.com/content/pdf/10.1007/s13347-017-0290-2.pdf>]

Anticipating, defence is guaranteed to be ineffective as a deterrence strategy in cyberspace because cyber defence mechanisms have little control over cyber attacks. This deprives defence of any strategic power (Taddeo 2017a, 2017b) and transforms it into a means of ensuring resilience of information systems, rather than a means to deter new attacks. Let me unpack this analysis. Defence in cyberspace is porous in nature (Morgan 2010); every system has its security vulnerabilities and identifying and exploiting them is simply a matter of time, means, and determination. This makes ephemeral even the most sophisticated defence mechanisms, thus limiting their potential to deter new attacks (Taddeo 2017a). At the same time, even when successful, cyber defence does not lead to a strategic advantage, insofar as dismounting a cyber attack very rarely leads to the ultimate defeating of an adversary. This creates an environment of persistent offence (Harknett and Goldman 2016), where attacking is tactically and strategically more advantageous than defending. An ‘offence-persistent’ environment differs from an ‘offence-dominant’ environment, in that defence is under constant stress, but is not superfluous, and the success of the offence is not a given. In an offence-persistent environment, defence can achieve tactical and operational success in the short term if it can adjust constantly to the means of attack, but it cannot win strategically. Offence will persist and the interactions with the enemy will remain constant (Harknett and Goldman 2016). In this kind of environment, deterrence by defence is guaranteed to be ineffective, as defence does not discourage attackers from their intention to offend. This is even more so in cyberspace, where uncertainty of attribution, low entry cost of attacks, and the inherently vulnerable nature of information systems encourage attackers to test defences. In cyberspace, defence remains salient and necessary, but primarily as a means to guarantee the resilience of a system once an attack has been launched (and also after it has breached the system), rather than as a means of deterring attackers (Bologna et al., 2013; Bendiek and Metzger 2015). Cyber defence, then, is more akin to safety engineering, in that it mitigates and manages the risk following an attack (Libicki 1997; Rattray 2009), rather than avoiding them.

#### Too many disagreements for Article 5 invocation

Jeane **Kirkpatrick** Visiting Research Fellow, American Enterprise Institute, **4-25**, 22, The Russian cyber threat is here to stay and NATO needs to understand it, https://www.aei.org/op-eds/the-russian-cyber-threat-is-here-to-stay-and-nato-needs-to-understand-it/

**Even if allies wanted to trigger Article 5 over cyber operations, disagreements about the definitions of threats, origins of attacks, and pain thresholds in cyberspace can derail the process. Collective retaliation requires a unanimous vote across NATO;** building unity across these points is nearly impossible for most cyber activity. **Unlike missile attacks or tanks in the streets, few “red lines” exist to distinguish cybercrime, cyber espionage, and cyber disruption from digital acts of war.** Beyond the bureaucratic and logistical limitations of elevating cyber to a casus belli, **focusing on cyber-attacks as acts of war distracts from the more likely Russian digital assaults below the level of armed conflict. These include ransomware attacks and supply chain infiltrations that look like criminal activity or espionage. The Kremlin is particularly adept at the latter.** In the SolarWinds compromise, Russia hacked one company’s software product to access networks of Fortune 500 companies and U.S. government agencies. Spillover from operations in Ukraine poses an additional risk. The Russians have already deployed several digital tools to destroy computer data, resulting in corrupted computers for Ukrainian companies with government support roles. The same malicious software has also affected several Latvian and Lithuanian businesses. The danger is another situation like NotPetya in 2017, where malware self-replicated, spread past Ukrainian targets to cripple networks in over 150 countries, and created $10 billion in damages. **Each of these scenarios are much more likely than a “cyber doomsday” that would justify an Article 5 response from NATO members.** To be fair, policymakers’ fears of cyber war have led to some positive developments for the alliance. For instance, over the last several years, NATO has developed its own framework for combining cyber and conventional military capabilities in warfighting. But allies remain unprepared to deal with “death by 1000 cuts” in cyberspace. **Concentrating only on acts of war comes at the expense of addressing the cumulative costs of low-level cyber threats over time. It leads to an overreliance on cyber deterrence or defensive whack-a-mole strategies, neither of which are sustainable.** Threats of retaliation simply don’t deter most cyber-attacks, and it is unrealistic for defensive measures to stop every hacker.

#### Deterrence through denial of attacks is impossible- the tech is too dynamic and changing.

Emilio Iasiello in 2018

chief threat analyst for a global cyber intelligence firm, supporting federal and¶ commercial entities to manage cyber risks, understand their threat environment, and help prioritize their¶ investments against those threats impacting their business or mission; Is Cyber Deterrence an Illusory¶ Course of Action?; ASPJ Africa & Francophonie; https://www.airuniversity.af.edu/Portals/10/ASPJ\_French/journals\_E/Volume-09\_Issue-1/iasiello\_e.pdf

In cyberspace, the effort to counter hostile acts through use of preemptive or¶ retaliatory strikes may seem like a step in the right direction, especially when considering the failures suffered by defenders to mitigate the threat of malicious activity.¶ However, thousands of cyber attacks occur per day, suggesting great difficulty in distinguishing serious threats from minor ones.50 Stepping on an ant in your kitchen¶ doesn’t prevent an infestation; similarly, cyber deterrence is not a panacea for threat¶ actors seeking to exploit public and private sector networks. At present, there are too¶ many unexplored variables and an undeveloped plan for its use to make this an effective course of action.¶ Attribution challenges, the ability to respond quickly, effectively, and accurately,¶ and the ability to create and sustain a model by which repeatability can be leveraged¶ against different threat actors will continue to prove too insurmountable in the near¶ term for victimized countries to launch pre-emptive or retaliatory cyber strikes. Cyber deterrence by denial has a better chance of succeeding; however, only in a limited¶ capacity as network defenders have consistently been beaten by smarter, more agile¶ adversaries obfuscating themselves in cyberspace. Instead of striking back against¶ adversaries, organizations need to evaluate their current security postures to determine its effectiveness in the current cyber climate.

# Offense

## Russia Turn

### 1nc – Russia Turn

#### Pursuing security cooperation with NATO over cyber sparks confrontation with Russa.

Zhiping 22 [Qi Zhiping, Chinese Academy of Sciences 4-22-2022 US sets dangerous precedents in cyberspace Global Times. https://www.globaltimes.cn/page/202204/1260039.shtml] 6-14-2022

Paul Nakasone, the Commander of US Cyber Command and Director of the National Security Agency, noted recently in a testimony before the US Senate that before the outbreak of the Russia-Ukraine conflict, the command “supported” Ukraine in cyberspace. After the outbreak, the US reinforced its “hunt-forward” operation and helped Ukraine strengthen its cyber defense. In fact, the US interference in the crisis through cyberspace is much more than just helping Ukraine with its defense, the US is also supporting it against Russia on all fronts, including cyber offense and defense, information awareness, digital connectivity and cyber intelligence, setting several extremely dangerous precedents. The first precedent is cyber warfare between nuclear-weapon states. Since the beginning of the Russia-Ukraine conflict, the US has repeatedly stressed that it will not be engaged in an armed conflict with Russia and has refrained from establishing a no-fly zone and test-launching intercontinental ballistic missiles. This indicates US clear understanding of the possibility of escalating the situation and even triggering a nuclear war with Russia. However, at the same time, the US is confronting Russia head-to-head in cyberspace even at the frontline. The reason is that the US believes it can unilaterally control the scale and consequences of cyber conflict with its technical superiority. However, as the Internet has gone deep into all aspects of social life, the width and depth of the impact of cyber warfare may be beyond the control of any country. In the context of a hot war, situations won’t exactly follow the US script that whether engagement in cyberspace would be considered armed engagement or whether it would provoke another nuclear weapon state to escalate the conflict. Against the backdrop of Russia’s announcement to raise its nuclear preparedness and unspecified cyberattacks on Russian nuclear facilities, US direct engagement in cyber conflict with Russia will easily lead to a strategic miscalculation. The Russian Foreign Ministry condemned the US and NATO in a statement for waging a cyber war against Russia involving a broader scale of hackers. This is a stern warning against the US’ “dangerous game” in cyberspace which would possibly trigger a conflict between nuclear-weapon states. The second precedent the US sets is a proxy war in cyberspace. The US uses China and Russia as imaginary enemies to promote its cyber strategy of “hunt-forward” and “persistent engagement.” The US is deeply involved in building the cyber power of Ukraine, using it as a bridgehead for close reconnaissance, network penetration and cyber attacks against Russia, preparing for its cyber confrontation with Russia. Apart from Ukraine, the US is also doing the same in the Asia-Pacific region, hyping China’s cybersecurity threats to China’s neighbors and thus luring them into “cybersecurity cooperation” in an attempt to bring the US cyber tentacles to China’s doorstep. This is similar to US intention of deploying its missile and anti-missile systems in the vicinity of China and Russia, which not only enhances the US deterrence and offensive capabilities, but also takes the opportunity to force China and Russia’s neighboring countries to the US’ chariot. The tragedy in Ukraine is a lesson to be learned. For the US, there will be a greater security dilemma with the pursuit of its own absolute security in spite of security concerns of others, or even at the cost of others’ insecurity. With good intentions to strengthen cyber security and cooperation with the US, regional countries not only failed to enhance their own security, but also put themselves in the vortex of competition between major powers, and even became cannon fodder for major power confrontation. The third precedent has been set for non-compliance with international rules. The US clamors that cyber attacks constitute armed attacks, and pushed NATO to declare for the first time at its 2021 summit that "significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack.” But the US launched such cyber activities that should be defined by itself as “armed attacks” against Russia. The US underlines that all offline rules apply online as well, fabricating cyber attacks charges, accusing other countries and abusing sanctions. At the same time, the US sees the digital world as a "land beyond law," and does not hesitate to attack other countries' critical infrastructure. While advocating democracy, freedom and human rights and opposing information manipulation and disinformation, the US cut off the Internet services for Russia, blocked Russia’s voice, and spread disinformation against Russia without limits, in a bid to confuse the public. Behind these actions is the arrogance of the US and its blatant double standards for international rules. Coincidentally, the US completely ignored the international consensus reached last year of “developing and implementing globally interoperable common rules and standards for supply chain security,” in the UNGGE report, and deliberately created closed and exclusive small circles to discuss supply chain issues for geopolitical purposes. What the US wants has never been universally applicable international rules in cyberspace, but "domestic laws" and "rules of its small gang" to serve its own selfish interests. The “framework for responsible State behavior” which the US claimed to adhere to only holds other countries accountable, and the US itself is above international rules. Washington’s practices of disregarding international rules have severely interfered with the efforts of the international community to establish order in cyberspace, and may even lead to serious consequences of a collapsed order. Cyberspace is a common space shared by all countries. The US should stop “playing the touch ball” in cyberspace. Instead, it is supposed to shoulder the responsibility of a major power, avoid strategic misjudgments, and earnestly maintain strategic stability among major powers and build a peaceful and secure cyberspace.

### 2nc – No Attacks Now

#### Russia not pursuing major cyberattacks in response to sanctions now but could be pushed to the brink.

Ishak ‘22 [Natasha Ishak is an independent journalist covering politics and public policy for Vox. Her work has been published by VICE, Fortune, Mic, The Nation, Harvard's Nieman Lab, and the Village Voice among other places.3-19-2022 Is Russia holding back from cyberwar? Vox https://www.vox.com/2022/3/19/22986316/russia-ukraine-cyber-attacks-holding-back] 6-5-2022

Why hasn’t Russia launched major cyberattacks yet? The lack of full-scale Russian cyberattacks is a phenomenon that has surprised some experts, including Wertheim. “On some level,” he said, “the reason Russia launched a full-scale war against Ukraine is precisely that it didn’t think cyber means were sufficient. But one might have expected the war itself to have involved more cyber operations.” It’s difficult to know exactly what is behind Russia’s behavior, but experts have speculated about a number of potential reasons why Russia has hesitated to launch any stronger attacks. Some have theorized that Russia’s cyberwarfare capabilities may have been inflated, which is why it has not thus far launched a more sophisticated cyberattack against Ukraine or its Western allies. However, a more likely reason may be that Russia is still weighing its options carefully, and is simply waiting for the right time to respond. “It could be that Russia fears retaliation that would set its cause back, at least at this point,” said Wertheim, noting the relative lack of progress by Russia’s armed forces so far. “Perhaps over time, if and when Russian leaders believe that the situation is stabilized then Russia would be better able to absorb retaliation, it could launch a cyberattack then. It’s possible.” Given the setbacks that Russia has encountered on the battlefield, combined with the notable resistance by Ukrainian forces that have held steady against Russia’s attacks for the last three weeks, it may also be a matter of Russia prioritizing its military actions, according to Wertheim. “There might just simply be a kind of finite attention problem operating for [Russia],” he said. According to Olena Lennon, an adjunct professor of political science and national security at the University of New Haven, setbacks for Russia include the loss of junior, and even some higher-level, commanders among its military personnel, which may be affecting its operations on the ground. “We’re definitely seeing some leadership deficiencies that could explain some of these surprises,” Lennon said. The US could also be a target of Russian cyberattacks US authorities were already wary of a possible cyberattack from Russian hackers as a potential response to US support for Ukraine. That concern has only increased following major sanctions imposed on Russia by Western powers, as well as escalating rhetoric from Russian President Vladimir Putin. Putin described the sanctions as “akin to declaring war,” and Russian government officials have warned there will be swift action from Russia in response. US officials warned public and private entities of potential ransomware attacks after President Joe Biden announced initial sanctions against Russia late last month. “DHS has been engaging in an outreach campaign to ensure that public and private sector partners are aware of evolving cybersecurity risks and taking steps to increase their cybersecurity preparedness,” a DHS spokesperson said in a statement to the press. But the strong response against sanctions that Russian officials have warned of has yet to materialize in the weeks since. Although it’s certainly possible that Russia will react to US sanctions at some future point, the absence of action so far is notable, according to Wertheim. “It’s very hard to sort of assign exact probabilities to these kinds of things,” Wertheim said. “But it’s notable that there hasn’t been a response. And I think it remains a real possibility that even if the West does nothing more to escalate in a conflict that Russia could do so by undertaking what it believes is retaliation.” That could be particularly likely as the impact of already-imposed sanctions continues to mount. Sanctions have had an enormous effect on day-to-day life inside the country: The value of the ruble, Russia’s official currency, has plummeted to less than 1 cent, and Russian citizens have already seen price surges, particularly for electronic goods and appliances. The early price hike has motivated many residents to stock up on items in case prices continue to rise as the conflict rages on. “For the past few days, it’s been like Christmas for us,” one electronics-shop staffer told the Financial Times. “People are ready to buy things even [though] we have been raising prices every few hours based on the forex situation.” With heavy economic sanctions already in place, Wertheim says there are potential risks to pushing Putin further into a corner, which in itself could motivate Russia to take more drastic measures — including, potentially, cyberattacks — as the war continues. “What I most worry about is a circumstance in which Vladimir Putin thinks that his regime may be teetering and that he has to do something dramatic to change the status quo in order to maintain his grip on power,” Wertheim said. “And, thus, perhaps his own personal survival.”

#### Russia has threatened retaliatory measures—accuses the US of cyber aggression.

Ignatius 22 [David Ignatius, associate editor, foreign affairs Washington Post 6-7-2022 Opinion Washington Post https://www.washingtonpost.com/opinions/2022/06/07/us-russia-conflict-is-heating-up-cyberspace/] 6-13-2022

As the war in Ukraine rages, a long-standing battle between Russia and the United States over cyberspace is also heating up, with a top Russian diplomat warning of “catastrophic” consequences if the United States or its allies “provoke” Russia with a cyberattack. The “information space,” as the Kremlin likes to call it, has been a growing domain of U.S.-Russian conflict, not only in the Ukraine war, but in Russia’s hacking attacks against the presidential campaigns in 2016 and 2020 as well as the congressional elections in 2018. The two countries briefly seemed to be working together for common rules for cyberspace last year, but that cooperation has now exploded. Andrei Krutskikh, the top cyber expert at the Russian foreign ministry, charged in an interview on Monday with the Russian newspaper Kommersant that the United States had allegedly “unleashed cyber aggression against Russia and its allies.” He claimed that Washington was using Ukrainian President Volodymyr Zelensky and “the IT Army created by him to carry out computer attacks against our country as a battering ram.” Krutskikh continued ominously: “We do not recommend that the United States provoke Russia into retaliatory measures. A rebuff will certainly follow. It will be firm and resolute. However, the outcome of this ‘mess’ could be catastrophic, because there will be no winners in a direct cyber clash of states.” To back up Krutskikh’s claim that the United States has attacked Russian cyber targets, Kommersant cited a June 1 comment by Army Gen. Paul Nakasone, head of U.S. Cyber Command. Speaking about Ukraine during a visit to Estonia, Nakasone told Sky News: “We’ve conducted a series of operations across the full spectrum: offensive, defensive, [and] information operations.” A Cyber Command spokesman had no comment. A senior State Department official said Krutskikh’s allegations were “nothing new” and a “rehash” of past statements. The Biden administration, for its part, accused Russia last month of conducting “malicious cyber activity” against Ukraine, including an attack on a commercial satellite communications network that damaged systems in other European countries. The State Department condemned Russia’s cyber-meddling, but the senior official said the United States hasn’t seen the “huge attacks” some were expecting, perhaps because the Russians “don’t want a war on two fronts.” Krutskikh contended that a “freeze” by the Biden administration in developing a common approach to cybersecurity had reversed progress made last year at the United Nations. U.S. and Russian officials had endorsed a joint U.N. resolution in October outlining a framework for discussing cybersecurity issues. Krutskikh called it a “historic moment.” But at that time, the Russians were already preparing their invasion of Ukraine, which began on Feb. 24. Even so, contact between the two countries on cyber issues has continued, with two meetings since December and another scheduled in July, the senior official said. The Kremlin’s cyber chief said Monday that Russia was still ready to negotiate “appropriate legal agreements with all states that soberly assess the threat of cyberwarfare.” But that same day, Russia included Michele Markoff, the State Department’s cyber security coordinator and the main channel of contact with Krutskikh, on a new list of sanctions permanently banning travel to Russia. Russia’s view of the internet is fundamentally different from that of the United States, the senior State Department official said during an interview on Tuesday. Whereas the United States seeks an open, free and interoperable system, Russia wants “an internet with sovereign borders,” where it can suppress speech it doesn’t like. Russia’s obsession with cyberspace partly reflects Moscow’s view that the United States controls the internet and its governance. A favorite Russian target is a group of experts known as ICANN, which oversees the internet’s system of domain names. ICANN used to operate under a Commerce Department contract but has been fully independent since 2016. On Monday, the group published a compendium of Russia’s attempts to rewrite internet rules, through the United Nations or other international regulatory bodies it seeks to control. From President Vladimir Putin on down, the Russians quoted in the ICANN report resent the United States’ digital dominance. The U.S.-Russian contest over cyberspace will play out in this September’s election for a new secretary general of the International Telecommunications Union, a U.N. agency that could, in theory, take over internet governance. Two leading candidates are Doreen Bogdan-Martin, an American who currently runs one of the ITU’s bureaus, and Rashid Ismailov, a Russian who has worked in his country’s communications ministry and for Huawei, Nokia and other companies. Watch that space, folks. The internet confrontation is a microcosm of Russia’s larger standoff with the West. Russia yearns for recognition as a great power and global standard setter. But as the war in Ukraine grinds on, Putin has become ever more prickly, isolated and angry at his foes. He is severing Russia’s connections to the world, even as he seeks to dominate cyberspace. His computer is crashing, and he doesn’t seem to know how to reboot.

### 2nc – Russia Retaliates

#### Use of NATO to bolster cyber defense fuels Russian fears of encirclement.

CEPA 21 [The Center for European Analysis (CEPA) is a non-partisan think-tank dedicated to strengthening the transatlantic relationship. Headquartered in Washington, D.C. and led by seasoned transatlanticists and young leaders from both sides of the Atlantic, CEPA brings an innovative approach to the policy arena. Our cuttingedge analysis and timely debates galvanize communities of influence while investing in the next generation of leaders to understand and address present and future challenges to transatlantic values and principles. The Evolution of Russian Hybrid Warfare January 2021 <https://cepa.org/wp-content/uploads/2021/01/CEPA-Hybrid-Warfare-1.28.21.pdf>] 6/16/2022

The chaos strategy, and the tactical use of hybrid warfare, was borne out of the perception among the Russian leadership that Russia is locked in a form of greatpower competition with the United States and Europe, as well as increasingly with China. The stakes are high: ultimately, it is about the survival of the current Russian regime.4 For decades since the end of the Cold War, Russian authorities have been feeding a sense of post-Cold War humiliation that Russia’s security concerns were not sufficiently taken into consideration, if not downright ignored. This grievance narrative is reinforced by a “besieged fortress” mentality at home that is fueled by a fear of encirclement by NATO forces and exclusion from the European security architecture. This would have forced Russia to choose confrontation over cooperation with the West. The Russian leadership has the perception that there is a window of opportunity to take action and make foreign policy and security intentions a reality5 — the war with Georgia in 2008 was a harbinger of Russia’s reassertion. What followed were calculated steps aimed at doing away with an international order the Kremlin leadership feels cheated by and disappointed with. For Russia, the problem remains that it cannot compete in a direct contest of national power — political or conventional military — with its peer and near-peer competitors. The Russian leadership fundamentally feels its conventional military is inferior to the West’s, and especially NATO. Therefore, as Russia cannot compete symmetrically, it chooses to contest and disrupt asymmetrically.6 It follows that Russia has seeded chaos via asymmetrical means through disinformation, cyberattacks, political subversion, business ties, and economic warfare, among other tools. The approach has combined both old and new, drawing on lessons from the successful use of Soviet-era asymmetric strategies, but amplified with the power of modern technology and social media. Nonmilitary hybrid tools, as those being pondered by Russian military planners, are part of warfare per se. 7 Such means represent a coordinated and tailored effort at the strategic level to reshape the internal course — be it political, economic, or societal — of target countries. Russia uses a synergetic and convergent toolkit of military and nonmilitary tactics8 in its protracted conflict with the West, honed by a willingness to alter, by force if necessary, the Western-led liberal international order. This effort also seeks to increase Russia’s international standing in absolute and relative terms as well as advance Russian interests against the West.

#### Err neg – any effort at security cooperation by NATO is likely to be perceived as antagonistic by Russia

Pezard and Rhoades 20 [Pezard, Stephanie, Senior Political Scientist and Associate Research Department Director for Defense and Political Sciences (DPS) and Ashley L. Rhoades, Policy Researcher Washington Office, RAND Corporation. What Provokes Putin's Russia? Deterring Without Unintended Escalation. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/perspectives/PE338.html.]

Although the United States and its allies can make every effort to send clear signals and communicate effectively with Russian leadership, there is always a risk that Russia will misinterpret U.S. and NATO actions. A variety of factors beyond the control of the deterring party—including cultural differences, cognitive biases, irrational behavior, and f lawed assumptions—can cause the target state to mis-read or misjudge the actions of its adversary.99 Domestic concerns or political constraints can also color how a state perceives and reacts to the actions of its adversary. One potent example of misperception occurred in 1983, when the Russians mistook a NATO nuclear warfare exercise called “Able Archer” as a cover for an actual nuclear strike, and nearly retaliated in kind.100 Only belatedly did then-President Ronald Reagan come to the realization that [m]any people at the top of the Soviet hierarchy were genuinely afraid of America and Americans many of us in the administration took it for granted that the Russians, like ourselves, considered it unthink-able that the United States would launch a first strike against them. But I began to realize that many Soviet officials feared us not only as adversaries but as potential aggressors who might hurl nuclear weapons at them in a first strike. . . .101 This incident illustrates the importance of trying to understand how the other side will interpret one’s actions and the dangers of presuming that the adversary will share the same logic and assumptions. Moreover, Russia tends to view any defense- or security-related actions taken by the United States or NATO in the European theater as being targeted at it, regardless of the actual intent behind these actions. As one RAND report notes, Any actions in Europe to support American operations elsewhere have been and will be observed by a Russian military more interested in us than we are in it. It is critical that operational planning take this into account and that planners and operators take steps to prevent Russia from mistaking operations and actions as unintended “signals.”102Of course, Russia may also make such claims about perceived U.S. and NATO “aggression” with the aim of justifying its own defense- or security-related actions. Whether rooted in genuine concern over U.S. actions or political theater, the reality is that Russia frequently does not modulate its responses based on the perceived or stated U.S. intent behind its actions, but rather reacts to transgressions of its redlines irrespective of the reason behind the violation. Nonetheless, if U.S. and NATO planners fail to account for Russian sensitivities and assumptions when deciding on courses of action, seemingly minor or irrelevant actions could inadvertently trigger escalation with Russia. Deterrence strategies must also be designed with careful consideration of the broader context and environment in which they will be applied. Because some deterrence measures take a long time to implement, the context might have changed by the time they are enacted, which can “inadvertently signal aggressive intent under changed cir-cumstances.”103 A recent example was the timing of events when NATO revealed, in May 2016, that it had installed a 16missile defense site in Romania and was beginning work on a site in Poland. At the same time, NATO announced a series of unconnected posture-enhancement proposals in preparation for the approaching Warsaw Summit. The coincidence of these actions further convinced Russia that it is the intended recipient of those ballistic missile defense systems, despite U.S. assurances to the contrary. In a similar vein, multiple deterrent actions undertaken in a short time span can have the cumulative effect of crossing a red-line, even if the individual actions would not have had such a significant effect. For instance, the placement of newly developed Pershing II ballistic missiles in West Germany the same year as the Able Archer exercise drastically raised tensions and Soviet paranoia over U.S. and NATO actions, leading to the Soviet decision to raise its nuclear alert statuses and prepare for nuclear war. Policymakers therefore should “consider delaying final completion or announcements of posture enhancements that may take place during times of heightened tension and should routinely reassess posture decisions in the process of being implemented.”104Otherwise, actions that would strengthen deterrence under different circumstances may counterproductively increase the risk of escalation. In some cases, deterrence may fail to prevent escalation because there is too great an asymmetry of stakes or interests between the parties involved. In these instances, An enemy that perceives that its stakes are high will be willing to bear greater costs and, therefore, will be less sensitive to threats of punishment. And if that enemy believes that the threatener’s stakes are low, there may be doubt that the threatener is willing to bear the reciprocal costs of escalation or pay the political price of carrying out the threats.105 Should Russia believe it faces an existential threat from the United States or U.S. allies, it will most likely decide that the costs of not acting outweigh the risks associated with escalating to full-scale war. Similarly, if the Russian interest in achieving a certain objective far outweighs U.S. interests in pursuing the objective, the United States may choose to back down. Putin also has demonstrated a high level of opportunism and a willingness to use any low-cost opportunities available to expand the Russian sphere of influence, destabilize adversaries, or otherwise strengthen Russia’s position in the world order. If Putin believes the United States and NATO have a low level of interest in a particular area, he may seize the opportunity to act, calculating that he can do so without risking escalation. This may lead to a problematic pattern of probing for U.S. and NATO resolve and looking for areas of weakness to exploit. Relatedly, unpublished RAND research suggests that Putin’s appetite for risk may be high, and will remain so as long as he continues to enjoy high levels of support from Russian elites and retains the ability to sell oil and gas to other countries.1

#### The link straight turns deterrence and takes out the case — Russia only has an incentive to start a nuclear crisis when they are provoked — don’t poke the bear!

Taylor ’22 — Jeffrey; the managing partner of U.S. Government Relations Intl., LLC (USGRI), a comprehensive and cost effective government affairs firm. 2022; "Deterring Russian Nuclear Threats with Low-Yield Nukes May Encourage Limited Nuclear War." *Journal of Advanced Military Studies*, Volume 13; <https://muse.jhu.edu/article/851414>; //CYang

U.S. and NATO war games and military exercises can also be leveraged to enhance resilience against inadvertent escalation. The purpose of deterrence is to prevent nuclear war and therefore must account for any number of ways in which it might start. Current American deterrence policies toward Russia are largely focused on putting barriers in place to prevent the onset of nuclear escalation by aggression. Such escalation would almost certainly have a catastrophic [End Page 222] global impact. However, Russia has very little incentive to start a nuclear war through aggression, making the probability of this scenario relatively low. An arguably more likely scenario is that the security situation in Eastern Europe would precipitate a conventional conflict in which U.S./NATO military actions, strategic misperception, or an accident caused by an operational error could create a crisis that provokes a nuclear response by Russia. Planning for this type of scenario is complicated by the fact that Russia's already uncertain operational threshold for nuclear use is likely to shift in a conflict. However, by building scenarios — based on an accurate assessment of Russian doctrine and threat perceptions — that simulate these types of challenges and uncertainties in military exercises, Western military and political decision makers can gain insights into what events Russia or the United States might most easily misinterpret and what actions are most likely to prompt a nuclear response. From these insights, policy makers and defense planners can craft resilient operational deterrence policies that better anticipate and mitigate the risks of unintended escalation.

In this way, military exercises and simulations can present unique opportunities to strengthen operational resistance against accidental or inadvertent escalation and to identify methods for reestablishing operational deterrence should initial deterrence fail. By regularly practicing operational procedures, nuclear support forces maintain a high level of readiness and institutional proficiency, which reduces the risk of accidents caused by human error. Moreover, regular exercises provide an opportunity to safely stress test U.S.–NATO deterrence and operational and declaratory policies against difficult scenarios that reflect the realities of current geopolitical conditions. Measures to strengthen adaptability could be easily incorporated into such exercises by changing scenarios dynamically to reflect evolving global challenges. By thinking through these scenarios and practicing them in a controlled environment, U.S. and NATO military and political decision makers can better identify weaknesses in current nuclear policy and outline opportunities for restoring deterrence and managing nuclear escalation should it begin.

In planning and conducting any nuclear-related exercises, it is important that the United States and NATO carefully work to avoid inadvertently communicating an escalatory message. Beatrice Heuser, Tormod Heier, and Guillaume Lasconjarias note that military exercises, including nuclear exercises, are often an important method of political communication. However, their intended message may easily be misinterpreted by an opponent.107 Therefore, to avoid unintended messaging, it is important that the United States and NATO continually seek to improve their understanding of how Russia perceives U.S./NATO nuclear exercises. When carried out, nuclear-related exercises should adhere strictly to nonescalatory political aims and always be accompanied by clear communication and ongoing discussions between the United States/NATO and Russia. Moreover, as suggested by James A. Blackwell, careful planning of nuclear exercises to focus on broad and general nuclear training rather than [End Page 223] specific scenarios or specific messaging can also help to prevent or mitigate the negative effects of misinterpreted messaging.108

## Cyberwar Good

### 1nc – Cyberwar Good

#### Low-level attacks are stabilizing- no escalation

Yoo, 17—Emanuel S. Heller Professor of Law, University of California, Berkeley, School of Law (John, “Embracing the Machines: Rationalist War and New Weapons Technologies,” 105 Calif. L. Rev. 443 (2017), dml)

New weapons technologies can help overcome the obstacles of imperfect information. Coercive measures can signal political will, the value placed on the resources at stake, or military capabilities that could influence the outcome of a broader armed conflict. The more costly the signal, the more credible the information becomes. A nation's leader can make a threat of war and send military forces near disputed territory or a potential conflict zone. Deployment eats up resources that would go to waste if the nation is bluffing and incurs "audience costs" domestically if the leader backs down."' Escalating steps of force will provide the opportunity to send more precise signals that gradually consume more resources, reveal more military capability, and edge closer to war. With more avenues to credibly signal capabilities, there are more opportunities to reveal reliable, private information, and the likelihood of bluffing is reduced. While new weapons technology may produce more opportunities for violence, it can signal nations' capabilities and therey lead to peace settlements rather than war.

Limiting the ability to deploy new weapons technologies might make war more harmful. A ban could narrow the range of targets and the means of coercion to produce more destructive signaling and ultimately more lethal conflicts. One nation may want to send a signal during a crisis that inflicts a precise cost on its opponent. With a broader set of targets and more levels of harm, the nations can send more discrete signals in the bargaining process. If nations limit their signals to conventional attacks on military targets, they will have to employ more destructive levels of force. They might develop even more devastating kinetic weapons to produce the same effects as the precision offered by cyber or robotic weapons. Limits on new weapons technology might even destabilize crises by encouraging nations to use offensive weapons early in a crisis because they might themselves be vulnerable to attack. 15 4

New weapons technologies can more easily send specific signals that advance the bargaining process toward settlement. Cyberweapons, for example, can be used to shut down an opponent's financial markets or transportation and communication networks for a limited time. During the Kosovo War, the United States Air Force achieved a similar result by dropping graphite on Belgrade's electrical grid, which temporarily disabled power to Serbia's capital city. While NATO claimed that the disruption in electricity undermined Serbian military operations, the attack on the electricity grid also sought to pressure Serbian civilians against supporting the Milosevic regime.15 5 While such an attack would violate the ban on targeting civilian objects set out in the Additional Protocol I of 1977 to the Geneva Conventions, it can send a signal that may cause less loss of life and destruction than an attack on a hardened military target using kinetic weapons. Cyberweapons, in particular, present opportunities to send a more nuanced range of signals during interstate crises.' 5 6 Nations can use cyberweapons to attack each other's armed forces more precisely, and hence reduce direct casualties to both military personnel and civilians. In a contest over Taiwan, for example, China could use cyberattacks to disable communications between the Pentagon and the U.S. Seventh Fleet. These cyberattacks can inflict fewer, more directed costs than kinetic attacks. Cyberweapons' precision can reduce collateral harm to civilians by targeting only military communications. While cyberattacks can cause widespread harm, such as cutting water and electricity services to civilian populations, they still offer more precise and controlled power than kinetic weapons.

One might respond that some type of international regulation could forestall long-term harms from cyber conflict that might outweigh the benefits of credible signaling. Cyberweapons, for example, might also make possible new types of harms that did not previously appear in warfare, such as China's alleged theft of the U.S. personnel management database or North Korea's entry into Sony's network. Or cyberwarfare might open up a means for a faster escalation of hostilities. But even if true, these costs have to compare to existing means of signaling, which would depend on the use of conventional, kinetic weapons and their accompanying destruction and loss of life. They would also have to balance against the costs of cutting off a set of communications, which might impede peaceful bargaining.

Even if nations could overcome informational asymmetry, the international system's anarchy creates a second, more difficult, obstacle to cooperation. While nations may understand that avoiding war is mutually advantageous, they may not trust each other. The enforcement problem is acute in situations where a settlement changes the status quo between states, or where rapid changes are already affecting the balance of power."' One nation may find it difficult to trust the other to keep a promise if the latter will become even more powerful as a result of the agreement.

Information problems, for example, do not seem to explain the problems with ending internal armed conflict or long wars. Internal armed conflicts between a government and a rebel group often go on for years-sixteen years, on average.15 8 Over the course of the war, both sides acquire information about each other's goals, resources, and will. Even with far more information than at the war's outset, the parties often choose to fight rather than reach an agreement. This may well be due to lack of enforcement mechanisms. A settlement may put one of the two parties in a better position than when the fighting continues. A rebel group may gain breathing space where it can regroup, or the government may restore its authority in lost territory. One side cannot be confident that the other will not take advantage of its new position to break the agreement and take even more resources in the following year.

A hypothetical territorial agreement between the United States and China over Taiwan illustrates the difficulties of securing enforcement of a settlement amidst a shifting balance of power. In the first time period, the United States protects an independent iTaiwan. The United States has a greater probability of prevailing in any conflict with China because of its larger navy, air force, and forward bases in Korea, Japan, and the Philippines. In the second time period, China's economy has boomed, which translates into greater military power. China gains a higher probability of winning in a war with the United States. In this period, China and the United States agree to divide Taiwan in the middle because, with full information, they both estimate their chances of winning a war at fifty-fifty. China's gain of territory on Taiwan, however, gives it a greater than 50 percent chance of prevailing in the next time period because it now has a land base on the island itself. China's prospects will also improve in the third time period because of faster economic growth and military spending rates.

Under these conditions, the United States will have little confidence that China will keep its agreement in the second time period. An agreement will endow Beijing with an even greater advantage in future time periods, which will encourage it to revise the division of Taiwan further in its favor. China's conduct under its agreement with the United Kingdom over Hong Kong illustrates the problem. In December 1984, China achieved a superior military position relative to the United Kingdom in any conflict over Hong Kong. In 1982, for example, China spent $49.5 billion on defense whereas the United Kingdom spent $27.4 billion (they were the third and fourth largest spenders, respectively, with the Soviet Union first at $257 billion and the United States second at $196.3 billion). 59 But, much of the British military was deployed in Europe as part of NATO, and China's proximity to Hong Kong created a strategic advantage. To guarantee a peaceful transfer of power, Beijing promised in an agreement with London that Hong Kong would continue to enjoy an independent political system. Today, it appears that China is reneging on this negotiated agreement; the Communist Party has installed unpopular political leaders in Hong Kong to extend the mainland's power over the territory. In the twenty-first century, the United Kingdom has little military ability to prevent Beijing's revision of the deal. The 1984 handover agreement could not withstand a serious shift in the balance of power between China and the United Kingdom.

Cyberwarfare might provide an unexpected way to increase the ability of nations to commit to the terms of an agreement. In order to make a reliable agreement, a nation has to be willing to suffer a serious loss if it fails to perform, much like a borrower putting up property as collateral for a loan. But nations may have difficulty offering territory or resources as a security deposit on their treaty promises. A nation, however, could leave some valuable resource deliberately vulnerable to attack by cyberassault from its treaty partner. It could ensure that the cyber defense of the resource could only be overcome by capabilities in the hands of the other nation. If one state violated its international agreement, the other state could use cyber weapons to destroy the resource. This would be the twenty-first century equivalent of the ancient and medieval practice of sending the children of aristocratic families to foreign nations to serve as hostages, or the more recent concept of mutually assured destruction during the Cold War. Due to the lack of enforcement, however, states could never be certain that a nation would not renege even on these guarantees-a nation could always remove the vulnerabilities or suddenly deploy new defenses. But these expensive signals of commitment could improve the ability to cooperate beyond matters as they stand now.

A critic might argue that without international regulation of these new technologies, the risk to civilians will increase. Nations at war, however, will have an incentive to distinguish between military and civilian targets to the extent allowed by the capabilities of weapon systems. Rational nations should seek to contain the harms of war in order to maintain the conditions for peace and to preserve the value of the civilian economy in the postwar period. 160 Defenders in a war do not want to kill their fellow citizens or harm their own territory, although they might destroy civilian property to prevent it from falling into enemy hands. Invaders will have no interest in ruining the object of their aggression. Reducing civilian casualties may also encourage an end to conflict. Targeting civilians and destroying nonmilitary resources may harden nations at war and make a diplomatic compromise more difficult. The unexpected carnage of World War I, for example, made a peace agreement restoring the status quo to pre-August 1914 politically impossible for both the Allied and Central Powers.

Nations, moreover, have long pursued indirect coercion against civilian populations in war. They have often turned to economic sanctions to conduct hostilities short of direct armed conflict, or in conjunction with active hostilities. In World Wars I and II, of course, the Allies conducted economic warfare against Germany and its allies by levying a blockade of both military and civilian shipping. 161 After the wars, the UN Charter even expressed a preference for such tactics by authorizing the Security Council to impose "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication" in the case of a threat to international peace and security.

While nations such as Great Britain and the United States have argued in the past that embargos blocked only goods that might contribute to the enemy military, this seems difficult to sustain in the case of the complete embargoes that prevailed during the World Wars. Instead, economic warfare serves the same objectives as the approach described here for cyber and robotic weapons. First, new cyber and robotic weapons provide nations with a way to send signals in international bargaining through the gradual escalation of coercion short of outright hostilities. Second, embargoes pressure civilian populations to change the policies of their leaders, or even the leaders themselves. Perhaps cyber and robotic weapons, when employed as steps in the escalation of force, will also be understood as more akin to economic than kinetic warfare.

A rationalist approach to war also provides an answer to the broader critique of the new weapons technologies as facilitating war. Recall that some UN officials and scholars share the concern that drones and cyberweapons will encourage states to wage war more often. Critics argue that these weapons remove a nation's soldiers from the battlefield, theteby emboldening leaders to choose force more frequently. But, understanding war as a bargaining failure reveals the importance of signaling to resolving international disputes. New weapons create more opportunities for signaling, which allows nations to communicate their intentions and capabilities more effectively. Greater signaling should allow nations to share more information, which on the margins will lead to more international deals and therefore an overall reduction of major wars. Ironically, an effort to ban new weapons may well produce more war, not less.

#### Chinese Turn – They’re dependence on cyberweapons gives the US an advantage because we’re better at shutting down their systems than they are at targeting ours. Having cyber options give them false confidence and decreases their emphasis on conventional capabilities.

Jon **Lindsay 15**, Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies., Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction.” International Security, vol. 39, no. 3, Jan. 2015, pp. 7–47.

the downside of “informatization” China’s ambition to become a world-class military power will lead the PLA to become more like the U.S. military in its dependence on networks and space assets. This modernization will undermine the asymmetry of vulnerability thought to make cyberweapons so dangerous to the United States and instead put some of the PLA’s own most sophisticated systems at risk. PLA antiaccess capabilities against U.S. power projection also include antiship ballistic missiles, cruise missile boats, antisatellite weapons, and ªfth-generation aircraft. The PLA requires traditional forces, moreover, for other missions that might require warªghting, military operations other than war, or coercive diplomacy (a role ill-suited for secret and intangible cyberweapons). China’s goal of “winning local wars under the conditions of informatization” requires the PLA to “enhance [its] warªghting capabilities based on information systems.”94 This transformation into a modern “informatized” force, inspired in no small part by American RMA ideals and force structure, entails greater reliance on C4ISR systems and computer networks. Yet China’s pursuit of the promise of the RMA will also reveal its liabilities. In imagining and planning for a potential war with the United States, the PLA has to worry about the demonstrated ability and willingness of the U.S. military to conduct cyber operations on the battleªeld (in Iraq and Afghanistan) and in covert action (e.g., the Stuxnet attack). If cyberwarfare is as effective as Chinese writers believe it is but they underestimate the costs of mastery, then the PLA is doubly disadvantaged. Chinese attacks can be expected to be less skillfully coordinated against more robust U.S. defenses, and vice versa. The United States already has, while China still struggles to develop, the institutional complements and experience required to plan and control cyber operations in synchrony with the larger battle. Meanwhile the fear of cyberwarfare has prompted considerable U.S. military investment in network protection, active cyber defense measures (e.g., counterintelligence deception and “hack back” counterattack), and exercises in cyber-degraded conditions. The vaunted asymmetry of cyberwarfare, usually posed as an advantage for the weaker power, in fact runs in the opposite direction, giving the stronger and more experienced force the advantage.95 If the military utility of cyber- warfare is actually more limited than Chinese doctrine writers seem to believe, then conventional considerations about military effectiveness (e.g., the balance of power as well as skill in combined arms warfare and joint operations) should be expected to dominate strategic calculation and operational interaction in any conºict.

### 2nc – Prevents Escalation

#### Provocative friction is good --- reduces escalation by demonstrating capability, and the capacity to escalate deters attackers from crossing red lines --- the aff undermines both dynamics

Jon **Lindsay and** Erik **Gartzke 14**, Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies, AND Erik Gartzke is Professor and Director of cPASS at the Department of Political Science @ UCSD, Lindsay, Jon R., and Erik Gartzke. “Coercion through Cyberspace: The Stability-Instability Paradox Revisited.” The Power to Hurt: Coercion in the Modern World, Oct. 2014.

1 Introduction Information technology is the nervous system of the global economy. Critical infrastructure for banking, power, transportation, and industry increasingly depends on embedded computers connected to the internet. Firms and citizens entrust vital personal, medical, and financial data to distant servers in return for more convenient and efficient services. Military command and control relies on digital networks to connect far-flung surveillance and strike systems and to project power rapidly and precisely. Yet this vital interconnectivity also facilitates new modes of crime, protest, espionage, and warfare. Ubiquitous computer networks both provide access to valuable targets and become targets themselves. Protecting and influencing cyber infrastructure has thus become a major priority for governments and other political actors around the world. The very ubiquity of information technology makes the danger of cyber threats easy to exaggerate. In contemporary defense policy discourse there are three influential narratives of mounting cyber peril. The most dangerous envisions the paralysis of industrial control systems of military command and control through surprise attack by anonymous hackers. This scenario is often described as a “digital Pearl Harbor” or a “cyber 9/11” depending on whether the imagined aggressor is a revisionist state like China or Iran or a non-state anarchist or terrorist empowered by the information revolution. A second narrative offers an alternative to the shock of sudden catastrophe by warning of the long term erosion of economic and military competitiveness. The relentless theft of vital secrets stored on corporate and government networks is thus thought to cause a prolonged “death by a thousand cuts.” In both of these scenarios, weaker states and terrorists gain increasing access to powerful hacking tools while technology-dependent advanced industrial states become increasingly vulnerable to cyber attack and exploitation. 1 A third category of threat narrative concerns the transformation of internet architecture to decisively benefit one political group at the expense of the other. At one extreme, the growth of flexible social media enables connected protesters to overwhelm and overthrow authoritarian regimes.2 At the other extreme governments censor and reconfigure the internet to undermine innovation and freedom. State paranoia about paralysis and erosion thus leads to digital lockout or “the end of the internet” as we know it.3 National security officials, the defense industry, and media pundits all have incentives to exaggerate the cyber threat.4 The secrecy of cyber operations further complicates assessment, even as states make major investments in cyber defense. Each of the three narratives above are indeed exaggerations, but they point toward more plausible scenarios using cyber operations as subtle complements to or even substitutes for more traditional forms of aggression. Understanding the dynamics, magnitude, and likelihood of aggression online requires greater attention to the operational requirements for staging various types of cyber operations, the strategic benefits actors hope to gain through them, and the risks of unintended consequences. Too often defenders of the cyber revolution focus narrowly on the technological possibility for harm but discount operational and institutional obstacles to effectiveness and ignore the strategic utility of cyber harm or threats of harm. 5 A realistic appraisal of cyber threats must take not only technological but also strategic logic into account. Thomas Schelling distinguishes brute force, which is needed in a contest of strength, from coercive threats, which are useful in a contest of resolve.6 Both require the power to inflict harm, but brute force exercises it while coercion holds (at least some of) it in reserve. Likewise, actors might use cyber operations to attempt to change the balance of power directly or they might use them to provide information about their intentions and commitment. To paraphrase Clausewitz, cyberwar is politics by other means. As a result of technical and political constraints, the coercive potential of cyberspace is more limited than generally appreciated, but it is not negligible, especially when exploited in conjunction with other forms power such as military force. In this chapter we lay out a typology of cyber operations, distinguishing the skills and resources needed to cause different types of harm. Not all cyber options are equally available to all actors because of varying requirements in organizational capacity, intelligence support, and risk sensitivity. For each of the exaggerated myths mentioned above, there are low-cost, low- payoff irritants widely available as well as higher-cost, potentially higher-payoff adjunct capabilities available to a more restricted set of predominantly nation-state actors. Next we evaluate the coercive utility of these various harms, or threats of these harms, by taking into consideration the interaction of cyberspace with other domains. Finally we ask, what types of cyber coercion are most likely? We argue that there exist two important bounds on the distribution of cyber harm. First, because voluntary connections to the internet make cyber harms possible in the first place, aggressors must be careful not to provoke their victims to disconnect. Second, the availability of military instruments beyond the cyber domain, creates potential for retaliation for unacceptable harms. These constraints combine to make small-scale cyber aggression relatively appealing and thus more likely while making large-scale aggression difficult and undesirable for initiators and thus less likely. The finding of this chapter extends the logic of the stability-instability paradox pioneered in the 1960s. While nuclear weapons can deter nuclear war, they can fail to deter, and even encourage, conventional or peripheral war. Mutually assured destruction restrained the superpowers from engaging in direct confrontations during the Cold War, even as this restraint encouraged and facilitated the exercise of proxy wars throughout the Third World. The mechanisms of restraint in the cyber domain are slightly different than in the nuclear world—the risk of voluntary disconnection and military retaliation vs. mutual Armageddon—but the results are similar: little truly dangerous behavior and a lot of provocative friction. The social and economic value of the internet expands the scope for minor aggression like espionage, covert influence, and symbolic protest. Cyber operations also act as valuable adjuncts for battlefield operations akin to signals intelligence and electronic warfare for states who are willing and able to go to war for other reasons. However, there are diminishing incentives to “go big” with cyber warfare alone given the incentives targets have to identify even a hard-to-identify attacker and shift domains to punish cyber aggression. Although the attribution of the attacker’s identity is widely thought to be hard problem in cyberspace, anonymity is never guaranteed and might not even be useful for some forms of coercion. A nonzero risk of attribution opens the door to retaliatory punishment, which encourages attackers to exercise restraint in cyber aggression. Ironically enough, the instability we perceive in cyberspace is indicative of the stability of deterrence of the most dangerous cyber threats.

#### Cold war empirics prove --- tactical instability creates strategic calm

Jon **Lindsay 15**, Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies., Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction.” International Security, vol. 39, no. 3, Jan. 2015, pp. 7–47.

Barring gross misperception, however, one can expect the risk of unwanted escalation from cyber to other military domains to deter both sides from resorting to more destructive forms of computer network attack in most situations. 113 Yet although nuclear or conventional deterrence might be able to check catastrophic cyberattack, it cannot credibly discourage minor cyber aggression such as nationalist hacktivism, industrial espionage, or harassment of dissident expatriates. Indeed, the observable pattern of Chinese (and American) cyber activity conforms to the logic of the Cold War stability-instability paradox, but in slightly revised form. In the original formulation of the paradox, mutual vulnerability to nuclear retaliation inhibits nuclear war but encourages conventional war in peripheral theaters where nuclear threats are not credible.114 Today, the intensity of cyber aggression is bounded by the risk of any form of military retaliation as well as the need to preserve interconnection and protect sources and methods that rely on deception. Cyberattackers intentionally keep the costs they inflict below the assessed threshold of even limited military retaliation by opponents, occupying a region where military threats of punishment would be utterly noncredible. The aggressor’s freedom of action is further constrained by the need to maintain stealth and plausible deniability for ongoing operations. Actors that are deterred by threats of military punishment, on the one hand, and threats of counterintelligence detection or loss of connection, on the other, are encouraged to find more limited ways to inflict costs. The complexity of modern computer network infrastructure, in particular, offers many inexpensive ways to inflict minor costs. One implication is that cyberspace creates more scope for nontraditional security concerns (e.g., harassment of human rights organizations and vulnerable user communities) that powerful actors usually ignore in their focus on protecting high-value economic and military assets.115 As long as dense interconnection and economic interdependence remain mutually beneficial for powers such as the United States and China, they will be able to tolerate the irritants that they will inevitably inflict on one another. The modern intelligence-counterintelligence contest plays out in a complicated sociotechnical space where states take advantage of economic cooperation and hedge against security competition. If their broader mutual interest frays, however, then cyberwarfare becomes just one facet of a more serious strategic problem involving more dangerous means. Exaggeration of the cyber threat feeds spirals of mistrust, which make this undesirable outcome slightly more likely. The United States and China should discuss the interaction of cybersecurity and traditional military force in depth and take steps to limit misunderstandings about the other’s intentions. They might even learn to interpret chronic cyber friction as a sign that more truly dangerous threats have been constrained. Contrary to conventional wisdom, the emergence of complex cyber threats may be a positive development in the tragic history of international politics: the bad news about cybersecurity is good news for global security.

### 2nc – Reduces War

#### Cyberwar reduces physical war

Thomas **Rid 13**, THOMAS RID is a Reader in War Studies at King’s College London, 12-1-2013, "Cyberwar and Peace," Foreign Affairs, https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace

Cyberwar Is Coming!” declared the title of a seminal 1993 article by the RAND Corporation analysts John Arquilla and David Ronfeldt, who argued that the nascent Internet would fundamentally transform warfare. The idea seemed fanciful at the time, and it took more than a decade for members of the U.S. national security establishment to catch on. But once they did, a chorus of voices resounded in the mass media, proclaiming the dawn of the era of cyberwar and warning of its terrifying potential. In February 2011, then CIA Director Leon Panetta warned Congress that “the next Pearl Harbor could very well be a cyberattack.” And in late 2012, Mike McConnell, who had served as director of national intelligence under President George W. Bush, warned darkly that the United States could not “wait for the cyber equivalent of the collapse of the World Trade Centers.” Yet the hype about everything “cyber” has obscured three basic truths: cyberwar has never happened in the past, it is not occurring in the present, and it is highly unlikely that it will disturb the future. Indeed, rather than heralding a new era of violent conflict, so far the cyber-era has been defined by the opposite trend: a computer-enabled assault on political violence. Cyberattacks diminish rather than accentuate political violence by making it easier for states, groups, and individuals to engage in two kinds of aggression that do not rise to the level of war: sabotage and espionage. Weaponized computer code and computer-based sabotage operations make it possible to carry out highly targeted attacks on an adversary’s technical systems without directly and physically harming human operators and managers. Computer-assisted attacks make it possible to steal data without placing operatives in dangerous environments, thus reducing the level of personal and political risk. These developments represent important changes in the nature of political violence, but they also highlight limitations inherent in cyberweapons that greatly curtail the utility of cyberattacks. Those limitations seem to make it difficult to use cyberweapons for anything other than one-off, hard-to-repeat sabotage operations of questionable strategic value that might even prove counterproductive. And cyber-espionage often requires improving traditional spycraft techniques and relying even more heavily on human intelligence. Taken together, these factors call into question the very idea that computer-assisted attacks will usher in a profoundly new era. THE THIN CASE FOR CYBERWAR One reason discussions about cyberwar have become disconnected from reality is that many commentators fail to grapple with a basic question: What counts as warfare? Carl von Clausewitz, the nineteenth-century Prussian military theorist, still offers the most concise answer to that question. Clausewitz identified three main criteria that any aggressive or defensive action must meet in order to qualify as an act of war. First, and most simply, all acts of war are violent or potentially violent. Second, an act of war is always instrumental: physical violence or the threat of force is a means to compel the enemy to accept the attacker’s will. Finally, to qualify as an act of war, an attack must have some kind of political goal or intention. For that reason, acts of war must be attributable to one side at some point during a confrontation. No known cyberattack has met all three of those criteria; indeed, very few have met even one. Consider three incidents that today’s Cassandras frequently point to as evidence that warfare has entered a new era. The first of these, a massive pipeline explosion in the Soviet Union in June 1982, would count as the most violent cyberattack to date -- if it actually happened. According to a 2004 book by Thomas Reed, who was serving as a staffer on the U.S. National Security Council at the time of the alleged incident, a covert U.S. operation used rigged software to engineer a massive explosion in the Urengoy-Surgut-Chelyabinsk pipeline, which connected Siberian natural gas fields to Europe. Reed claims that the CIA managed to insert malicious code into the software that controlled the pipeline’s pumps and valves. The rigged valves supposedly resulted in an explosion that, according to Reed, the U.S. Air Force rated at three kilotons, equivalent to the force of a small nuclear device. But aside from Reed’s account, there is hardly any evidence to prove that any such thing happened, and plenty of reasons to doubt that it did. After Reed published his book, Vasily Pchelintsev, who was reportedly the KGB head of the region when the explosion was supposed to have taken place, denied the story. He surmised that Reed might have been referring to a harmless explosion that happened not in June but on a warm April day that year, caused by pipes shifting in the thawing ground of the tundra. Moreover, no Soviet media reports from 1982 confirm that Reed’s explosion took place, although the Soviet media regularly reported on accidents and pipeline explosions at the time. What’s more, given the technologies available to the United States at that time, it would have been very difficult to hide malicious software of the kind Reed describes from its Soviet users. Another incident often related by promoters of the concept of cyberwar occurred in Estonia in 2007. After Estonian authorities decided to move a Soviet-era memorial to Russian soldiers who died in World War II from the center of Tallinn to the city’s outskirts, outraged Russian-speaking Estonians launched violent riots that threatened to paralyze the city. The riots were accompanied by cyber-assaults, which began as crude disruptions but became more sophisticated after a few days, culminating in a “denial of service” attack. Hackers hijacked up to 85,000 computers and used them to overwhelm 58 Estonian websites, including that of the country’s largest bank, which the attacks rendered useless for a few hours. Estonia’s defense minister and the country’s top diplomat pointed their fingers at the Kremlin, but they were unable to muster any evidence. For its part, the Russian government denied any involvement. In the wake of the incident, Estonia’s prime minister, Andrus Ansip, likened the attack to an act of war. “What’s the difference between a blockade of harbors or airports of sovereign states and the blockade of government institutions and newspaper websites?” he asked. It was a rhetorical question, but the answer is important: unlike a naval blockade, the disruption of websites is not violent -- indeed, not even potentially violent. The choice of targets also seemed unconnected to the presumed tactical objective of forcing the government to reverse its decision on the memorial. And unlike a naval blockade, the attacks remained anonymous, without political backing, and thus unattributable. A year later, a third major event entered the cyber-Cassandras’ repertoire. In August 2008, the Georgian army attacked separatists in the province of South Ossetia. Russia backed the separatists and responded militarily. The prior month, in what might have been the first time that an independent cyberattack was launched in coordination with a conventional military operation, unknown attackers had begun a campaign of cyber-sabotage, defacing prominent Georgian websites, including those of the country’s national bank and the Ministry of Foreign Affairs, and launching denial-of-service attacks against the websites of Georgia’s parliament, its largest commercial bank, and Georgian news outlets. The Georgian government blamed the Kremlin, just as the Estonians had done. But Russia again denied sponsoring the attacks, and a NATO investigation later found “no conclusive proof” of who had carried them out. The attack set off increasingly familiar alarm bells within American media and the U.S. national security establishment. “The July attack may have been a dress rehearsal for an all-out cyberwar,” an article in The New York Times declared. Richard Clarke, a former White House cybersecurity czar, warned that the worst was yet to come: the Georgian attack did not “begin to reveal what the Russian military and intelligence agencies could do if they were truly on the attack in cyberspace.” Yet the actual effects of these nonviolent events were quite mild. The main damage they caused was to the Georgian government’s ability to communicate internationally, thus preventing it from getting out its message at a critical moment. But even if the attackers intended this effect, it proved short-lived: within four days after military confrontations had begun in earnest, the Georgian Foreign Ministry had set up an account on Google’s blog-hosting service. This move helped the government keep open a channel to the public and the news media. What the Internet took away, the Internet returned. ISTOCK.COM / -ANTONIO- Overblown: keyboard as grenade. IN CODE WE TRUST? Perhaps the strongest evidence presented by advocates of the concept of cyberwar is the Stuxnet operation launched against Iran by the United States and Israel. Stuxnet, part of a set of attacks known as Operation Olympic Games, was a sophisticated multiyear campaign to sabotage Iran’s nuclear enrichment facility in Natanz by inserting a harmful computer worm into the software that ran the facility’s centrifuges, causing them to overload. American and Israeli developers started designing the project as early as 2005, and it launched in 2007, growing more sophisticated until its discovery in 2010. The attack was groundbreaking in several ways. The developers built highly target-specific intelligence into the code, enabling the Stuxnet software to make autonomous decisions in its target environment. Most important, Stuxnet represented the first and only physically destructive cyberattack launched by one state (or, in this case, two states) against another. Yet even cyberattacks that cause damage do so only indirectly. As an agent of violence, computer code faces a very basic limit: it does not have its own force or energy. Instead, any cyberattack with the goal of material destruction or harming human life must utilize the force or energy embedded in its target: for example, shutting down an air traffic control system and causing trains or planes to crash or disrupting a power plant and sparking an explosion. Yet besides Stuxnet, there is no proof that anyone has ever successfully launched a major attack of this sort. Lethal cyberattacks, while certainly possible, remain the stuff of fiction: none has ever killed or even injured a single human being. Thanks to its lack of direct physical impact, code-induced violence also has less emotional impact. It would be difficult for a cyberattack to produce the level of fear that coordinated campaigns of terrorism or conventional military operations produce. Owing to their invisibility, cyberweapons also lack the symbolic power of traditional ones. Displays of weaponry, such as the elaborate military parades put on by China and North Korea, sometimes represent nothing more than nationalist pageantry. But revealing one’s arsenal can also serve tactical and strategic ends, as when countries deploy aircraft carriers to demonstrate their readiness to use force or carry out operations designed to intimidate the enemy, such as using military aircraft to conduct deliberately low flyovers. Indeed, displaying weapons systems and threatening to use them can prove more cost-efficient than their actual use. But cyberweapons are hard to brandish. Perhaps the most crucial limitation of violence in cyberspace is its almost entirely destructive quality: unlike traditional political violence, which can maintain trust in institutions and states as well as undermine it, violence in cyberspace can do only the latter. Any established political order comes with a certain degree of inherent violence; consolidated states, after all, survive only if they maintain monopolies on the legitimate use of force. By encouraging trust in the ability of state institutions to protect property and safeguard citizens, this inherent violence buttresses a state’s power and allows the state to establish the rule of law. But cyber-violence lacks this ability, since it does little or nothing to build up trust in institutions; indeed, it is very difficult to imagine how cyberattacks could be used to enforce rules or laws, either domestically or internationally. Digital surveillance presents a more complicated picture. In democracies, intelligence agencies tread a thin line between providing security and eroding public trust in the state, as demonstrated by the recent controversy over the U.S. National Security Agency’s data-collection practices. In authoritarian countries, digital surveillance can assist the state’s coercive use of force, but it cannot replace it. Such limitations, however, should not lead anyone to dismiss the corrosive potential of cyberattacks. Indeed, such assaults can undermine social trust in a more direct way than traditional political violence. Cyberattacks are more precise; they do not necessarily undermine the state’s monopoly of force in a wholesale fashion. Instead, they can be tailored to attack specific companies or public-sector organizations and used to undermine those groups’ authority selectively. Stuxnet provides a good example of this dynamic. Putting aside the question of whether the attack was an act of war, its primary intention was to undermine the trust of the Iranian scientists in their systems and in themselves and the trust of the Iranian regime in its ability to build nuclear weapons. The original intention was to cause physical damage to as many Iranian centrifuges as possible. But the American and Israeli attackers knew that the physical effect could be exploited to unleash a much more damaging psychological effect. “The intent was that the failures should make them feel they were stupid, which is what happened,” an American participant told The New York Times. The Americans and the Israelis hoped that once a few machines failed, the Iranian engineers would shut down more machines because they distrusted their own technology or indeed their own skills. At the headquarters of the International Atomic Energy Agency, in Vienna, rumors circulated that the Iranians had lost so much confidence in their own systems and instruments that the management of the Natanz facility took the extraordinary step of assigning engineers to sit in the plant and radio back what they saw to confirm the instrument readings. “They overreacted,” one of the attackers revealed to David Sanger of The New York Times, “and that delayed them even more.” The Iranians also began to assign blame internally, pointing fingers at one another and even firing some personnel. DIGITAL UNDERGROUND Damaging though it may have been, Stuxnet, along with the cyber-scuffles in Estonia and Georgia, represents not a new form of warfare but something more akin to other, less lethal forms of aggression: sabotage and espionage. Unlike acts of war, these political crimes, which are often committed by nonstate actors, need not be violent to work. And although saboteurs and spies do act politically, they often seek to avoid attribution, unlike those who launch acts of war. For those reasons, the cyber-era has been a boon for political crime. Consider sabotage. Before the computer age, saboteurs had trouble calibrating and controlling the effects of their actions. Sabotage had to target physical property and relied on physical violence, which often proves unpredictable. During postal and railway strikes in France in 1909 and 1910, for instance, saboteurs cut signal wires and tore down telegraph posts. Destroying property risked running afoul of public opinion, and the tactic ultimately divided the workers. The strikes themselves, as a form of sabotage, also ran the risk of leading to unpredictable violence: indeed, labor demonstrations often intensified into riots, making it easier for opponents to portray the strikers as uncompromising radicals. It is much easier for saboteurs to avoid counterproductive side effects in the age of computer-assisted attacks, which can contain violence and generally avoid it altogether. Cyberattacks can maliciously affect software and business processes without interfering with physical industrial processes, remaining nonviolent but sometimes still causing greater damage than a traditional assault. A 2012 attack against the computer network of the oil company Saudi Aramco illustrates this potential. The attack physically harmed neither hardware nor humans. Yet by allegedly erasing the hard disks of some 30,000 computers, the attackers likely did much more monetary damage to Saudi Aramco than they could have through an act of traditional sabotage against machinery in one of the company’s plants. The oil giant reportedly had to hire six specialized computer security firms to help with its forensic investigation and post-attack cleanup. Despite such potential, it is also important to remember the inherent limitations of computer-assisted political crime and to note that human agents remain critical in the age of digital violence. Even Stuxnet, the most successful example of cyber-sabotage, demonstrates this fact. For the United States and Israel, the “holy grail,” in the words of one of the attack’s architects, was getting a piece of malicious software into the control system at Natanz. The Americans and Israelis needed fine-grained data from inside the Iranian plant to develop their weaponized code. The problem was that the control system was protected by an air gap: it was not connected to the Internet or even internal networks. As a result, the attackers had to deliver the malicious code via a removable hard drive such as a USB flash drive -- delivered by a human hand. To make this happen, U.S. intelligence operatives first obtained a list of the people who were visiting the targeted plant to work on its computer equipment and who could carry the payload there. “We had to find an unwitting person on the Iranian side of the house who could jump the gap,” one planner later told Sanger. The list of possible carriers included engineers from the German company Siemens, who were helping their Iranian colleagues maintain the control system -- work that required the Siemens engineers to bring portable computers into the plant. Precisely how the U.S.-Israeli team managed to exploit this vulnerability remains unknown. Suffice it to say that although “Siemens had no idea they were a carrier,” in the words of one U.S. official quoted by Sanger, “it turns out there is always an idiot around who doesn’t think much about the thumb drive in their hand.” SAFETY IN ONES AND ZEROS If cyberattacks reduce the amount of violence inherent in conflict, and if they often take the form of sabotage or espionage, then many officials and commentators who have been warning about the dawn of cyberwar have been ringing false alarms. Digital violence does have implications for ethics and for national security strategy, however. Weaponized code, or cyberattacks more generally, can achieve goals that used to require conventional force. The most sophisticated cyberattacks are highly targeted, and cyberweapons are unlikely to cause collateral damage in the same way conventional weapons do. Therefore, in many situations, the use of computers would be ethically preferable to the use of conventional weapons: a cyberattack might be less violent, less traumatizing, and more limited.

#### Cyber-attacks are good---key to enhanced precision in crisis bargaining.

Rabkin, 17 — \*Jeremy A. Rabkin; PhD, Harvard University; Professor of Law at the Antonin Scalia Law School, George Mason University. Professor Rabkin serves on the Board of Directors of the U.S. Institute of Peace (originally appointed by President George W. Bush in 2007, then appointed for a second term by President Barack Obama and reconfirmed by the Senate in 2011). He also serves on the Board of Academic Advisers of the American Enterprise Institute and on the Board of Directors of the Center for Individual Rights, a public interest law firm based in Washington, D.C. \*\*John Yoo; Emanuel Heller Professor of Law and director of the Korea Law Center, the California Constitution Center, and the Law School’s Program in Public Law and Policy. (2017; “Striking Power: How Cyber, Robots, and Space Weapons Change the Rules for War;” Ch. 1—We Must Think Anew; //GrRv)

Instead, we question the idea that nations should look to formal treaties and **rules** to produce **lasting limits on war**. Despite the recent deterioration in the Syrian civil war, nation-states have generally **refrained** from the use of **chemical weapons** against each other since the end of World War I. They have followed the Geneva Conventions on prisoners of war, though not consistently. Nations have observed other **norms** in the breach, chief among them the immunity of the civilian population and resources from attack. World War Il not only saw the aerial bombing of cities and the nuclear attacks on Japan, but the years since have seen precision targeting of terrorists off the battlefield, attacks on urban infrastructure, and the acceptance of high levels of collateral damage among civilians. International lawyers and diplomats may proclaim that nations follow universal rules, either because of morality or a sense of legal obligation, but the record of practice tells a far different story. Efforts to impose more **specific** and **demanding rules**, such as **limiting** targeted drone attacks, banning **cyber attacks**, or requiring human control of robotic weapons, will similarly fail because they cannot take into account **unforeseen circumstances**, new **weapons** and **military situations**, and the immediate **exigencies** of war. Just as new technology led to increases in economic productivity, so too has it allowed nations to make war more effectively. Nations will readily **adhere** to humanitarian standards when they gain a **benefit** that **outweighs the cost**, as when protecting enemy prisoners of war secures reciprocal protection for a nation's own soldiers taken captive by the enemy. Limitations on the use of weapons will follow a **similar logic**. Nations will be most inclined to respect legal restraints on new weapons when their use by both sides would leave no one better off or would provide little advantage. **Cyber** and robotic **weapons** do not bear the same features as the weapons where legal bans have **succeeded**, as with use of poison gas on the battlefield. **Cyber** and robotic **weapons** need not inflict unnecessary suffering out **of proportion** to their military advantages, as do poisoned bullets or blinding lasers. Rather, these weapons improve the **precision of force** and thereby **reduce human death** and **destruction** in war. **Nor** have these new weapons technologies yet sparked a **useless arms race**. Nuclear weapons eventually became opportune for arms control because larger stockpiles provided marginal, if any, benefits due to the destructive potential of each weapon and the deterrence provided by even a modest arsenal. Mutual reductions could leave both sides in the same position as they were before the agreement. Today, the marginal cost of nuclear weapons for the U.S. and Russia so outweighs their marginal benefit that it is not even clear that a binding international agreement is needed to reduce their arsenals. Russia, for example, reduced its arsenal below New START's ceilings of 1,550 nuclear warheads and 700 strategic launchers even before the U.S. approved the deal. 45 The United States likely would have reduced its forces to those levels even if the Senate had refused to consent to the treaty, a position the executive branch also took in 2002 with the Treaty of Moscow's deep reduction in nuclear weapons. Today's new weapons do not yet bear these characteristics. The **marginal gains** in deploying these weapons will likely be asymmetric across nations insofar as some nations will experience **much greater gains** in **military capability** by developing **cyber** and drone **technology**. Put differently, **prohibition** or **regulation** of these new weapons will not have **equal impacts on rival nations**. Indeed, we do not even now have enough information to understand which nations will benefit and which will not, which makes any form of international ban even less likely.

### 2nc – China Turn

#### We should make China as dependent on cyber as possible. They can’t punish us for it --- they haven’t practiced, hacking the US military is harder than it seems, and China’s bad at it

Jon **Lindsay 15**, Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies., Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction.” International Security, vol. 39, no. 3, Jan. 2015, pp. 7–47.

Military Threats of Cyberwarfare Just as the social context of exploitation and adversary counteraction combine to blunt the potential of cyber espionage, similar challenges in operational weaponization and strategic interaction constrain the potency of more disruptive cyber threats. Yet conventional wisdom holds that a multitude of technical factors favor offense over defense in cyberspace and that the difªculty of attribution undermines the credibility of deterrence; therefore, weaker actors can attack the control systems of superior adversaries to achieve levels of physical disruption possible previously only through kinetic bombing. As President Obama writes in a Wall Street Journal opinion article, “Computer systems in critical sectors of our economy—including the nuclear and chemical industries—are being increasingly targeted. . . . In a future conºict, an adversary unable to match our military supremacy on the battleªeld might seek to exploit our computer vulnerabilities here at home. Taking down vital banking systems could trigger a ªnancial crisis. The lack of clean water or functioning hospitals could spark a public health emergency. And as we’ve seen in past blackouts, the loss of electricity can bring businesses, cities and entire regions to a standstill.”74 A number of former U.S. government ofªcials have even likened the advent of cyberweapons to a new atomic age and have wondered why a catastrophic cyberattack has not yet occurred.75 Chinese military doctrine similarly envisions cyberwarfare to be a low-cost, long-range, highly effective counter to a superior adversary.76 There are reasons, however, to doubt the PLA’s ability to implement these ideas or to defend itself against cyberattacks launched by a superior adversary. chinese cyber doctrine The aggressive tenor of Chinese writings on cyberwarfare and the copious APT activity described above are the major sources of evidence that Western analysts usually offer to characterize the Chinese cyberwarfare threat. Ofªcial Chinese military doctrine and sources in Chinese military professional literature consistently describe cyberwarfare as a revolutionary development in military affairs. Senior Col. Ye Zheng, author of books published by the Chinese Academy of Military Science entitled On Informationalized Warfare and Information Warfare Course, writes, “Although the main melody of the times—peace and development—is still playing strongly, the dark spirit of network warfare is lurking in the sky above humanity.” This rhetorical construction implies that the cyber revolution undermines Deng Xiaoping’s diagnosis of the largely stable nature of the international environment. Ye singles out the United States for experimenting with cyberweapons such as Stuxnet (used in the attack on Iranian enrichment infrastructure) and hints at the prospect of more to come: “[J]ust as nuclear war was the strategic warfare of the industrial age, network warfare will be the strategic warfare of the information age. It has already become a ‘top level’ form of operation that is highly destructive and relates to national security and survival.”77 He further describes cyberwarfare as an integral force multiplier as well as an instrument for achieving more strategic effects such as paralyzing another state’s economy or exerting psychological inºuence on entire populations. Similarly, an author in the PLA’s Science of Information Operations writes that cyber strikes “can seek to achieve partial or large-scale paralysis of enemy systems. As soon as a virus enters the enemy’s command and control system, it will have tremendous destructive impact. . . . Therefore computer network war is an important means for paralyzing the enemy in wars of the future.”78 The PLA recognizes the existence of an “information domain” (xinxi lingyu), although as with “information security” it encompasses a wider range of subcategories to include computer network and electronic warfare as well as psychological and intelligence operations.79 Information operations are con-sidered so vital for the limited high-technology wars the PLA envisions ªghting that information supremacy is thought to be a precondition for gaining military supremacy anywhere else. The PLA’s general strategic principle of “active defense” stresses offensive operations to seize the initiative. The authoritative Science of Campaigns thus states that the beginning of a network war will determine its outcome: “Whoever strikes ªrst prevails.”80 PLA strategists assert that the vital targets of an advanced technology adversary are its information systems, and by attacking them covertly from beyond the range of enemy weapon systems it is possible to cause paralysis of the enemy’s organization, strategic decisionmaking, and national economy. As an important article by Gen. Dai Qingmin on the concept of “integrated network-electronic warfare” points out, “Information operations in high-tech warfare are, to a very great extent, a struggle which revolves around the destruction and the protection of C4ISR systems.”81 Chinese writers argue that a relatively weaker PLA can achieve information superiority against a stronger military only as long as it is able to launch paralyzing strikes at the beginning of a conºict. The Chinese perspective on using information technology to improve awareness, synchronization, and precision is inspired by 1990s-era American writings about the “revolution in military affairs [RMA].”82 RMA ideas were themselves inspired by Soviet strategists, and the common Marxist-Leninist belief that “technology determines tactics” surely inºuences PLA thought.83 Yet the most recent and relevant inspiration comes from Chinese study of U.S. operations in Iraq and the Balkans and analysis of the U.S. military’s heavy dependence on communication and logistics networks.84 In particular, the accidental U.S. bombing of the Chinese embassy in Belgrade prompted President Jiang Zemin to direct the PLA to develop so-called assassin’s mace (shashoujian) weapons to solve the problems of “seeing far, striking far, and striking accurately.” Jiang reasoned that “what the enemy is most fearful of is what we should be developing.”85 As the consummately “network centric” U.S. military leverages data links to reduce its force size—substituting information for mass in the RMAformula for success—those links become vulnerabilities and thus tempting targets for the PLA. Insofar as the cyber revolution thesis is inºuential in U.S. strategic planning, moreover, the specter of PLA cyberwarfare may indeed have some success in creating fear and encouraging restraint in U.S. planning. Remarkably, however, there appears to be little mention in Chinese writings of the considerable controversy over the RMA in Western strategic literature or considerations of the downsides of the RMA.86 The United States has fought several regional wars in recent decades and in the process has experienced no small amount of confusion and the “fog of war” as computer systems break down unexpectedly, adversaries refuse to conform to the assumptions of network-centric doctrine, and service members resort to ad hoc improvisations to muddle through. The PLA, by contrast, has not had the opportunity to test its ideas of “integrated network electronic warfare” in combat, and realistic command and control training is notoriously hard to achieve absent interaction with a real enemy and complex environment. The following review of Chinese cyber capabilities suggests that similar skepticism is also warranted for Chinese cyberwarfare. chinese cyber capabilities Although Chinese writers emphasize the revolutionary potential of cyberwarfare, episodes of Chinese aggression in cyberspace have been more mundane. China’s “hacker wars” ºare up during episodes of tension in Chinese foreign relations, as between Taiwan and the mainland between 1996 and 2004 in the wake of Taiwanese elections, between the United States and China following the 1999 bombing of the Chinese embassy in Belgrade and the 2001 EP-3 spy plane collision, and between China and Japan throughout the past decade during controversies involving the Yasukuni Shrine and the Senkaku/ Diaoyu Islands.87 Nationalist hackers (as distinguished from PLA units) deface foreign websites and launch temporary distributed denial of service attacks. Nationalist online outbursts may take place with the tacit consent or encouragement of the Chinese government, yet patriotic “hacktivism” is essentially just another form of symbolic protest. There has been speculation that PLA “cyber militias” associated with Chinese universities maintain a more potent reserve capability, but one study of open sources suggests that they are oriented toward more mundane educational and network defense activities.88 The majority of known PLA cyber operations are CNE for intelligence rather than computer network attacks to cause disruption.89 Nevertheless, many analysts worry that CNE is “only a keystroke away” from CNA, thereby generating dangerous ambiguity between intelligence gathering and offensive operations. Intrusion techniques developed for industrial espionage might be used to plant more dangerous payload code into sensitive controllers or constitute reconnaissance for future assaults. Chinese probing of critical infrastructure such as the U.S. power grid is aggressive, to be sure, so a latent potential for the PLA to convert CNE into CNA cannot be discounted.90 The discovery of access vectors and exploitable vulnerabilities, however, is only the first step to achieving effective reconnaissance of a target, and effective reconnaissance is just one step toward planning and controlling a physically disruptive attack. The most signiªcant historical case of kinetic CNA to date, the Stuxnet attack on Iran’s enrichment infrastructure, suggests that painstaking planning, careful rehearsals, and sophisticated intelligence are required to control a co- vert disruption.91 The U.S. military also considered using cyberattacks to take down Libya’s air defense system in 2011, but reportedly it would have taken too long to develop the option.92 The latency between CNE and CNA is more complicated than generally assumed.

#### Seriously, they’re totally uncoordinated and terrible

Jon **Lindsay 15**, Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies., Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction.” International Security, vol. 39, no. 3, Jan. 2015, pp. 7–47.

china’s fragmented cyber defenses The CCP’s obsession with political “information security” has so far not translated into effective technical “network security.”34 Cybercrime thrives amid a fragmented bureaucracy. Lax and uneven law enforcement emboldens Chinese cybercriminals to prey on domestic targets and creates a blatantly open online underground economy in China. Chinese cybercriminals target Chinese victims given the relatively low risk of domestic police action; by comparison, Eastern Europe cybercriminals tend to avoid hacking at home, instead focusing their predation abroad. Stolen usernames and passwords, ªnancial data, video game accounts, and hacker tools can be bought and sold openly on Chinese social media forums such as Baidu and Tencent QQ. By one estimate, cybercrime damage to the economy exceeded $830 million and affected more than 20 percent of users and websites in 2011 alone.35 Rampant cybercrime is a result, in part, of China’s below-average cyber defenses.36 Importantly, networks exposed to criminal predation are also vulnerable to foreign exploitation, because state intelligence services use some of the same technology and methods. Cyber policy coordination among defense, law enforcement, and regulatory agencies is a challenge in any state, but China’s lack of governmental transparency makes a hard problem worse. Prior to 2014, primary responsibility for cybersecurity policy resided in a subcommittee of the CCP State Informatization Leading Group (SILG), formed in 2001 to guide national information technology development or “informatization” (xinxihua) and chaired by the CCP premier. SILG’s early focus on cybersecurity was eclipsed by the Chinese elite’s preoccupation with the 2008 Beijing Olympics and ªnancial crisis, leaving regulatory agencies and newly funded companies to their own devices. SILG updated its guidance criteria in 2012 to reºect renewed concerns about critical infrastructure and privacy, but elite focus remained sporadic. In February 2014, amid tension stemming from the Snowden leaks, the CCP announced the creation of the Cybersecurity and Informatization Leading Group (CILG), chaired by Xi Jinping (with twenty-one other Politburo or ministeriallevel ofªcials on the roster).37 The CILG aids Xi’s efforts to tighten Party discipline and respond to foreign cyber threats.38 Greater attention by China’s elite via CILG may improve cyber policy coordination, but prior experience does not bode well. In China, as in other states, a large and diverse set of public and private entities has a stake in the making of cyber policy, yet the steady stream of cyber friction does not add up to sustained elite pressure for reform. Policy elites with more pressing priorities usually do not focus consistent pressure on a heterogeneous set of bureaucratic interests.39 Numerous agencies under the State Council are responsible for the implementation of policy and the regulation of information technology in China. The People’s Liberation Army, subordinate to the CCP rather than the state, has considerable military and intelligence cyber capacity as well as civilian regulatory responsibility (e.g., in the transportation sector). Provincial governments, furthermore, enjoy substantial de facto autonomy and compete ªercely for patronage. In response to a glut of funding for SILG initiatives, expenditure in China’s information security industry grew from $527 million in 2003 to $2.8 billion in 2011. In the assessment of one industry observer, however, this expansion was marred by a “lack of overall planning,” “decentralization of decisionmaking power,” and a “lack of adequate communication.”40 As in other areas of Chinese policy, the implementation of cybersecurity is disjointed functionally and regionally, rife with rent seeking by bureaucratic agencies and enterprises. Haphazard interagency cooperation and industrial regulation create a permissive environment for cybercrime, which saps the potential of e-commerce and user trust in online services.

## OCOs Turn

### 1nc – OCOs Bad

#### Increasing OCO use risks ally provocation and escalation.

Jeffrey Caton 16, President of Kepler Strategies LLC, Carlisle, Pennsylvania, a veteran-owned small business specializing in national security, cyberspace theory, and aerospace technology. He is also an Intermittent Professor of Program Management with the Defense Acquisition University. NATO CYBERSPACE CAPABILITY: A STRATEGIC AND OPERATIONAL EVOLUTION Jeffrey L. Caton June 2016 Offensive Cyberspace. https://publications.armywarcollege.edu/pubs/2390.pdf

A significant “elephant in the room” issue for NATO cyberspace operations is the possibility of any use of offensive cyber by the Alliance. Cyber expert James Lewis poses this challenge as: “The central question for NATO’s cyber doctrine is how the lack of an articulated offensive cyber capability affects its ability to deter or defend.”115 In general, offensive cyberspace operations may be considered as the use of cyber capabilities outside of the defensive firewall of the NATO network. Such operations could be conducted in support of tactical activities by forces in the physical domains (e.g., land, sea, or air) or the operations may be used as long-range strategic weapons directed at the military and infrastructure of another nation. The implications of the purposeful use of devastating cyber methods against a foreign homeland bring up allusions to the use of nuclear weapons. In fact, Lewis asserts that there is a “cyber club” with NATO—the United States, the United Kingdom, and France—that possess not only nuclear weapons, but also an active offensive cyberspace capability.116 Indeed, the United States has officially incorporated offensive cyberspace operations (OCO) in its publicly available joint doctrine in general terms, but details of any OCO implementation remain classified.117 In practical terms, NATO may already be entering the gray zone of developing active cyber defense capabilities that go beyond the firewall to neutralize 27 specific Internet nodes that are conducting attacks, such as those that facilitated distributed denial of service actions experienced by Estonia in 2007. As one NATO cyber officer noted, “NATO has established a capable defence for most cyber threats, but that is just the first step and what needs to quickly follow is the development of ‘active defence’ capabilities.”118 In implementing such measures, decision-makers must recognize that whether acts of active cyber defense are considered offensive is not up to the sender, rather the receiver, because well-justified defensive acts may be misinterpreted as aggression.119 However, if NATO operations do evolve to embrace active cyber defense, and then go further to adopt OCO in a manner similar to that of nuclear weapons, the issue of political control of OCO release and use must be resolved first.120 Healey and Jordan assert that the focus should remain on offensive coordination, not capability, and suggest that NATO should create a group “with voluntary optin for states, modeled after NATO’s existing Nuclear Planning Group, to discuss and map out an offensive cyber policy.”121

#### More US OCOs encourages preemptive attacks and targeting countries global infrastructure---both cascade and entangle allies into conflict

Arts 18—Program coordinator supporting The German Marshall Fund of the United States’ (GMF) security and defense policy work in Washington DC, German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan [Sophie, December 2018, “Offense as the New Defense: New Life for NATO’s Cyber Policy”, GMF Policy Brief, No. 039, <https://nato-engages.org/wp-content/uploads/2019/04/Offense-as-the-New-Defense-New-Life-for-NATO%E2%80%99s-Cyber-Policy.pdf>] AMarb

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

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

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

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

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

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

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

### 2nc – OCOs Bad

#### US explicit commitment to OCOs means that’s the info that they’ll share – the plan ensures they’ll be used.

Trey Herr 18, visiting fellow at the Hoover Institution. Jacquelyn Schneider is an assistant professor and affiliate faculty at the Center for Cyber Conflict Studies at the U.S. Naval War College. You can follow Schneider @JackieGSchneid. Her comments are her own and do not represent the views of the U.S. Navy, the Naval War College, or the Department of Defense, 10-10-2018, "Sharing is Caring: The United States’ New Cyber Commitment for NATO," Council on Foreign Relations, https://www.cfr.org/blog/sharing-caring-united-states-new-cyber-commitment-nato

Given the recent blockbuster headlines about alleged Chinese snooping on server hardware sold to major technology companies and the latest joint-denunciation of Russian cyber operations, you could be forgiven for having missed an important NATO-related development. The Associated Press reports that the U.S. Defense Department will announce a new commitment to use offensive and defensive cybersecurity capabilities on behalf of NATO allies.

The new commitment is notable given how cybersecurity has long been treated as an exceptional domain of operations, and cyber capabilities reserved as strategic national assets to be shared with only the closest of allies. With this announcement, the Pentagon is suggesting that cyber capabilities might be used alongside conventional weapons with allies and indeed, equal weight appears to be given to offensive and defensive operations. Perhaps most significantly, the announcement moves NATO partners closer to what has been a tight coterie of U.S.-favored signals intelligence partners such as the United Kingdom, New Zealand, Australia, and Canada.

The DoD announcement is a sign of the continued, if nascent, normalization of cybersecurity under the current administration and in Europe. Even where offensive cyber operations may not rise to the level of war, they provide decision-makers with options to influence the geopolitical environment. This aligns with recent trends in the U.S. military to integrate cyber capabilities into maneuver units and large exercises, and reflects the shift towards more risk acceptant and offensive measures to counter cyberattacks found in the 2018 DoD Cyber Strategy.

Moving cyber capabilities into the same strategic frame as conventional weapons, especially with NATO, reflects a shift in institutional cyber arrangements within the United States and the growing power of the military relative to the intelligence community. For the United States, cyber capabilities have always had a complicated relationship with the intelligence community, in particular the National Security Agency (NSA). When Cyber Command stood up in 2010 as a sub-unified combatant command within the Department of Defense, it moved into the NSA’s headquarters, staffed its management ranks with longtime NSA employees, borrowed networks and technical capabilities, and to this day shares a dual-hatted commander. In the immediate years after the command was created, it was logical that the structure of partnerships with allies looked more like the special signals intelligence relationships formed around the NSA rather than traditional alliance networks in NATO and Asia. The recent announcement aligns cyber operations more closely with Department of Defense missions, which are more likely to posture capabilities for deterrent effects, than intelligence missions, which view capabilities as assets to be carefully husbanded.

Treating cybersecurity capabilities more like conventional arms and less like national assets also helps drive the integration of cyber operations into the planning and execution of a broader array of conventional military missions. Early cyber operations were largely conventional espionage and surveillance activities supercharged by the spread of computing and the internet. In the United States, this led to the creation of large and complex software tools, carefully guarded by the intelligence community as national assets (sometimes unsuccessfully). The DoD’s announcement indicates a move towards treating at least some of these capabilities, along with their supporting infrastructure, more like conventional armaments and making them available for broader use; a model closer to Central or Special Operations Command and less like the National Security Agency.

The Pentagon’s new commitment also reflects changes in how Europe talks about cybersecurity and characterizes the Russian threat. The last two years have seen a trend toward more open discussion of offensive cyber operations and the possibility of the alliance adopting more assertive postures to counter cyber operations against its members. After years of devastating ransomware attacks and cyber-enabled information attacks, NATO members are more willing to explore cyber triggers to Article 5. They have also been more willing to articulate the cyber threat against the alliance. In addition to last week’s denunciation by Dutch, UK, and U.S. authorities, Russian state actors are widely suggested to be responsible for an increasingly brazen series of operations, including targeting German government ministries, French and British TV stations, and more.

Sharing offensive cyber capabilities raises the question of whether cyber operations can extend effective deterrence to NATO partners. There seems to be little focus on using these operations to deter conventional or nuclear attacks on NATO countries, but this may evolve. The United States seems to want NATO to use cyber operations to deter other cyber operations, particularly those falling under the threshold of armed conflict. Cyber operations have all sorts of problems for deterrence: signaling is difficult, they can be perceived as a cheap threat, and their effects are largely uncertain. By contrast, moving new military forces in Eastern Europe or conducting ground exercises are credible signals of extended deterrence, but are costly and time consuming. Cyber capabilities aren’t free, nor are they necessarily cheap, but the promise to use them can add new credibility to a deterrent threat without the same investment and delay as conventional alternatives. Sharing cyber capabilities may be a cheaper way to signal alliance commitment than other options and might signal a further maturation, and acceptance, of cybersecurity into geopolitics.

#### Defending forward with OCOs crates endless cyberwar with miscalculation---intelligence solves

Brandon Valeriano & Benjamin Jensen 19, 1-15-2019, Brandon Valeriano is a Senior Fellow at the Cato Institute. He is also the Bren Chair of Military Innovation at the Marine Corps University and serves as Senior Advisor for the Cyber Solarium Commission. Dr. Valeriano has published six books and dozens of articles for such outlets as the Journal of Politics, International Studies Quarterly, and the Journal of Peace Research. His two most recent books are Cyber War versus Cyber Reality (2015) and Cyber Strategy (2018), both with Oxford University Press. "The Myth of the Cyber Offense: The Case for Restraint," Cato Institute, https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint

The Myth of the Offense

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

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

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

Defense and Deception

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

Fear and the Security Dilemma

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

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