# Ban Offensive Cyber Operations Affirmative



## 1AC

### 1AC – Inherency

#### Cyberwarfare has become increasingly important and complex. The United States and NATO are at an important crossroads when it comes to their offensive cyber operations policy. Continuing their offensive cyber operations could make a global conflict inevitable which is why a ban is needed now.

Brandon Valeriano and Benjamin Jensen, 19, (Brandon Valeriano and Benjamin Jensen, Brandon Valeriano Senior Fellow, Cato Institute Benjamin Jensen Professor of Strategic Studies, School of Advanced Warfighting at the Marine Corps University, 1-15-2019, Cato Institute, The Myth of the Cyber Offense: The Case for Restraint, https://www.cato.org/policy-analysis/myth-cyber-offense-case-restraint#notes, 6-26-2022) SCade

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

### 1AC – Plan

**Plan: The United States federal government substantially increase its security cooperation with the North Atlantic Treaty Organization in the area of cybersecurity by banning offensive cyber operations.**

### 1AC - Advantage – Miscalculation

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

Sophie **Arts, 18**, (Sophie Arts, Sophie is 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, 2018, The German Marshall Fund of the United States, “Offense as the New Defense: New Life for NATO’s Cyber Policy”, https://nato-engages.org/wp-content/uploads/2019/04/Offense-as-the-New-Defense-New-Life-for-NATO%E2%80%99s-Cyber-Policy.pdf, 6-26-2022) SCade

Deter, then Defend? NATO’s defenses are only as strong as the sum of those of its members. Like in other domains, alliance cyber assets are not NATO-owned but provided by member states.19 **U.S. capabilities** in the cyber domain are by far the **most sophisticated among the allies**. Besides having an edge over most competitors in the field of cyber security,20 the United States **tops rankings** as a **global leader in offensive cyber capabilities**.21 The recent announcement that it would contribute its capabilities to NATO operations consequently could help the alliance **bolster its deterrence posture** against hostile cyber-attacks. Until recently, NATO and member states, including the United States, have relied on strictly defensive cyber tools to protect their infrastructure. However, given that this approach has done **little to discourage hostile actors**, the strategic value of incorporating **o**ffensive **c**yber **o**perations 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 **o**ffensive **c**yber **o**peration**s**. 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.

**Preemptive cyberwar causes nuclear war and draw-in even if NATO-Russia war does not---independently crushes nuclear deterrence**

Michael T. **Klare, 19**, (Michael T. Klare, Michael T. Klare is a professor emeritus of peace and world security studies at Hampshire College and senior visiting fellow at the Arms Control Association. This is the fourth in the “Arms Control Tomorrow” series, in which he considers disruptive emerging technologies and their implications for war-fighting and arms control., 11-1-2019, Arms Control Association, Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation, https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#bio, 6-26-2022) SCade

Edited for language

For the past several years, the U.S. Department of Defense has been exploring how it could employ its own very robust cyberattack capabilities to compromise or destroy enemy missiles from such states as North Korea before they can be fired, a strategy sometimes called “left of launch.”3 Russia and China can assume, on this basis, that their own launch facilities are being probed for such vulnerabilities, presumably leading them to adopt escalatory policies such as those espoused in the 2018 NPR report. Wherever one looks, therefore, the links between cyberwar and nuclear war are growing. The Nuclear-Cyber Connection These links exist because the NC3 systems of the United States and other nuclear-armed states are heavily dependent on computers and other digital processors for virtually every aspect of their operation and because those systems are **highly vulnerable to cyberattack**. Every nuclear force is composed, most basically, of weapons, early-warning radars, launch facilities, and the top officials, usually presidents or prime ministers, empowered to initiate a nuclear exchange. Connecting them all, however, is an extended network of communications and data-processing systems, all reliant on cyberspace. Warning systems, ground- and space-based, must constantly watch for and analyze possible enemy missile launches. Data on actual threats must rapidly be communicated to decision-makers, who must then weigh possible responses and communicate chosen outcomes to launch facilities, which in turn must provide attack vectors to delivery systems. All of this involves operations in cyberspace, and it is in this domain that great power rivals seek vulnerabilities to exploit in a constant struggle for advantage. The use of cyberspace to gain an advantage over adversaries takes many forms and is not always aimed at nuclear systems. China has been accused of engaging in widespread cyberespionage to steal technical secrets from U.S. firms for economic and military advantages. Russia has been accused, most extensively in the Robert Mueller report, of exploiting cyberspace to interfere in the 2016 U.S. presidential election. Nonstate actors, including terrorist groups such as al Qaeda and the Islamic State group, have used the internet for recruiting combatants and spreading fear. Criminal groups, including some thought to be allied with state actors, such as North Korea, have used cyberspace to extort money from banks, municipalities, and individuals.4 Attacks such as these occupy most of the time and attention of civilian and military cybersecurity organizations that attempt to thwart such attacks. Yet for those who worry about strategic stability and the risks of nuclear escalation, it is the threat of cyberattacks on NC3 systems that provokes the greatest concern. Gen. Paul M. Nakasone, commander of U.S. Cyber Command, testifies during a Senate Armed Services Committee hearing on February 14. He warned that China and Russia are conducting sustained cybercampaigns against the United States. (Photo: Mark Wilson/Getty Images)Gen. Paul M. Nakasone, commander of U.S. Cyber Command, testifies during a Senate Armed Services Committee hearing on February 14. He warned that China and Russia are conducting sustained cybercampaigns against the United States. (Photo: Mark Wilson/Getty Images)This concern stems from the fact that, despite the immense effort devoted to protecting NC3 systems from cyberattack, no enterprise that relies so extensively on computers and cyberspace can be made 100 percent invulnerable to attack. This is so because such systems employ many devices and operating systems of various origins and vintages, most incorporating numerous software updates and “patches” over time, offering multiple vectors for attack. Electronic components can also be modified by hostile actors during production, transit, or insertion; and the whole system itself is dependent to a considerable degree on the electrical grid, which itself is vulnerable to cyberattack and is far less protected. Experienced “cyberwarriors” of every major power have been working for years to probe for weaknesses in these systems and in many cases have devised cyberweapons, typically, malicious software (malware) and computer viruses, to exploit those weaknesses for military advantage.5 Although activity in cyberspace is much more difficult to detect and track than conventional military operations, enough information has become public to indicate that the major nuclear powers, notably **China**, **Russia**, and the **U**nited **S**tates, along with such secondary powers as **Iran** and **No**rth **Ko**rea, have established extensive cyberwarfare capabilities and engage in **offensive cyberoperations** on a regular basis, often aimed at **critical military infrastructure**. “Cyberspace is a contested environment where we are in constant contact with adversaries,” General Paul M. Nakasone, commander of the U.S. Cyber Command (Cybercom), told the Senate Armed Services Committee in February 2019. “We see near-peer competitors [China and Russia] conducting sustained campaigns below the level of armed conflict to erode American strength and gain strategic advantage.” Although eager to speak of adversary threats to U.S. interests, Nakasone was noticeably but not surprisingly reluctant to say much about U.S. offensive operations in cyberspace. He acknowledged, however, that Cybercom took such action to disrupt possible Russian interference in the 2018 midterm elections. “We created a persistent presence in cyberspace to monitor adversary actions and crafted tools and tactics to frustrate their efforts,” he testified in February. According to press accounts, this included a cyberattack aimed at paralyzing the Internet Research Agency, a “troll farm” in St. Petersburg said to have been deeply involved in generating disruptive propaganda during the 2016 presidential elections.6 Other press investigations have disclosed two other offensive operations undertaken by the United States. One called “Olympic Games” was intended to disrupt Iran’s drive to increase its uranium-enrichment capacity by sabotaging the centrifuges used in the process by infecting them with the so-called Stuxnet virus. Another left of launch effort was intended to cause malfunctions in North Korean missile tests.7 Although not aimed at either of the U.S. principal nuclear adversaries, those two attacks demonstrated a willingness and capacity to conduct cyberattacks on the nuclear infrastructure of other states. Efforts by strategic rivals of the United States to infiltrate and eventually degrade U.S. nuclear infrastructure are far less documented but thought to be no less prevalent. Russia, for example, is believed to have planted malware in the U.S. electrical utility grid, possibly with the intent of cutting off the flow of electricity to critical NC3 facilities in the event of a major crisis.8 Indeed, every major power, including the United States, is believed to have crafted cyberweapons aimed at critical NC3 components and to have implanted malware in enemy systems for potential use in some future confrontation. Pathways to Escalation Knowing that the NC3 systems of the major powers are constantly being probed for weaknesses and probably infested with malware designed to be activated in a crisis, what does this say about the risks of escalation from a nonkinetic battle, that is, one fought without traditional weaponry, to a kinetic one, at first using conventional weapons and then, potentially, nuclear ones? None of this can be predicted in advance, but those analysts who have studied the subject worry about the emergence of dangerous new pathways for escalation. Indeed, several such scenarios have been identified.9 The first and possibly **most dangerous path to escalation** would arise from the **early use** of cyberweapons in a great power crisis to ~~paralyze~~ the vital command, control, and communications capabilities of an adversary, many of which serve nuclear and conventional forces. In the “fog of war” that would naturally ensue from such an encounter, the recipient of such an attack might fear more punishing follow-up kinetic attacks, possibly **including the use of nuclear weapons**, and, fearing the loss of its own arsenal, launch its weapons immediately. This might occur, for example, in a **confrontation between NATO and Russian forces** in east and central Europe or between U.S. and Chinese forces in the Asia-Pacific region. Speaking of a possible confrontation in Europe, for example, James N. Miller Jr. and Richard Fontaine wrote that “both sides would have overwhelming incentives to go early with offensive cyber and counter-space capabilities to negate the other side’s military capabilities or advantages.” If these early attacks succeeded, “it could result in huge military and coercive advantage for the attacker.” This might induce the recipient of such attacks to back down, affording its rival a major victory at very low cost. Alternatively, however, the recipient might view the attacks on its critical command, control, and communications infrastructure as the **prelude to a full-scale attack** aimed at neutralizing its nuclear capabilities and **choose to strike first**. “It is worth considering,” Miller and Fontaine concluded, “how even a very limited attack or incident could set both sides on a **slippery slope to rapid escalation**.”10 U.S. servicemen conduct a defensive cyberoperations exercise at Ramstein Air Base, Germany, on March 8. (U.S. Air Force photo by Master Sgt. Renae Pittman)U.S. servicemen conduct a defensive cyberoperations exercise at Ramstein Air Base, Germany, on March 8. (U.S. Air Force photo by Master Sgt. Renae Pittman)What makes the insertion of latent malware in an adversary’s NC3 systems so dangerous is that it may not even need to be activated to increase the risk of nuclear escalation. If a nuclear-armed state comes to believe that its critical systems are infested with enemy malware, its leaders might not trust the information provided by its early-warning systems in a crisis and might misconstrue the nature of an enemy attack, leading them to overreact and possibly launch their nuclear weapons out of fear they are **at risk of a preemptive strike**. “The uncertainty caused by the unique character of a cyber threat could **jeopardize the credibility of the nuclear deterrent** and **undermine strategic stability** in ways that advances in nuclear and conventional weapons do not,” Page O. Stoutland and Samantha Pitts-Kiefer wrote in 2018 paper for the Nuclear Threat Initiative. “[T]he introduction of a flaw or malicious code into nuclear weapons through the supply chain that compromises the effectiveness of those weapons could lead to a lack of confidence in the nuclear deterrent,” undermining strategic stability.11 Without confidence in the reliability of its nuclear weapons infrastructure, a nuclear-armed state may misinterpret confusing signals from its early-warning systems and, fearing the worst, launch its own nuclear weapons rather than lose them to an enemy’s first strike. This makes the scenario proffered in the 2018 NPR report, of a nuclear response to an enemy cyberattack, that much more alarming.

**It triggers tit-for-tat retaliation that escalates out of control**

Jason **Healy**, **2019**, (School of International and Public Affairs, Columbia University), “The implications of persistent (and permanent) engagement in cyberspace” Journal of Cybersecurity, 2019, https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878#140575448/ceng

The new strategy is a compelling assessment of cyber conflict as a state of constant contact and presents a strong case that reduced operational constraints enabling tactical friction to regain the initiative will nudge conflict back towards lower levels of aggression [9]. It is worth noting that forward defense is only one among several policies that can be termed active defense or indeed cyber deterrence: the administration of Donald Trump has continued and expanded a wide set of policy tools used by previous administrations, including sanctions and indictments [59]. It has also introduced new responses, most importantly coordinated international attribution of Russian [60] and North Korean [61] operations seen as particularly insulting to global norms and getting search warrants for computers outside of US territory in order to disrupt a North Korean botnet [62]. Still, it is no wonder that the US military has embraced an academic concept justifying its decade-long desire for **reduced operational constraints** and a more **active posture** to “take the fight to the enemy.” There remain major concerns. An **overarching worry** is that US Cyber Command **does not** appear to see this approach as fundamentally **risky.** The Vision asserts that the Command wants to be “not risk averse but risk aware” but it only highlights one procedural risk (an insufficient body of highly trained personnel) and one diplomatic risk (adversaries will falsely “seek to portray our strategy as ‘militarizing’ the cyberspace domain”). But those are the only risks the Command can imagine, or at least, is willing to publicly acknowledge. Indeed, because defending forward is framed as essential—“if the United States is to shape the development of international cyberspace norms, it can do so only through active cyber operations” [54], and “not a choice, but a structurally and strategically driven imperative” [57]—then the main risk is failing to adapt quickly and forcefully enough. To get to the promised land of milk and honey, superiority and stability, there is only one path: forward defense. It is technically determined that there is a single dominant strategy, one that is the best regardless of the strategies chosen by US adversaries. As in the Cold War, the military is again attempting to “pose starker alternatives and to couch them in terms of necessity rather than choice:” either remove constraints on the military or lose [63]. Imperatives are slippery things. Some are not imperatives at all, just a particularly unyielding perspective or preference presented as a dichotomy. How many US airmen died in World War Two because of the bomber-driven cult of the offensive? Other imperatives may be critical to tactical success but imperil the larger strategy, perhaps winning the battle but losing the war. The battlefield imperative to use overwhelming firepower can, for example, be fatal to a counterinsurgency strategy if it causes extensive collateral damage. Even seeming strategic imperatives can lead to catastrophic national security outcomes, as with Wilhelmine Germany’s pursuit of a grand fleet-in-being to challenge the British [64]. The dynamics here may be similar. A more thorough assessment of the risks must be rooted with the simplest one, the strategy might fail and **intensify competition**. Many assumptions, apparently unrecognized, underlie the belief that the USA can have both superiority and overmatch as well as stability. Yet, in a system as complex as the Internet, “we can never merely do one thing” [9, page 10].8 As Herb Lin and Max Smeets of Stanford University highlight, “neither ‘escalate’ or ‘escalation’ appear in the [Vision] document,” a significant omission which suggests US Cyber Command is **downplaying**, or not fully thinking through, the full dynamics of conflict [65]. A more engaged forward defense might result not in “negative” feedback—reducing conflict by bringing it back to the historical norm—but instead “**positive” feedback**, exacerbating the conflict and adversaries may see the new US vision as a challenge to **rise to,** rather than one from which to back away [9, chapter 4]. According to my colleague Robert Jervis, “a failure to anticipate positive feedback is one reason why consequences are often unintended,” [9, page 165] and sufficient positive feedback can push the system past **a tipping point**, at which the system resets itself into a new, and potentially far more dangerous, equilibrium. States have decided to keep their attacks below certain thresholds, but conflict and **competition** in cyberspace is only a few decades old. This may only be a phase, and an early one at that. As cyberspace becomes more **existential** for more states, the stakes continue to rise, elevating the risks along with them.

**That causes hack-backing which is uniquely destabilizing**

**Sorcher ’15**, Sara; April 6; National Security Correspondent for the National Journal and Deputy Editor of Passcode at the Christian Science Monitor; "Influencers: Companies should not be allowed to hack back," Passcode. http://passcode.csmonitor.com/influencers-hackback/ceng

Even as companies are hit by increasingly sophisticated cyberattacks, 82 percent of Influencers say they should not be allowed to **"hack back"** to retrieve stolen data or shut down computers targeting their networks. There's been hot debate over companies' rights to defend themselves in cyberspace by taking offensive action. The US government has been **reluctant to intervene** as foreign-based hackers strike private companies – leaving this type of hacker-on-hacker retaliation a **tantalizing option** for some victims. But Passcode's pool of experts from across government, the private sector, and the privacy advocacy community warn the strategy, commonly known as **"hacking back," could go very wrong**. "Hacking back is the **worst option** for companies because they don't know who is on the other end of the keyboard nor what capabilities that person has. What may start as simple [intellectual property] theft could, after a 'hacking back' attempt, result in the utter destruction of the entire network," says Jeffrey Carr, president of cybersecurity firm Taia Global. "For a small to medium-sized company, that could put them out of business. For an enterprise, it could cost them hundreds of millions of dollars. People with any life experience usually understand and respect the adage 'never pick a fight with a stranger.' The same adage applies in cyberspace." It could also **spark foreign policy consequences**. Hackers could be backed by other nation-states, heightening the prospect of a **wider digital conflict** **inadvertently launched** by the private sector. "We should not be looking to **escalate a cyberwar**; we should be trying to defuse it," said one Influencer who chose to remain anonymous. Another added: "Would we let it happen in the physical world?" The Passcode Influencers Poll brings together a diverse group of more than 90 security and privacy experts from across government, the private sector, academia, and the privacy community. To preserve the candor of their responses, Influencers have the choice to keep their comments anonymous, or voice their opinions on the record. Some Influencers drew upon their own personal experiences to explain the potential perils. "I am an old Army cyber guy and I had a boss who, when I was feeling frustrated when I could not respond in kind back to a bad guy who was attacking us, would pull me aside and say, 'You know what, Rick? The enemy gets a vote,' " says Rick Howard, chief security officer for Palo Alto Networks. "Just because you are able to jab back against a cyber adversary does not mean that you should. Do you think the bad guy will just go away simply because you took a swing at him? Do you think he will say, 'Wow, these guys are tough. I guess I will hang up my hacking spurs forever?' More likely than not, you would have succeeded in **poking the beehive** and you may have unleashed a world of hurt on your organization that it did not need." Even government organizations where the sole purpose, Mr. Howard said, is to attribute attacks have a hard to doing it with any level of confidence that would warrant an offensive action. "The idea of turning that problem over to a commercial organization who does not have a **tenth of the resources** is ludicrous," he said. "The result would be to transform the Internet into the **Wild Wild West**; commercial organizations pointing their cyber six-shooters at any perceived slight rightfully or wrongly." Even then, Howard says, the task should be left to **professionals: law enforcement and intelligence**. They too "absolutely should not get carte blanche for this kind of activity. There has to be some rules put in place that all citizens understand. There has to be some oversight put in place that regularly reports back to the citizenry about what these forces are doing." A minority of 18 percent of Influencers said companies should be allowed to hack back after they're hit. "There is a significant spectrum of options for a victim to employ against a cyberattacker; 'shutting down' the computers used in an attack is at the extreme end of that spectrum," one Influencer said. "The fact is, the US government is **not responding** to vast majority of cyberintrusions, whether for theft or destruction; private companies are on their own, and as such, they should be able to defend themselves in cyberspace. Does the Second Amendment not extend to cyberspace?" If companies cannot get timely help and protection from law enforcement, one Influencer said, "they should be allowed to take responsible action to mitigate the impact of theft of their data. This should be done with full accountability for any damage to innocent parties." Companies should be allowed to hack back "but only under strict controls, such as using a bonded, licensed company – perhaps even deputized by an accredited law enforcement agency – which acts on their behalf," suggested Jay Healey, head of the Cyber Statecraft Initiative at the Atlantic Council think tank. "This should start as a small pilot project as the **international blow back** is likely to be **significant**." We want to hear from you. Take the readers version of the Influencers poll here. "Hacking back sounds like a great idea until you think about how easy it is to subvert. Today's attackers go to great lengths to hide the source of their attacks. How can any company know they're really hacking their attacker, and not some innocent bystander?" - Matthew Green, Johns Hopkins University "The idea that someone could 'hack back' without producing unintended consequences is absurd pipe dream promoted by businesses trying to monetize the concept. The millions of innocent people around the world whose machines are unwittingly serving as waypoints or botnet hosts would be the ones who ultimately pay the price." - Chris Finan, Manifold Security "Today the Internet is the Wild West; with hack back it moves closer to Hobbes' Leviathan." - Jacob Olcott, BitSight Technologies "Companies should be investing in actual defense mechanisms, not offensive capabilities. Actually doing defense is a far better security tactic than 'hack back.' Additionally, companies tend to have a misunderstanding of how difficult doing offense is and a misunderstanding of what can be gained. Applying the resources to being able to do 'hack back' to security would be a better use of those resources and go farther for the intended goals. Additionally, once data is gone from the network there is rarely any ability to 'retrieve' it or keep it from ending up in the adversary's hands. Executives in companies discussing 'hack back' strategies should focus efforts on empowering and training their people, breaking down cultural barriers hampering security, and aligning efforts to the threats they actually face." - Robert Lee, Dragos Security "It depends. There are so many possible unintended consequences in hacking back that unless you truly understand what you are doing, it isn't worth the risk. Remember, when you hack back, you are escalating an event with someone who may have far greater skills, resources and evil intent than you. Hacking back should only be done after consulting with legal counsel because this opens a company up to all sorts of complex legal issues – especially if you hack back and find out you’ve made a mistake. Additionally and this is a bit unfair, but if you couldn’t keep someone out of your environment in the first place, what makes you think you have the skill to up the game by attacking back?" - Mark Weatherford, Chertoff Group "Hey, I've got an idea, let's legalize vigilantism, but only for the one type of crime where people constantly talk about how difficult accurate attribution is. What could go wrong?" - Julian Sanchez, Cato Institute "This is the role of law enforcement. Allowing a safe harbor for 'hack backs' would be an invitation to abuse competitors and the like. Let's keep the job where it belongs, with law enforcement." - Influencer "We can't be taking law into our own hands as a general rule. Would need to understand the facts and circumstances. One should always contact law enforcement as fast as possible." - Influencer "Vigilantism feels good but is rarely effective (for anyone other than Liam Neeson)." - Peter Singer, New America "While we can imagine cases where it'd be satisfying for companies to do this, madness this way lies. Bad actors almost never directly tunnel into a network; they hide behind hijacked accounts and machines. To contemplate 'hacking back' puts those intermediate accounts and machines more in the crossfire. This isn't to say nothing should be done – ISPs and others can play a helpful role in quarantining the launching pads of attacks that are being used without their owners' knowledge – but hacking back should be off the table." - Jonathan Zittrain, Harvard University "The legal right to 'hack back' would incentivize an **escalating** spiral of **attacks** with almost certain **collateral damage** to both networks and individuals. In the most sophisticated and damaging attacks, accurately identifying the attacker has proven elusive at best." - Influencer "Hack back, retaliation, vigilantism. These words not only make for great headlines; they spark heated debate over the appropriate roles of the private sector and government in cybersecurity. Unfortunately, the 'hack-back' debate often obscures a much more fundamental debate over the future direction of US cybersecurity policy. For the past two decades, US cybersecurity has focused almost exclusively on defense – we've dedicated our time and resources to making it harder for our adversaries to penetrate our networks. But strong network fortifications are not fail-safe. Especially against nation-states and other concerted adversaries who are willing to go to almost any level of time, effort, and expense to penetrate a target's network. Defensive measures alone may delay – but are unlikely to prevent – penetration of target networks by concerted adversaries. Focusing exclusively on defense will not solve our cybersecurity problem. We need to raise the costs and risks to concerted adversaries in order to deter their activities. There are many divergent views as to the best way to do this, but one thing is clear: the time has come for a national conversation. Effective **deterrence** is **not synonymous with hack-back**, retaliation, or vigilantism. Elements of an effective deterrence strategy include: real-time **detection** of intrusions (a high likelihood of discovery will deter some would-be intruders) as well as **identification** and punishment of cyberintruders. In the absence of such consequences, cyberintruders should be expected to continue targeting our networks." - Melanie Teplinsky, American University "There is a range of activities from passive defense, through more active defense, to offensive tactics. We do need to move to where something **more active than today**, but perhaps less than **full scale 'hack back'** is acceptable and even more commonplace." - Influencer

**It overwhelms conventional norms---MAD can’t check**

Erik **Gartzke** **and** Jon R. **Lindsay**, **2017**, Gartzke is at the Department of Political Science, University of California, San Diego; Lindsay is at the Munk School of Global Affairs, University of Toronto. 03/01/2017. “Thermonuclear Cyberwar.” Journal of Cybersecurity, vol. 3, no. 1, pp. 37–48/ceng

Cyber warfare is routinely overhyped as a new weapon of mass destruction, but when used in **conjunction** with actual weapons of mass destruction, **severe**, and **underappreciated, dangers** emerge. One side of a stylized debate about cybersecurity in international relations argues that offensive advantages in cyberspace empower weaker nations, terrorist cells, or even lone rogue operators to paralyze vital infrastructure [4–8]. The other side argues that operational difficulties and effective deterrence restrains the severity of cyber attack, while governments and cybersecurity firms have a pecuniary interest in exaggerating the threat [9–13]. Although we have contributed to the skeptical side of this debate [14–16], \*\*\*BEGIN FOOTNOTE\*\*\* 14. **Gartzke** E. The **myth of cyberwar**: bringing war in cyberspace back down to earth. Int Security 2013;38:41–73. Google ScholarCrossRef 15 **Lindsay** JR. Stuxnet and the **limits of cyber war**fare. Security Stud 2013;22:365–404. Google ScholarCrossRef 16 **Lindsay** JR. The impact of China on cybersecurity: **fiction and friction**. Int Security 2014;39:7–47. Google ScholarCrossRef \*\*\*END FOOTNOTE\*\*\* the same strategic logic that leads us to view cyberwar as a limited political instrument in most situations also leads us to view it as **incredibly destabilizing** in rare situations. In a recent Israeli wargame of a regional scenario involving the United States and Russia, one participant remarked on “how quickly **localized** cyber events can turn **dangerously kinetic** when leaders are ill-prepared to deal in the cyber domain” [17]. Importantly, this sort of **catalytic instability** arises not from the cyber domain itself but through its interaction with forces and characteristics in other domains (land, sea, air, etc.). Further, it arises only in situations where actors possess, and are willing to use, robust **traditional** military forces to defend their interests. Classical deterrence theory developed to explain nuclear deterrence with nuclear weapons, but different types of weapons or **combinations** of operations in different domains can have **differential effects** on deterrence and defense [18, 19]. Nuclear weapons and cyber operations are particularly **complementary** (i.e. nearly complete opposites) with respect to their strategic characteristics. Theorists and practitioners have stressed the unprecedented **destructiveness** of nuclear weapons in explaining how nuclear deterrence works, but it is equally, if not more, important for deterrence that capabilities and intentions are **clearly communicated**. As quickly became apparent, **public displays** of their nuclear arsenals improved deterrence. At the same time, disclosing **details** of a nation’s nuclear capabilities did not much degrade the ability to strike or retaliate, given that defense against nuclear attack remains extremely difficult. Knowledge of nuclear capabilities is necessary to achieve a deterrent effect [20]. **Cyber** operations, in contrast, rely on **undisclosed vulnerabilities**, social engineering, and creative guile to generate indirect effects in the information systems that coordinate military, economic, and social behavior. Revelation enables crippling countermeasures, while the imperative to conceal capabilities constrains both the scope of cyber operations and their utility for coercive signaling [21, 22]. The diversity of cyber operations and confusion about their effects also contrast with the obvious destructiveness of nuclear weapons. The problem is that transparency and deception **do not mix well**. An attacker who hacks an adversary’s nuclear command and control apparatus, or the weapons themselves, will gain an **advantage in warfighting** that the attacker **cannot reveal**, while the **adversary** will **continue to believe it wields a deterrent that may no longer exist.** Most analyses of inadvertent escalation from cyber or conventional to nuclear war focus on “use it or lose it” pressures and fog of war created by attacks that become visible to the target [23, 24]. In a US–China conflict scenario, for example, conventional military strikes in conjunction with cyber attacks that blind sensors and confuse decision making could generate incentives for both sides to rush to preempt or escalate [25–27]. These are plausible concerns, but the revelation of information about a newly unfavorable balance of power might also cause hesitation and lead to compromise. Cyber blinding could potentially make traditional offensive operations more difficult, shifting the advantage to defenders and making conflict less likely. **Clandestine attacks** that remain invisible to the target potentially present a **more insidious threat to crisis stability**. There are empirical and theoretical reasons for taking seriously the effects of offensive cyber operations on nuclear deterrence, and we should expect the dangers to vary with the relative cyber capabilities of the actors in a crisis interaction. Nuclear command and control vulnerability General Robert Kehler, commander of US Strategic Command (STRATCOM) in 2013, stated in testimony before the Senate Armed Services Committee, “we are very concerned with the potential of a cyber-related attack on our nuclear command and control and on the weapons systems themselves” [28]. Nuclear command, control, and communications (NC3) form the nervous system of the nuclear enterprise spanning intelligence and early warning sensors located in orbit and on Earth, fixed and mobile command and control centers through which national leadership can order a launch, operational nuclear forces including strategic bombers, land-based intercontinental missiles (ICBMs), submarine-launched ballistic missiles (SLBMs), and the communication and transportation networks that tie the whole apparatus together [29, 30]. NC3 should ideally ensure that nuclear forces will **always be available** if **authorized** by the National Command Authority (to **enhance deterrence**) and never used **without authorization** (to enhance **safety** and **reassurance**). **Friendly errors** or **enemy interference** in NC3 can **undermine the “always-never” criterion**, **weakening deterrence** [31, 32]. NC3 has long been recognized as the **weakest link** in the US nuclear enterprise. According to a declassified official history, a Strategic Air Command (SAC) task group in 1979 “reported that tactical warning and communications systems … were ‘fragile’ and susceptible to electronic countermeasures, electromagnetic pulse, and sabotage, which could deny necessary warning and assessment to the National Command Authorities” [33]. Two years later, the Principal Deputy Under Secretary of Defense for Research and Engineering released a broad-based, multiservice report that doubled down on SAC’s findings: “the United States could not assure survivability, endurability, or connectivity of the national command authority function” due to: major command, control, and communications deficiencies: in tactical warning and attack assessment where existing systems were vulnerable to disruption and destruction from electromagnetic pulse, other high altitude nuclear effects, electronic warfare, sabotage, or physical attack; in decision making where there was inability to assure national command authority survival and connection with the nuclear forces, especially under surprise conditions; and in communications systems, which were susceptible to the same threats above and which could not guarantee availability of even minimum-essential capability during a protracted war. [33] The nuclear weapons safety literature likewise provides a number of troubling examples of NC3 glitches that illustrate some of the **vulnerabilities** attackers **could**, in principle, **exploit** [34–36]. The SAC history noted that **NORAD** has received **numerous false launch indications** from faulty computer components, **loose circuits**, and even a **nuclear war training tape** loaded by mistake into a live system that produced erroneous Soviet launch indications [33]. In a 1991 briefing to the STRATCOM commander, a Defense Intelligence Agency targeteer confessed, “Sir, I apologize, but we have found a problem with this target. There is a mistake in the computer code … . Sir, the error has been there for at least the life of this eighteen-month planning cycle. The nature of the error is such that the target would not have been struck” [37]. It would be a difficult operation to intentionally plant undetected errors like this, but the presence of bugs does reveal that such **a hack is possible**. Following many near-misses and self-audits during and after the Cold War, American NC3 improved with the addition of new safeguards and redundancies. As General Kehler pointed out in 2013, “the nuclear deterrent force was designed to operate through the most extreme circumstances we could possibly imagine” [28]. Yet vulnerabilities remain. In 2010, the US Air Force lost contact with 50 Minuteman III ICBMs for an hour because of a faulty hardware circuit at a launch control center [38]. If the accident had occurred during a crisis, or the component had been sabotaged, the USAF would have been unable to launch and unable to detect and cancel unauthorized launch attempts. As Bruce Blair, a former Minuteman missileer, points out, during a control center blackout the antennas at unmanned silos and the cables between them provide potential surreptitious access vectors [39]. The unclassified summary of a 2015 audit of US NC3 stated that “known capability gaps or deficiencies remain” [40]. Perhaps more worrisome are the unknown deficiencies. A 2013 Defense Science Board report on military cyber vulnerabilities found that while the: nuclear deterrent is regularly evaluated for reliability and readiness … , most of the systems have not been assessed (end-to-end) against a [sophisticated state] cyber attack to understand possible weak spots. A 2007 Air Force study addressed portions of this issue for the ICBM leg of the U.S. triad but was still not a complete assessment against a high-tier threat. [41] If NC3 **vulnerabilities** are unknown, it is also **unknown** whether an **advanced cyber actor** would be able to **exploit** them. As Kehler notes, “**We don’t know what we don’t know**” [28]. Even if NC3 of nuclear forces narrowly conceived is a hard target, cyber attacks on **other critical infrastructure** in preparation to or during a nuclear crisis could **complicate** or **confuse government decision making**. General Keith Alexander, Director of the NSA in the same Senate hearing with General Kehler, testified that: our infrastructure that we ride on, the **power** and the communications grid, are one of the things that is a source of concern … we can go to backup generators and we can have independent routes, but … our ability to **communicate** would be **significantly reduced** and it would complicate our **governance** … . I think what General Kehler has would be intact … [but] the **cascading effect** … in that kind of environment … concerns us. [28] Kehler further emphasized that “there’s a continuing need to make sure that we are protected against electromagnetic pulse and any kind of electromagnetic interference” [28]. Many NC3 components are antiquated and hard to upgrade, which is a mixed blessing. Kehler points out, “Much of the nuclear command and control system today is the legacy system that we’ve had. In some ways that helps us in terms of the cyber threat. In some cases it’s point to point, hard-wired, which makes it very difficult for an external cyber threat to emerge” [28]. The Government Accountability Office notes that the “Department of Defense uses 8-inch floppy disks in a legacy system that coordinates the operational functions of the nation’s nuclear forces” [42]. While this may limit some forms of remote access, it is also indicative of reliance on an earlier generation of software when **security** engineering standards were **less mature**. Upgrades to the digital Strategic Automated Command and Control System planned for 2017 have the potential to correct some problems, but these changes may also introduce new access vectors and vulnerabilities [43]. Admiral Cecil Haney, Kehler’s successor at STRATCOM, highlighted the challenges of NC3 modernization in 2015: Assured and reliable NC3 is fundamental to the credibility of our nuclear deterrent. The aging NC3 systems continue to meet their intended purpose, but risk to mission success is increasing as key elements of the system age. The unpredictable challenges posed by today’s complex security environment make it increasingly important to optimize our NC3 architecture while leveraging new technologies so that NC3 systems operate together as a core set of survivable and endurable capabilities that underpin a broader, national command and control system. [44] In no small irony, the internet itself owes its intellectual origin, in part, to the threat to NC3 from large-scale physical attack. A 1962 RAND report by Paul Baran considered “the problem of building digital communication networks using links with less than perfect reliability” to enable “stations surviving a physical attack and remaining in electrical connection … to operate together as a coherent entity after attack” [45]. Baran advocated as a solution decentralized packet switching protocols, not unlike those realized in the ARPANET program. The emergence of the internet was the result of many other factors that had nothing to do with managing nuclear operations, notably the meritocratic ideals of 1960s counterculture that contributed to the neglect of security in the internet’s founding architecture [46, 47]. Fears of NC3 vulnerability helped to create the internet, which then helped to create the present-day cybersecurity epidemic, which has come full circle to create new fears about NC3 vulnerability. NC3 vulnerability is not unique to the United States. The NC3 of other nuclear powers may even be easier to compromise, especially in the case of new entrants to the nuclear club like North Korea. Moreover, the United States has already demonstrated both the ability and willingness to infiltrate sensitive foreign nuclear infrastructure through operations such as Olympic Games (Stuxnet), albeit targeting Iran’s nuclear fuel cycle rather than NC3. It would be surprising to learn that the United States has failed to upgrade its Cold War NC3 attack plans to include offensive cyber operations against a wide variety of national targets. Hacking the deterrent The United States included NC3 attacks in its Cold War counterforce and damage limitation war plans, even as contemporary critics perceived these options to be destabilizing for deterrence [48]. The best known example of these activities and capabilities is a Special Access Program named Canopy Wing. East German intelligence obtained the highly classified plans from a US Army spy in Berlin, and the details began to emerge publicly after the Cold War. An East German intelligence officer, Markus Wolf, writes in his memoir that Canopy Wing “listed the types of electronic warfare that would be used to neutralize the Soviet Union and Warsaw Pact’s command centers in case of all-out war. It detailed the precise method of depriving the Soviet High Command of its high-frequency communications used to give orders to its armed forces” [49]. It is easy to see why NC3 is such an attractive target in the unlikely event of a nuclear war. If for whatever reason deterrence fails and the enemy decides to push the nuclear button, it would obviously be better to disable or destroy missiles **before they launch** than to rely on possibly futile efforts to shoot them down, or to accept the loss of millions of lives. American plans to disable Soviet NC3 with electronic warfare, furthermore, would have been intended to complement plans for decapitating strikes against Soviet nuclear forces. Temporary disabling of information networks in isolation would have failed to achieve any important strategic objective. A blinded adversary would eventually see again and would scramble to reconstitute its ability to launch its weapons, expecting that preemption was inevitable in any case. Reconstitution, moreover, would invalidate much of the intelligence and some of the tradecraft on which the blinding attack relied. Capabilities fielded through Canopy Wing were presumably intended to facilitate a preemptive military strike on Soviet NC3 to disable the ability to retaliate and limit the damage of any retaliatory force that survived, given credible indications that war was imminent. Canopy Wing included [50]: “Measures for short-circuiting … communications and weapons systems using, among other things, microscopic carbon-fiber particles and chemical weapons.” “Electronic blocking of communications immediately prior to an attack, thereby rendering a counterattack impossible.” “Deployment of various weapons systems for instantaneous destruction of command centers, including pin-point targeting with precision-guided weapons to destroy ‘hardened bunkers’.” “Use of deception measures, including the use of computer-simulated voices to override and substitute false commands from ground-control stations to aircraft and from regional command centers to the Soviet submarine fleet.” “Us[e of] the technical installations of ‘Radio Free Europe/Radio Liberty’ and ‘Voice of America,’ as well as the radio communications installations of the U.S. Armed Forces for creating interference and other electronic effects.” Wolf also ran a spy in the US Air Force who disclosed that the Americans had managed to penetrate the [Soviet air base at Eberswalde]’s ground-air communications and were working on a method of blocking orders before they reached the Russian pilots and substituting their own from West Berlin. Had this succeeded, the MiG pilots would have received commands from their American enemy. It sounded like science fiction, but, our experts concluded, it was in no way impossible that they could have pulled off such a trick, given the enormous spending and technical power of U.S. military air research. [49] One East German source claimed that Canopy Wing had a $14.5 billion budget for research and operational costs and a staff of 1570 people, while another claimed that it would take over 4 years and $65 million to develop “a prototype of a sophisticated electronic system for paralyzing Soviet radio traffic in the high-frequency range” [50]. Canopy Wing was not cheap, and even so, it was only a research and prototyping program. Operationalization of its capabilities and integration into NATO war plans would have been even more expensive. This is suggestive of the level of effort required to craft effective offensive cyber operations against NC3. Preparation comes to naught when a sensitive program is compromised. Canopy Wing was caught in what we describe below as the cyber commitment problem, the inability to disclose a warfighting capability for the sake of deterrence without losing it in the process. According to New York Times reporting on the counterintelligence investigation of the East German spy in the Army, Warrant Officer James Hall, “officials said that one program rendered useless cost hundreds of millions of dollars and was designed to exploit a Soviet communications vulnerability uncovered in the late 1970's” [51]. This program was probably Canopy Wing. Wolf writes, “Once we passed [Hall’s documents about Canopy Wing] on to the Soviets, they were able to install scrambling devices and other countermeasures” [49]. It is tempting to speculate that the Soviet deployment of a new NC3 system known as Signal-A to replace Signal-M (which was most likely the one targeted by Canopy Wing) was motivated in part by Hall’s betrayal [50]. Canopy Wing underscores the potential and limitations of NC3 subversion. Modern cyber methods can potentially perform many of the missions Canopy Wing addressed with electronic warfare and other means, but with even greater stealth and precision. Cyber operations might, in principle, compromise any part of the NC3 system (early warning, command centers, data transport, operational forces, etc.) by blinding sensors, injecting bogus commands or suppressing legitimate ones, monitoring or corrupting data transmissions, or interfering with the reliable launch and guidance of missiles. In practice, the operational feasibility of cyber attack against NC3 or any other target depends on the software and hardware configuration and organizational processes of the target, the intelligence and planning capacity of the attacker, and the ability and willingness to take advantage of the effects created by cyber attack [52, 53]. Cyber compromise of NC3 is technically plausible though operationally difficult, a point to which we return in a later section. To understand which threats are not only technically possible but also probable under some circumstance, we further need a political logic of cost and benefit [14]. In particular, how is it possible for a crisis to escalate to levels of destruction more costly than any conceivable political reward? Canopy Wing highlights some of the strategic dangers of NC3 exploitation. Warsaw Pact observers appear to have been deeply concerned that the program reflected an American willingness to undertake a surprise decapitation attack: they said that it “sent ice-cold shivers down our spines” [50]. The Soviets designed a system called Perimeter that, not unlike the Doomsday Device in Dr. Strangelove, was designed to detect a nuclear attack and retaliate automatically, even if cut off from Soviet high command, through an elaborate system of sensors, underground computers, and command missiles to transmit launch codes [54]. Both Canopy Wing and Perimeter show that the United States and the Soviet Union took nuclear warfighting seriously and were willing to develop secret advantages for such an event. By the same token, they were not able to reveal such capabilities to improve deterrence to avoid having to fight a nuclear war in the first place. Nuclear deterrence and credible communication Nuclear weapons have some salient political properties. They are singularly and obviously destructive. They kill in more, and more ghastly, ways than conventional munitions through electromagnetic radiation, blast, firestorms, radioactive fallout, and health effects that linger for years. Bombers, ICBMs, and SLBMs can project warheads globally without significantly mitigating their lethality, steeply attenuating the conventional loss-of-strength gradient [55]. Defense against nuclear attack is very difficult, even with modern ballistic missile defenses, given the speed of incoming warheads and use of decoys; multiple warheads and missile volleys further reduce the probability of perfect interception. If one cannot preemptively destroy all of an enemy’s missiles, then there is a nontrivial chance of getting hit by some of them. When one missed missile can incinerate millions of people, the notion of winning a nuclear war starts to seem meaningless for many politicians. As defense seemed increasingly impractical, early Cold War strategists championed the threat of assured retaliation as the chief mechanism for avoiding war [56–59]. Political actors have issued threats for millennia, but the advent of nuclear weapons brought deterrence as a strategy to center stage. The Cold War was an intense learning experience for both practitioners and students of international security, rewriting well-worn realities more than once [60–62]. A key conundrum was the practice of brinkmanship. Adversaries who could not compete by “winning” a nuclear war could still compete by manipulating the “risk” of nuclear annihilation, gambling that an opponent would have the good judgment to back down at some point short of the nuclear brink. Brinkmanship crises—conceptualized as games of Chicken where one cannot heighten tensions without increasing the hazard of the mutually undesired outcome—require that decision makers behave irrationally, or possibly that they act randomly, which is difficult to conceptualize in practical terms [63]. The chief concern in historical episodes of chicken, such as the Berlin Crisis and Cuban Missile Crisis, was not whether a certain level of harm was possible, but whether an adversary was resolved enough, possibly, to risk nuclear suicide. The logical inconsistency of the need for illogic to win led almost from the beginning of the nuclear era to elaborate deductive contortions [64–66]. Both mutually assured destruction (MAD) and successful brinksmanship depend on a less appreciated, but no less fundamental, feature of nuclear weapons: political transparency. Most elements of military power are weakened by disclosure [67]. Military plans are considerably less effective if shared with an enemy. Conventional weapons become less lethal as adversaries learn what different systems can and cannot do, where they are located, how they are operated, and how to devise countermeasures and array defenses to blunt or disarm an attack. In contrast, relatively little reduction in destruction follows from enemy knowledge of nuclear capabilities. For most of the nuclear era, no effective defense existed against a nuclear attack. Even today, with evolving ABM systems, one ICBM still might get through and annihilate the capital city. Nuclear forces are more robust to revelation than other weapons, enabling nuclear nations better to advertise the harm they can inflict. The need for transparency to achieve an effective deterrent is driven home by the satirical Cold War film, Dr. Strangelove: “the whole point of a Doomsday Machine is lost, if you keep it a secret! Why didn’t you tell the world, eh?” During the real Cold War, fortunately, Soviet leaders paraded their nuclear weapons through Red Square for the benefit of foreign military attaches and the international press corps. Satellites photographed missile, bomber, and submarine bases. While other aspects of military affairs on both sides of the Iron Curtain remained closely guarded secrets, the United States and the Soviet Union permitted observers to evaluate their nuclear capabilities. This is especially remarkable given the secrecy that pervaded Soviet society. The relative transparency of nuclear arsenals ensured that the superpowers could calculate risks and consequences within a first-order approximation, which led to a reduction in severe conflict and instability even as political competition in other arenas was fierce [61, 68]. Recent insights about the causes of war suggest that **divergent expectations** about the costs and consequences of war are **necessary for contests to occur** [69–73]. These insights are associated with rationalist theories, such as deterrence theory itself. Empirical studies and psychological critiques of the **rationality** assumption have helped to **refine models** and bring some **circumspection** into their application, but the formulation of **sound strategy** (if not the **execution**) still requires the articulation of **some rational linkage** between cause and effect [19, 62, 74]. Many supposedly **nonrational factors**, moreover, simply manifest as **uncertainty** in strategic interaction. Our focus here is on the effect of uncertainty and ignorance on the ability of states and other actors to bargain in lieu of fighting. Many wars are a product of what adversaries do not know or what they misperceive, whether as a result of **bluffing**, **secrecy**, or **intrinsic uncertainty** [75, 76]. If knowledge of capabilities or resolve is a prerequisite for deterrence, then one reason for **deterrence failure** is the inability or unwillingness to **credibly communicate details of the genuine balance of power**, threat, or interests. Fighting, conversely, can be understood as a costly process of discovery that informs adversaries of their actual relative strength and resolve. From this perspective, successful deterrence involves instilling in an adversary perceptions like those that result from fighting, but before fighting actually begins. Agreement about the balance of power can enable states to bargain (tacit or overt) effectively without needing to fight, forging compromises that each prefers to military confrontation or even to the bulk of possible risky brinkmanship crises. Despite other deficits, nuclear weapons have long been considered to be stabilizing with respect to **rational incentives for war** (the risk of nuclear accidents is another matter) [77]. If each side has a secure second strike—or even a minimal deterrent with some nonzero chance of launching a few missiles—then each side can expect to gain little and lose much by fighting a nuclear war. Whereas the costs of conventional war can be more mysterious because each side might decide to hold something back and meter out its punishment due to some internal constraint or a theory of graduated escalation, even a modest initial nuclear exchange is recognized to be extremely costly. As long as both sides understand this and understand (or believe) that the adversary understands this as well, then the relationship is stable. Countries engage nuclear powers with considerable deference, especially over issues of fundamental national or international importance. At the same time, nuclear weapons appear to be of limited value in prosecuting aggressive action, especially over issues of secondary or tertiary importance, or in response to aggression from others at lower levels of dispute intensity. Nuclear weapons are best used for signaling a willingness to run serious risks to protect or extort some issue that is considered of vital national interest. As mentioned previously, both superpowers in the Cold War considered the warfighting advantages of nuclear weapons quite apart from any deterrent effect, and the United States and Russia still do. High-altitude bursts for air defense, electromagnetic pulse for frying electronics, underwater detonations for anti-submarine warfare, hardened target penetration, area denial, and so on, have some battlefield utility. Transparency per se is less important than weapon effects for warfighting uses, and can even be deleterious for tactics that depend on stealth and mobility. Even a single tactical nuke, however, would inevitably be a political event. Survivability of the second strike deterrent can also militate against transparency, as in the case of the Soviet Perimeter system, as mobility, concealment, and deception can make it harder for an observer to track and count respective forces from space. Counterforce strategies, platform diversity and mobility, ballistic missile defense systems, and force employment doctrine can all make it more difficult for one or both sides in a crisis to know whether an attack is likely to succeed or fail. The resulting uncertainty affects not only estimates of relative capabilities but also the degree of confidence in retaliation. At the same time, there is reason to believe that platform diversity lowers the risk of nuclear or conventional contests, because increasing the number of types of delivery platforms heightens second strike survivability without increasing the lethality of an initial strike [78]. While transparency is not itself a requirement for nuclear use, stable deterrence benefits to the degree to which retaliation can be anticipated, as well as the likelihood that the consequences of a first strike are more costly than any benefit. Cyber operations, in contrast, are neither robust to revelation nor as obviously destructive. The cyber commitment problem Deterrence (and compellence) uses force or threats of force to “warn” an adversary about consequences if it takes or fails to take an action. In contrast, defense (and conquest) uses force to “win” a contest of strength and change the material distribution of power. Sometimes militaries can change the distribution of information and power at the same time. Military mobilization in a crisis signifies resolve and displays a credible warning, but it also makes it easier to attack or defend if the warning fails. Persistence in a battle of attrition not only bleeds an adversary but also reveals a willingness to pay a higher price for victory. More often, however, the informational requirements of winning and warning are in tension. Combat performance often hinges on well-kept secrets, feints, and diversions. Many military plans and capabilities degrade when revealed. National security involves trade-offs between the goals of preventing war, by advertising capabilities or interests, and improving fighting power should war break out, by concealing capabilities and surprising the enemy. The need to conceal details of the true balance of power to preserve battlefield effectiveness gives rise to the military commitment problem [79, 80]. Japan could not coerce the United States by revealing its plan to attack Pearl Harbor because the United States could not credibly promise to refrain from reorienting defenses and dispersing the Pacific Fleet. War resulted not just because of what opponents did not know but because of what they could not tell each other without paying a severe price in military advantage. The military benefits of surprise (winning) trumped the diplomatic benefits of coercion (warning). Cyber operations, whether for disruption and intelligence, are extremely constrained by the military commitment problem. Revelation of a cyber threat in advance that is specific enough to convince a target of the validity of the threat also provides enough information potentially to neutralize it. Stuxnet took years and hundreds of millions of dollars to develop but was patched within weeks of its discovery. The Snowden leaks negated a whole swath of tradecraft that the NSA took years to develop. States may use other forms of covert action, such as publicly disavowed lethal aid or aerial bombing (e.g. Nixon’s Cambodia campaign), to discretely signal their interests, but such cases can only work to the extent that revelation of operational details fails to disarm rebels or prevent airstrikes [81]. Cyber operations, especially against NC3, must be conducted in extreme secrecy as a condition of the efficacy of the attack. Cyber tradecraft relies on stealth, stratagem, and deception [21]. Operations tailored to compromise complex remote targets require extensive intelligence, planning and preparation, and testing to be effective. Actions that alert a target of an exploit allow the target to patch, reconfigure, or adopt countermeasures that invalidate the plan. As the Defense Science Board points out, competent network defenders: can also be expected to employ highly-trained system and network administrators, and this operational staff will be equipped with continuously improving network defensive tools and techniques (the same tools we advocate to improve our defenses). Should an adversary discover an implant, it is usually relatively simple to remove or disable. For this reason, offensive cyber will always be a fragile capability. [41] The world’s most advanced cyber powers, the United States, Russia, Israel, China, France, and the United Kingdom, are also nuclear states, while India, Pakistan, and North Korea also have cyber warfare programs. NC3 is likely to be an especially well defended part of their cyber infrastructures. NC3 is a hard target for offensive operations, which thus requires careful planning, detailed intelligence, and long lead-times to avoid compromise. Cyberspace is further ill-suited for signaling because cyber operations are complex, esoteric, and hard for commanders and policymakers to understand. Most targeted cyber operations have to be tailored for each unique target (a complex organization not simply a machine), quite unlike a general purpose munition tested on a range. Malware can fail in many ways and produce unintended side effects, as when the Stuxnet code was accidentally released to the public. The category of “cyber” includes tremendous diversity: irritant scams, hacktivist and propaganda operations, intelligence collection, critical infrastructure disruption, etc. Few intrusions create consequences that rise to the level of attacks such as Stuxnet or BlackEnergy, and even they pale beside the harm imposed by a small war. Vague threats are less credible because they are indistinguishable from casual bluffing. Ambiguity can be useful for concealing a lack of capability or resolve, allowing an actor to pool with more capable or resolved states and acquiring some deterrence success by association. But this works by discounting the costliness of the threat. Nuclear threats, for example, are usually somewhat veiled because one cannot credibly threaten nuclear suicide. The consistently ambiguous phrasing of US cyber declaratory policy (e.g. “we will respond to cyber-attacks in a manner and at a time and place of our choosing using appropriate instruments of U.S. power” [82]) seeks to operate across domains to mobilize credibility in one area to compensate for a lack of credibility elsewhere, specifically by leveraging the greater robustness to revelation of military capabilities other than cyber. This does not mean that cyberspace is categorically useless for signaling, just as nuclear weapons are not categorically useless for warfighting. Ransomware attacks work when the money extorted to unlock the compromised host is priced below the cost of an investigation or replacing the system. The United States probably gained some benefits in general deterrence (i.e. discouraging the emergence of challenges as opposed to immediate deterrence in response to a challenge) through the disclosure of Stuxnet and the Snowden leaks. Both revelations compromised tradecraft, but they also advertised that the NSA probably had more exploits and tradecraft where they came from. Some cyber operations may actually be hard to mitigate within tactically meaningful timelines (e.g. hardware implants installed in hard-to-reach locations). Such operations might be revealed to coerce concessions within the tactical window created by a given operation, if the attacker can coordinate the window with the application of coercion in other domains. As a general rule, however, the cyber domain on its own is better suited for winning than warning [83]. Cyber and nuclear weapons fall on extreme opposite sides of this spectrum. Dangerous complements Nuclear weapons have been used in anger twice—against the Japanese cities Hiroshima and Nagasaki—but cyberspace is abused daily. Considered separately, the nuclear domain is stable and the cyber domain is unstable. In combination, the results are ambiguous. The nuclear domain can bound the intensity of destruction that a cyber attacker is willing to inflict on an adversary. US declaratory policy states that unacceptable cyber attacks may prompt a military response; while nuclear weapons are not explicitly threatened, neither are they withheld. Nuclear threats have no credibility at the low end, where the bulk of cyber attacks occur. This produces a cross-domain version of the stability–instability paradox, where deterrence works at the high end but is not credible, and thus encourages provocation, at low intensities. Nuclear weapons, and military power generally, create an upper bound on cyber aggression to the degree that retaliation is anticipated and feared [22, 83, 84]. In the other direction, the unstable cyber domain can undermine the stability of nuclear deterrence. Most analysts who argue that the cyber–nuclear combination is a recipe for danger focus on the fog of crisis decision making [85–87]. Stephen Cimbala points out that today’s relatively smaller nuclear arsenals may perversely magnify the attractiveness of NC3 exploitation in a crisis: “Ironically, the downsizing of U.S. and post-Soviet Russian strategic nuclear arsenals since the end of the Cold War, while a positive development from the perspectives of nuclear arms control and nonproliferation, makes the concurrence of cyber and nuclear attack capabilities more alarming” [88]. Cimbala focuses mainly on the risks of **misperception** and **miscalculation** that emerge when a cyber attack muddies the **transparent communication** required for opponents to understand one another’s interests, redlines, and willingness to use force, and to ensure reliable control over subordinate commanders. Thus a nuclear actor “faced with a sudden burst of **holes** in its vital warning and response systems might, for example, press the **preemption button** instead of **waiting to ride out the attack and then retaliate**” [85]. The outcome of fog of decision scenarios such as these depend on how humans react to risk and uncertainty, which in turn depends on bounded rationality and organizational frameworks that might confuse rational decision making [89, 90]. These factors exacerbate a hard problem. Yet within a rationalist framework, cyber attacks that have already created their effects need not trigger an escalatory spiral. While being handed a fait accompli may trigger an aggressive reaction, it is also plausible that the target’s awareness that its NC3 has been compromised in some way would help to convey new information that the balance of power is not as favorable as previously thought. This in turn could encourage the target to accommodate, rather than escalate. While defects in rational decision making are a serious concern in any cyber–nuclear scenario, the situation becomes even more hazardous when there are rational incentives to escalate. Although “known unknowns” can create confusion, to paraphrase Donald Rumsfeld, the “unknown unknowns” are perhaps more dangerous. A successful clandestine penetration of NC3 can **defeat the informational symmetry that stabilizes nuclear relationships**. Nuclear weapons are useful for deterrence because they impose a degree of **consensus** about the distribution of power; each side knows the other can inflict prohibitive levels of damage, even if they may disagree about the precise extent of this damage. Cyber operations are attractive **precisely because they can secretly revise the distribution of power**. NC3 neutralization may be an expensive and rarified capability in the reach of only a few states with mature signals intelligence agencies, but it is much cheaper than nuclear attack. Yet the very usefulness of cyber operations for nuclear warfighting ensure that deterrence failure during brinksmanship crises is more likely. Nuclear states may initiate crises of risk and resolve to see who will back down first, which is not always clear in advance. Chicken appears viable, ironically, because each player understands that a nuclear war would be a disaster for all, and thus all can agree that someone can be expected swerve. Nuclear deterrence should ultimately make dealing with an adversary diplomatically more attractive than fighting, provided that fighting is costly—as would seem evident for the prospect of nuclear war—and assuming that bargains are available to states willing to accept compromise rather than annihilation. If, however, one side knows, but the other does not, that the attacker has disabled the target’s ability to perceive an impending military attack, or to react to one when it is underway, then they will not have a shared understanding of the probable outcome of war, even in broad terms. Consider a brinksmanship crisis between two nuclear states where only one has realized a successful penetration of the rival’s NC3. The cyber attacker knows that it has a military advantage, but it cannot reveal the advantage to the target, lest the advantage be lost. The target does not know that it is at a disadvantage, and it cannot be told by the attacker for the same reason. The attacker perceives an imbalance of power while the target perceives a balance. A dangerous competition in risk taking ensues. The first side knows that it does not need to back down. The second side feels confident that it can stand fast and raise the stakes far beyond what it would be willing to if it understood the true balance of power. Each side is willing to escalate to create more risk for the other side, making it more likely that one or the other will conclude that deterrence has failed and move into warfighting mode to attempt to limit the damage the other can inflict. The targeted nature and uncertain effects of offensive cyber operations put additional pressure on decision makers. An intrusion will probably disable only part of the enemy’s NC3 architecture, not all of it (which is not only operationally formidable to achieve but also more likely to be noticed by the target). Thus the target may retain control over some nuclear forces, or conventional forces. The target may be tempted to use some of them piecemeal to signal a willingness to escalate further, even though it cannot actually escalate because of the cyber operation. The cyber attacker knows that it has escalation dominance, but when even a minor demonstration by the target can cause great damage, it is tempting to preempt this move or others like it. This situation would be especially unstable if only second strike but not primary strike NC3 was incapacitated. Uncertainty in the efficacy of the clandestine penetration would discount the attacker’s confidence in its escalation dominance, with a range of possible outcomes. Enough uncertainty would discount the cyber attack to nothing, which would have a stabilizing effect by returning the crisis to the pure nuclear domain. A little bit of uncertainty about cyber effectiveness would heighten risk acceptance while also raising the incentives to preempt as an insurance measure. Adding allies into the mix introduces additional instability. An ally emboldened by its nuclear umbrella might run provocative risks that it would be much more reluctant to embrace if it was aware that the umbrella was actually full of holes. Conversely, if the clandestine advantage is held by the state extending the umbrella, allies could become unnerved by the willingness of their defender to run what appear to be outsize risks, oblivious of the reasons for the defender’s confidence, creating discord in the alliance and incentives for self-protective action, leading to greater uncertainty about alliance solidarity. The direction of influence between the cyber and nuclear realms depends to large degree on which domain is the main arena of action. Planning and conducting cyber operations will be bounded by the ability of aggressors to convince themselves that attacks will remain secret, and by the confidence of nuclear nations in their invulnerability. Fears of cross-domain escalation will tend to keep instability in cyberspace bounded. However, if a crisis has risen to the point where nuclear threats are being seriously considered or made, then NC3 exploitation will be destabilizing. Brinksmanship crises seem to have receded in frequency since the Cuban Missile Crisis but may be more likely than is generally believed. President Vladimir Putin of Russia has insinuated more than once in recent years that his government is willing to use tactical nuclear weapons if necessary to support his policies. Cyber power and nuclear stability Not all crises are the same. Indeed, their very idiosyncrasies create the uncertainties that make bargaining failure more likely [75]. So far our analysis would be at home in the Cold War, with the technological novelty of cyber operations. Yet not every state has the same cyber capabilities or vulnerabilities. Variation in cyber power relations across dyads should be expected to affect the strategic stability of nuclear states. The so-called second nuclear age differs from superpower rivalry in important ways [91]. There are fewer absolute numbers of warheads in the world, down from a peak of over 70 000 in the 1980s to about 15 000 today (less than 5000 deployed), but they are distributed very unevenly [92]. The United States and Russia have comparably sized arsenals, each with a fully diversified triad of delivery platforms, while North Korea only has a dozen or so bombs and no meaningful delivery system (for now). China, India, Pakistan, Britain, France, and Israel have modest arsenals in the range of several dozen to a couple hundred weapons, but they have very different doctrines, conventional force complements, domestic political institutions, and alliance relationships. The recent nuclear powers lack the hard-won experience and shared norms of the Cold War to guide them through crises, and even the United States and Russia have much to relearn. Cyber warfare capacity also varies considerably across contemporary nuclear nations. The United States, Russia, Israel, and Britain are in the top tier, able to run sophisticated, persistent, clandestine penetrations. China is a uniquely active cyber power with ambitious cyber warfare doctrine, but its operational focus is on economic espionage and political censorship, resulting in less refined tradecraft and more porous defenses for military purposes [16]. France, India, and Pakistan also have active cyber warfare programs, while North Korea is the least developed cyber nation, depending on China for its expertise [93]. It is beyond the scope of this article to assess crisis dyads in detail, and data on nuclear and cyber power for these countries are shrouded in secrecy. Here, as a way of summing up the arguments above, we offer a few conjectures about how stylized aspects of cyber power affect crisis stability through incentives and key aspects of decision making. We do not stress relative nuclear weapon capabilities on the admittedly strong (and contestable) assumption that nuclear transparency in the absence of cyber operations would render nuclear asymmetry irrelevant for crisis bargaining because both sides would agree about the terrible consequences of conflict [94]. We also omit domestic or psychological variables that affect relative power assessments, although these are obviously important. Even if neither India nor Pakistan have viable cyber–nuclear capabilities, brinksmanship between them is dangerous for many other reasons, notably compressed decision timelines, Pakistan’s willingness to shoot first, and domestic regime instability. Our focus is on the impact of offensive and defensive cyber power on nuclear deterrence above and beyond the other factors that certainly play a role in real-world outcomes. First, does the cyber attacker have the organizational capacity, technical expertise, and intelligence support to “compromise” the target’s NC3? Can hackers access critical networks, exploit technical vulnerabilities, and confidently execute a payload to disrupt or exploit strategic sensing, command, forces, or transport capacity? The result would be some tangible advantage for warfighting, such as tactical warning or control paralysis, but one that cannot be exercised in bargaining. Second, is the target able to “detect” the compromise of its NC3? The more complicated and sensitive the target, the more likely cyber attackers are to make a mistake that undermines the intrusion. Attribution is not likely to be difficult given the constricted pool of potential attackers, but at the same time the consequences of misattributing “false flag” operations could be severe [95]. At a minimum, detection is assumed to provide information to the target that the balance of power is perhaps not as favorable as imagined previously. We assume that detection without an actual compromise is possible because of false positives or deceptive information operations designed to create pessimism or paranoia. Third, is the target able to “mitigate” the compromise it detects? Revelation can prompt patching or network reconfiguration to block an attack, but this assumption is not always realistic. The attacker may have multiple pathways open or may have implanted malware that is difficult to remove in tactically meaningful timelines. In such cases the cyber commitment problem is not absolute, since the discovery of the power to hurt does not automatically disarm it. Successful mitigation here is assumed to restore mutual assessments of the balance of power to what they would be absent the cyber attack. Table 1 shows how these factors combine to produce different deterrence outcomes in a brinksmanship (chicken) crisis. If there is no cyber compromise and the target detects nothing (no false positives) then we have the optimistic ideal case where nuclear transparency affords stable “deterrence.” Transparency about the nuclear balance, including the viability of secure second strike forces, provides strategic stability. We also expect this box to describe situations where the target has excellent network defense capabilities and thus the prospect of defense, denial or deception successfully deters any attempts to penetrate NC3. This may resemble the Cold War situation (with electronic warfare in lieu of cyber), or even the present day US–Russia dyad, where the odds of either side pulling off a successful compromise against a highly capable defender are not favorable. Alternately the attack may be deemed risky enough to encourage serious circumspection. However, the existence of Canopy Wing does not encourage optimism in this regard. [[TABLE 1 OMITTED]] Conversely, if there is a compromise that goes undetected, then there is a heightened risk of “war” because of the cyber commitment problem. This box may be particularly relevant for asymmetric dyads such as the United States and North Korea, where one side has real cyber power but the other side is willing to go to the brink where it believes, falsely, that it has the capability to compel its counterpart to back down. Cyber disruption of NC3 is attractive for damage limitation should deterrence fail, given that the weaker state’s diminutive arsenal makes damage limitation by the stronger state more likely to succeed. The dilemma for the stronger state is that the clandestine counterforce hedge, which makes warfighting success more likely, is precisely what makes deterrence more likely to fail. The United States would face similar counterforce dilemmas with other dyads like China or even Russia, although even a strong cyber power should be more circumspect when confronted with an adversary with a larger/more capable nuclear and conventional arsenal. More complex and cyber savvy targets, moreover, are more likely to detect a breach in NC3, leading to more ambiguous outcomes depending on how actors cope with risk and uncertainty. Paradoxically, confidence in cyber security may be a major contributor to failure; believing one is safe from attack increases the chance that an attack is successful. If the successful compromise is detected but not mitigated, then the target learns that the balance of power is not as favorable as thought. This possibility suggests fleeting opportunities for “coercion” by revealing the cyber coup to the target in the midst of a crisis while the cyber attacker maintains or develops a favorable military advantage before the target has the opportunity to reverse or compensate the NC3 disruption. Recognizing the newly transparent costs of war, a risk neutral or risk averse target should prefer compromise. The coercive advantages (deterrence or compellence) of a detected but unmitigated NC3 compromise will likely be fleeting. This suggests a logical possibility for creating a window of opportunity for using particular cyber operations that are more robust to revelation as a credible signal of superior capability in the midst of a crisis. It would be important to exploit this fleeting advantage via other credible military threats (e.g. forces mobilized on visible alert or deployed into the crisis area) before the window closes. One side may be able gain an unearned advantage, an opportunity for coercion via a “bluff,” by the same window-of-opportunity logic. A target concerned about NC3 compromise will probably have some network monitoring system and other protections in place. Defensive systems can produce false positives as a result of internal errors or a deception operation by the attacker to encourage paranoia. It is logically possible that some false positives would appear to the target to be difficult to mitigate. In this situation, the target could believe it is at a disadvantage, even though this is not in fact the case. This gambit would be operationally very difficult to pull off with any reliability in a real nuclear crisis. Cyber–nuclear coercion and bluffing strategies are fraught with danger. Detection without mitigation might put a risk-acceptant or loss-averse target into a “use-lose” situation, creating pressures to preempt or escalate. The muddling of decision-making heightens the risk of accidents or irrational choices in a crisis scenario. Worry about preemption or accident then heightens the likelihood that the initiator will exercise counterforce options while they remain available. These pressures can be expected to be particularly intense if the target’s detection is only partial or has not revealed the true extent of damage to its NC3 (i.e. the target does not realize it has already lost some or all of what it hopes to use). These types of scenarios are most usually invoked in analyses of inadvertent escalation [23–27]. The essential distinction between “use-lose” risks and “war” in this typology is the target’s knowledge of some degree of NC3 compromise. Use-lose and other cognitive pressures can certainly result in nuclear war, since the breakdown of deterrence leads to the release of nuclear weapons, but we distinguish these outcomes to highlight the different decision making processes or rational incentives at work. A “spiral” of mistrust may emerge if one side attempts a compromise but the defender detects and mitigates it. Both sides again have common mutual estimates of the relative balance of power, which superficially resembles the “deterrence” case because the NC3 compromise is negated. Unfortunately, the detection of the compromise will provide the target with information about the hostile intentions of the cyber attacker. This in turn is likely to exacerbate other political or psychological factors in the crisis itself or in the crisis-proneness of the broader relationship. The strange logical case where there is no compromise but one is detected and mitigated could result from a false positive misperception (including a third-party false flag operation) that could conflict spiraling [96, 97]. The bluff and coercion outcomes are also likely to encourage spiraling behavior once the fleeting bargaining advantage dissipates or is dispelled (provided anyone survives the interaction). The risk of crisis instability is not the same for all dyads. It is harder to compromise the NC3 of strong states because of the redundancy and active defenses in their arsenal. Likewise, strong states are better able to compromise the NC3 of any states but especially of weaker states, because of strong states’ greater organizational capacity and expertise in cyber operations. Stable deterrence or MAD is most likely to hold in mutually strong dyads (e.g. the United States and the Soviet Union in the Cold War or **Russia** today to a lesser extent). Deterrence is slightly less likely in other equally matched dyads (**India–Pakistan**) where defensive vulnerabilities create temptations but offensive capabilities may not be sufficient to exploit them. Most states can be expected to refrain from targeting American NC3 given a US reputation for cyber power (a general deterrence benefit enhanced by Stuxnet and Snowden). The situation is less stable if the United States is the attacker. The most dangerous dyad is a stronger and a weaker state (United States and **North Korea** or **Israel** and **Iran**). Dyads involving strong and middle powers are also **dangerous** (United States and **China**). The stronger side is tempted to disrupt NC3 as a warfighting hedge in case deterrence breaks down, while the weaker but still formidable side has a reasonable chance at detection. The marginally weaker may also be tempted to subvert NC3, particularly for reconnaissance; the stronger side is more likely to detect and correct the intrusion but will be alarmed by the ambiguity in distinguishing intelligence collection from attack planning [98]. In a brinksmanship crisis between them, windows for coercion may be available yet fleeting, with real risks of spiral and war.

**OCOs escalate conflict---three warrants**

Rebecca **Slayton**, **2017**, (Rebecca; 2/2017; PhD in chemical biology from Harvard University, Masters in chemistry and chemical biology from Harvard University, Bachelor’s in chemistry from Westmont College, author of Arguments that Count: Physics, Computing, and Missile Defense, winner of the Computer History Museum Prize, author of Shadowing Cybersecurity, winner of a 5-year National Science Foundation CAREER award, project lead on research funded by the Department of Homeland Security Center of Excellence’s Critical Infrastructure Resilience Institute; “Why Cyber Operations Do Not Always Favor the Offense,” <https://www.belfercenter.org/sites/default/files/files/publication/Cyber%20Ops%20Offense%20-%20final.pdf>; Date Accessed: 7/10/2017/ceng

Creating Unnecessary Vulnerabilities Prioritizing offensive operations can **increase adversaries’ fears**, suspicions, and **readiness to take offensive action**. Cyber offenses include cyber exploitation (intelligence gathering) and cyberattack (disrupting, destroying, or subverting an adversary’s computer systems). An adversary can easily mistake defensive cyber exploitation for offensive operations because the distinction is a matter of intent, not technical operation. The difficulty of distinguishing between offensive and defensive tactics makes mistrustful adversaries **more reactive**, and repeatedly conducting offensive cyber operations only **increases distrust**. A focus on offensive operations can also **increase vulnerabilities**; for example, secretly stockpiling information about vulnerabilities in computers for later exploitation, rather than publicizing and helping civil society to mitigate those vulnerabilities, leaves critical infrastructure vulnerable to attack. The skills and organizational capabilities for offense and defense are very similar. Defense requires understanding how to compromise computer systems; one of the best ways to protect computer systems is to engage in penetration testing (i.e., controlled offensive operations on one’s own systems). The similarity between offensive and defensive skills makes it **unnecessary to conduct offensive operations** against adversaries to maintain offensive capability. Thus, rather than stockpiling technologies in the hope of gaining offensive advantage, states should develop the skills and organizational capabilities required to innovate and maintain information and communications technologies. Managing Complexity The complexity of information systems gives the offense certain advantages for purely probabilistic reasons. Imagine a race: offense and defense go hunting for randomly distributed vulnerabilities, with the offense attempting to exploit those vulnerabilities and the defense aiming to patch them. The number of vulnerabilities grows with the **size and complexity** of the computer system, as do the technological advantages of offense—at least in principle. With a vast number of vulnerabilities, it is **unlikely** that the defense will be able to find and patch every vulnerability before the offense finds and exploits it. Technology is, however, embedded in social organizations, and organizations can help the defense better manage complexity. Those that develop software can check for common errors before making hardware-software systems available for use. The defender has complete access to its computer system, whereas the attacker has a more limited set of attack vectors. Organizations can help skilled defenders by establishing good cybersecurity processes, such as continually scanning for vulnerabilities and updating software. Assessing Kinetic Effects To date, failures of cyber defense have largely been failures of management, and the successes of offense are a result of its relatively simpler goals. Offense, like defense, becomes more difficult as its goals become more complex. In particular, the advantages that complexity offers the offense in cyberspace diminish in the physical world. Computers controlling physical machinery can be hacked, but achieving particular physical effects, such as covertly sabotaging nuclear enrichment facilities, requires knowledge of the physical processes that the computers control, not merely knowledge of the computers. Much of the detailed knowledge needed to run an industrial control system is tacit, passed from one engineer to another but never written down, let alone stored on a computer. Gathering such information requires traditional espionage by humans on the ground, which is both expensive and risky. A cost-benefit analysis of Stuxnet for both the offense and the defense demonstrates why damaging physical infrastructure is **more costly** than simply infiltrating information networks. The costs of Stuxnet were likely far greater for the offense (the United States and Israel) than for the defense (Iran), and Stuxnet was relatively ineffective, setting back Iran’s nuclear program by fewer than three months. The great expense of Stuxnet was intelligence; though digital espionage can be used to obtain some kinds of information, the knowledge needed to disrupt a physical control system, such as the detailed methods and settings used to control pressure in Iran’s nuclear centrifuges, is not generally held in computers. The costs for both sides are dominated not by technology but by skilled labor—for example, hackers who identify and exploit zero-day vulnerabilities, systems administrators who manage and defend computer systems, and the nuclear engineers who understand enrichment processes and the means of disrupting them. In addition, assessing costs alone is misguided: the perceived benefits of attacking with and defending from Stuxnet (i.e., the value of Iran’s nuclear weapons program) greatly exceeded the costs for both the offense and the defense. This is one reason not to be complacent about the need to secure industrial control systems and critical infrastructure: though cyberattacks on such systems will be costly, a determined adversary may be **willing to pay the cost** to achieve its aims. Conclusion The common assumption that the offense dominates cyberspace is dangerous and deeply misguided. The offense-defense balance can be assessed only for specific operations, not for all of cyberspace, as it is shaped by the capabilities of adversaries and the complexity of their goals in any conflict. When it comes to exerting precise physical effects, cyberspace **does not offer overwhelming advantages** to the offense. Because the capabilities of offense and defense are similar, improving defensive operations allows preparation for cyber offense without **risking geopolitical instability** or increasing vulnerability to attack.

**It triggers an arms race---nuclear war**

Rebecca **Slayton**, **2017**, (Rebecca; 2/1/2017; PhD in chemical biology from Harvard University, Masters in chemistry and chemical biology from Harvard University, Bachelor’s in chemistry from Westmont College, author of Arguments that Count: Physics, Computing, and Missile Defense, winner of the Computer History Museum Prize, author of Shadowing Cybersecurity, winner of a 5-year National Science Foundation CAREER award, project lead on research funded by the Department of Homeland Security Center of Excellence’s Critical Infrastructure Resilience Institute; “What is the Cyber Offense-Defense Balance?” What Is the Cyber Offense-Defense Balance?” <https://cornell.app.box.com/s/58xm5d4xwbdjq549vx5xnwc3qu1dqybk>; Date Accessed: 7/10/2017/ceng

“In cyberspace, the offense has the upper hand.” 1 These words, written in 2010 by Deputy Secretary of Defense William Lynn, reflect conventional wisdom among military officers, policymakers, and scholars. 2 A minority of scholars disagree. 3 Nonetheless, the prevalent belief that cyberspace favors the offense has major consequences for **international security**. According to offense-defense theory, state perceptions that technology favors the offense increase fears of attack **encourage arms races**, and through interactions between fears and capabilities, **increase the likelihood and consequences of war**. 4 Overconfidence in the advantages of offense can create a “cult of the offensive” with potentially **tragic results**. 5 Many of these dynamics appear to be at work with cyber conflict. Military leaders perceive cyberspace as favoring the offense and are seeking more discretion to conduct offensive cyber operations. 6 Cyberattack features prominently in the U.S. intelligence community’s list of global threats. 7 In 2012 Defense Secretary Leon Panetta warned of a potential “cyber-Pearl Harbor.” 8 Fears of being hacked, optimism about hacking others, or both have spurred massive investments in military cyber operations around the world, suggesting a cyber arms race. 9 Because cyber operations can **blur lines** between espionage (or “cyber exploitation”) and use of force (or “cyberattack”), they create a “cybersecurity dilemma,” wherein network intrusions undertaken for defensive purposes are easily misunderstood as preparation for an attack, **creating the risk of escalation** and use of force. 10

**Kinetic warfare**

David **Gompert and** Martin **Libicki**, **2015**, (David and Martin; 7/22/2015; researcher @ RAND and Principal Deputy Director of National Intelligence from 2009 to 2010, PhD in economics from the University of California Berkeley and Master’s in city and regional planning from the University of California Berkeley; “Waging Cyber War the American Way,” http://www.tandfonline.com/doi/pdf/10.1080/00396338.2015.1068551; Date Accessed: 7/10/2017/ceng

US ambivalence toward cyber war is both strategic and normative, the implication being that what is bad for the United States is also bad for the world. Washington insists that any cyber operations it might conduct would be ‘in a manner **consistent with US and international law’**.5 Perceiving cyber war as war implies the applicability of the laws of war, specifically the principles of non-aggression, non-intervention, proportionality, discrimination and respect for neutrality.6 Compliance with all these norms could be **challenging** when initiating and conducting offensive cyber war. Case in point: the United States and Israel are said to have created and inserted the Stuxnet worm to interfere with the control of centrifuges used by Iran to enrich uranium. However justified by the imperative of preventing Iran from building nuclear weapons, it is fair to ask if this act of cyber war was lawful, especially in light of the unintended collateral effects it reportedly had. More broadly, harming non-combatants and civilian life, which can occur when infecting non-military computer systems, raises especially vexing issues, at least for the United States – thus its defensive posture. There are **several obvious reasons** for US wariness about offensive cyber war. Firstly, US military, intelligence, economic, governmental and societal functions are **highly dependent on computer systems**, and vulnerable to their disruption and degradation. Put starkly, having led and benefited enormously from the ‘digital revolution’, the United States regards cyber war as counter-revolutionary. Moreover, once begun, the course a cyber war might take would be **hard to predict, control or contain**. It could trigger **kinetic hostilities**, visit indiscriminate harm on non-combatants, escalate far beyond what the belligerents intended, and cause grave economic damage.7 Finally, US superiority in conventional military capabilities limits the need for cyber war, whereas enemies could use cyber war as an asymmetric answer to such superiority. In other words, cyber war could level the battlefield to the US disadvantage.

**Prefer our evidence---the risks outweigh any potential benefit**

Jon **Lindsay** **and** Erik **Gartzke**, **2016**, (Jon and Erik; 8/25/2016; assistant professor of digital media and international affairs at the Univesrity of Toronto and PhD in political science form the Massachusetts Institute of Technology and wrote China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, professor of political science at the University of California San Diego and Director of cPASS; “Coercion through Cyberspace: The Stability-Instability Paradox Revisited,” <http://deterrence.ucsd.edu/_files/LindsayGartzke_CoercionThroughCyberspace_DraftPublic1.pdf>; Date Accessed: 7/10/2017/ceng

In contemporary defense policy discourse there are three **influential narratives** of mounting cyber peril, corresponding roughly to the three operational modes of attack, exploitation, and defense. The most dangerous scenarios envision the paralysis of industrial control systems or military command and control through surprise attack by anonymous hackers. The imagined aggressor may be 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, warning instead of the long term erosion of economic and military competitiveness drained away through persistent computer espionage. The relentless theft of vital secrets stored on corporate and government networks produces a “death by a thousand cuts” as states give their firms an unfair commercial advantage and equip their military forces with potent countermeasures to U.S. strengths. In both of these scenarios, commercial hacking tools and ubiquitous connectivity give weaker states and terrorists provide a **potent means** to exploit and attack the expanding attack surface of digitally-dependent advanced industrial states. A third 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.15 At the other extreme, authoritarian governments censor internet content and reconfigure internet governance to undermine the internet’s potential for innovation and freedom. State paranoia about the threats of paralysis and erosion thus leads to digital lockout or “the end of the internet” as we know it.16 Threats of catastrophic attack, omniscient exploitation, and unassailable defense are myths because they imagine major rewards for little cost. The actual rewards of any given cyber campaign are **rarely so great** and the costs are rarely so trivial. Potential benefits of attack are **discounted by uncertainty** about the true value of the target to the adversary and the ability for the attacker to take advantage of it. **Operative costs** include the bureaucratic resources, development and testing requirements, human capital, and intelligence experience required to plan and run an effective covert cyber campaign. Setting aside the myths of low costs and high rewards (no free lunch), there are a variety of more realistic cyber operations with significant variation in their operative costs and benefits. A set of higher cost, and, potentially, higher reward complements enhance the capabilities of stronger actors who can master them. A much larger set of low cost, low reward irritants are available to weaker actors or even solitary individuals, but they provide only a small marginal return on a small investment.

**US-Russia war is the *only* scenario for extinction---simulations prove**

Ellen **Ioanes** **and** Dave **Mosher**, 01-23-**2020**, (Ellen Ioanes is the Military & Defense Editorial Fellow at INSIDER. She is a graduate of Columbia Journalism School and Davidson College. Her work appears in the Guardian, the Center for Public Integrity, the Daily Dot, HuffPost India, and more. Dave Mosher reports news and features stories about science and technology, with human and robotic spaceflight as the primary focus of his 15-year multimedia journalism career.), “A terrifying new animation shows how 1 'tactical' nuclear weapon could trigger a US-Russia war that kills 34 million people in 5 hours”, Business Insider, https://www.businessinsider.com/tactical-nuclear-weapons-escalation-us-russia-war-animated-strike-map-2019-9/ceng

More than 91 million people in Russia, the US, and NATO-allied countries might be killed or injured within three hours following a single "nuclear warning shot," according to a terrifying new simulation. The simulation is called "Plan A," and it's an audio-visual piece that was first posted to to YouTube on September 6. (You can watch the full video at the end of this story.) Researchers at the Science and Global Security lab at Princeton University created the animation, which shows how a battle between Russia and NATO allies that uses so-called low-yield or "tactical" nuclear weapons — which can pack a blast equivalent to those the US used to destroy Hiroshima or Nagasaki in World War II — might feasibly and quickly snowball into a global nuclear war. "This project is motivated by the need to highlight the potentially catastrophic consequences of current US and Russian nuclear war plans. **The risk of nuclear war has increased dramatically in the past two years**," the project states on its website. The video has an ominous, droning soundtrack and a digital map design straight out of the 1983 movie "WarGames." The Cold War-era movie, in which a young Matthew Broderick accidentally triggers a nuclear war, "was exactly the reference point," simulation designer Alex Wellerstein told Insider. But while simulations can be frightening, they can also be incredibly helpful: governments can use them to develop contingency plans to respond to nuclear disasters and attacks in the least escalatory way, and they can also help ordinary citizens learn how to survive a nuclear attack. "Plan A" comes as tensions between Russia and NATO allies ratchet up. Both Russia and the US are testing weapons previously banned under the Intermediate-range Nuclear Forces treaty, often called INF. Russian bombers have also cruised into US airspace repeatedly, and the US recently sent its B-2 Spirit stealth bomber on a mission **in the Arctic** — right in Russia's backyard. This is how a NATO-Russian confrontation could quickly escalate into nuclear war. The simulation starts with a conventional war between NATO and Russian troops. Conventional warfare — namely all conflict short of nuclear, chemical or biological weapons — escalates into nuclear warfare when Russia launches a nuclear "warning shot" from a base near Kaliningrad **to stop NATO advancement**. Russia doesn't have a "no first use" policy — it dropped it in 1993. NATO forces respond by launching a tactical nuclear strike. The US already has tactical nuclear weapons, such as B61-12 gravity bombs, and more planned under US President Donald Trump's 2018 Nuclear Posture Review. Included in the plan is a low-yield warhead intended for use in a submarine-launched ballistic missile, as well as a sea-launched cruise missile. These kinds of weapons are designed for targets on the battlefield, like troops or munitions supplies, as opposed to long- or intermediate-range nuclear missiles that are fired from one country to another, for example, targeting an enemy's bombers and ICBM silos — or even cities. Tactical nuclear strikes up the ante. If the nuclear threshold is crossed, the simulation finds, then both the US and Russia would respond with tactical nuclear weapons. Russia would send 300 warheads to NATO targets, including advancing troops, in both aircraft and short-range missiles — overwhelming force that would obliterate tanks, fortified positions and soldiers unlike anything ever seen in battle before. Supporting forces and civilians not immediately killed would be susceptible to painful and even fatal radiation exposure. NATO would respond by sending about 180 tactical nuclear weapons to Russia via aircraft in equally devastating retaliation. The simulation was constructed using independent analysis of nuclear force postures in NATO countries and Russia, including the availability of nuclear weapons, their yields, and possible targets, according to the Science and Global Security lab. The tactical phase of the simulation shows about **2.6 million casualties over three hours**. Instead of the tactical weapons de-escalating the conflict, as proponents claim they would, **the simulation shows conflict spiraling out of control** after the use of tactical weapons. Russia's tactical weapons would destroy much of Europe, the simulation posits. In response, NATO would launch submarine- and US-based strategic nuclear weapons toward Russia's nuclear arsenals — 600 warheads in total. Strategic nuclear weapons have a longer range, so Russia, knowing that NATO nukes are headed for its weapons cache, would throw all its weight behind missiles launched from silos, mobile launchers, and submarines. The casualties during this phase would be 3.4 million in 45 minutes. This leads to 85.3 million additional casualties in the final phase of the nuclear war simulation. In the wake of previous attacks, both Russia and NATO would launch warheads toward each other's 30 most populous cities in the final stage of of the scenario, using five to 10 warheads for each city depending on its size. This phase would cause 85.3 million casualties — both deaths and injuries. But the total casualty count from the entire battle (of less than 5 hours) would be 34.1 million deaths and 57.4 million injuries, or a combined 91.3 million casualties overall. **But that's just the immediate conflict**: The entire world would be affected by nuclear disaster in the months, years, and decades to come. The radioactive fallout from the nuclear disaster would cause additional deaths and injuries. Studies also suggest that, even with a limited nuclear engagement, Earth's atmosphere would cool dramatically, driving famine, refugee crises, additional conflicts, and more deaths.

**Turns every impact**

**Starr 17** [Steven Starr is the director of the University of Missouri's Clinical Laboratory Science Program, as well as a senior scientist at the Physicians for Social Responsibility, 1-9-2017, "Turning a Blind Eye Towards Armageddon — U.S. Leaders Reject Nuclear Winter Studies," FAS, [https://fas.org/2017/01/turning-a-blind-eye-towards-armageddon-u-s-leaders-reject-nuclear-winter-studies]](https://fas.org/2017/01/turning-a-blind-eye-towards-armageddon-u-s-leaders-reject-nuclear-winter-studies%5d)

The detonation of an atomic bomb with this explosive power will instantly ignite fires over a surface area of three to five square miles. In the recent studies, the scientists calculated that the blast, fire, and radiation from a war fought with 100 atomic bombs could produce direct fatalities comparable to all of those worldwide in World War II, or to those once estimated for a “counterforce” nuclear war between the superpowers. However, the long-term environmental effects of the war could significantly disrupt the **global weather** for at least a decade, which would likely result in a **vast global famine**. The scientists predicted that nuclear **firestorms** in the burning cities would cause at least five million tons of **black carbon smoke** to quickly rise above cloud level into the stratosphere, where it could not be rained out. The smoke would circle the Earth in less than two weeks and would form a **global** stratospheric smoke **layer** that would remain for more than a **decade**. The smoke would absorb warming **sunlight**, which would heat the smoke to temperatures near the boiling point of water, producing **ozone losses** of 20 to 50 percent over populated areas. This would almost double the amount of UV-B reaching the most populated regions of the mid-latitudes, and it would create UV-B indices **unprecedented in** ~~human~~ [humyn} history. In North America and Central Europe, the time required to get a painful sunburn at mid-day in June could decrease to as little as six minutes for fair-skinned individuals. As the smoke layer blocked warming sunlight from reaching the Earth’s surface, it would produce the **cold**est average surface **temperatures** in the last 1,000 years. The scientists calculated that global food production would decrease by 20 to 40 percent during a five-year period following such a war. Medical experts have predicted that the shortening of growing seasons and corresponding decreases in agricultural production could cause up to **two billion** people to **perish** from famine. The climatologists also investigated the effects of a nuclear war fought with the vastly more powerful modern thermonuclear weapons possessed by the United States, Russia, China, France, and England. Some of the thermonuclear weapons constructed during the 1950s and 1960s were 1,000 times more powerful than an atomic bomb. During the last 30 years, the average size of thermonuclear or “strategic” nuclear weapons has decreased. Yet today, each of the approximately 3,540 strategic weapons deployed by the United States and Russia is seven to 80 times more powerful than the atomic bombs modeled in the India-Pakistan study. The smallest strategic nuclear weapon has an explosive power of 100,000 tons of TNT, compared to an atomic bomb with an average explosive power of 15,000 tons of TNT. Strategic nuclear weapons produce much larger nuclear firestorms than do atomic bombs. For example, a standard Russian 800-kiloton warhead, on an average day, will ignite fires covering a surface area of 90 to 152 square miles. A war fought with hundreds or thousands of **U.S. and Russian** strategic nuclear weapons would ignite immense nuclear firestorms covering land surface areas of many thousands or tens of thousands of square miles. The scientists calculated that these fires would produce up to 180 million tons of black carbon soot and smoke, which would form a dense, global stratospheric smoke layer. The smoke would remain in the stratosphere for 10 to 20 years, and it would block as much as 70 percent of sunlight from reaching the surface of the Northern Hemisphere and 35 percent from the Southern Hemisphere. So much sunlight would be blocked by the smoke that the noonday sun would resemble a full moon at midnight. Under such conditions, it would only require a matter of days or weeks for daily minimum temperatures to fall **below freezing in the largest agricultural areas** of the Northern Hemisphere, where freezing temperatures would occur every day for a period of between one to more than two years. Average surface temperatures would become colder than those experienced 18,000 years ago at the height of the last Ice Age, and the prolonged cold would cause average rainfall to decrease by up to 90%. Growing seasons would be completely eliminated for more than a decade; it would be too cold and dark to grow food crops, which would **doom the majority of the ~~human~~ [humyn] population**. NUCLEAR WINTER IN BRIEF The profound cold and darkness following nuclear war became known as nuclear winter and was first predicted in 1983 by a group of NASA scientists led by Carl Sagan. During the mid-1980s, a large body of research was done by such groups as the Scientific Committee on Problems of the Environment (SCOPE), the World Meteorological Organization, and the U.S. National Research Council of the U.S. National Academy of Sciences; their work essentially supported the initial findings of the 1983 studies. The idea of nuclear winter, published and supported by prominent scientists, generated extensive public alarm and put political pressure on the United States and Soviet Union to reverse a runaway nuclear arms race, which, by 1986, had created a global nuclear arsenal of more than 65,000 nuclear weapons. Unfortunately, this created a backlash among many powerful military and industrial interests, who undertook an extensive media campaign to brand nuclear winter as “bad science” and the scientists who discovered it as “irresponsible.” Critics used various uncertainties in the studies and the first climate models (which are primitive by today’s standards) as a basis to criticize and reject the concept of nuclear winter. In 1986, the Council on Foreign Relations published an article by scientists from the National Center for Atmospheric Research, who predicted drops in global cooling about half as large as those first predicted by the 1983 studies and described this as a “nuclear autumn.” The nuclear autumn studies were later shown to be deeply flawed, but the proof came too late to stop a massive smear campaign that effectively discredited the initial studies. Nuclear winter was subject to criticism and damning articles in the Wall Street Journal and Time magazine. In 1987, the National Review called nuclear winter a “fraud.” In 2000, Discover Magazine published an article that described nuclear winter as one of “The Twenty Greatest Scientific Blunders in History.” The endless smear campaign was successful; the general public, and even most anti-nuclear activists, were left with the idea that nuclear winter had been scientifically disproved. REJECTION BY LEADERS Yet the scientists did not give up. In 2006, they returned to their labs to perform the research I have previously described. Their new research not only upheld the previous findings but also found that the earlier studies actually underestimated the environmental effects of nuclear war. Dr. Robock of Rutgers and Dr. Toon of the University of Colorado have spent years attempting to bring official attention to their work and get follow-up research studies done by appropriate agencies in the federal government. In a recent (2016) interview, Dr. Toon stated: The Department of Energy and the Department of Defense, which should be investigating this problem, have done absolutely nothing. They have not published a single paper, in the open literature, analyzing this problem … We have made a list of where we think the important issues are, and we have gone to every [federal] agency we can think of with these lists, and said “Don’t you think someone should study this?” Basically, everyone we have tried so far has said, “Well that’s not my job.” In the same interview, Dr. Robock also noted: The Department of Homeland Security really should fund this. They will fund you to study one terrorist bomb in New York City. When you explain to them that a war between India and Pakistan is a much greater threat to the U.S. homeland than one terrorist bomb, as horrible as that is, they respond with “Oh, well that’s not my job, go talk to some other program manager” — who, of course, doesn’t exist. After the more recent series of studies were published in 2007 and 2008, Drs. Robock and Toon also made a number of requests to meet with members of the Obama administration. The scientists offered to brief Cabinet members and the White House staff about their findings, which they assumed would have a great impact upon nuclear weapons policy. Their offers were met with indifference. Finally, after several years of trying, Drs. Robock and Toon were allowed an audience with John Holdren, Senior Advisor to President Barack Obama on Science and Technology. Dr. Robock also eventually met with Rose Gottemoeller, then Under Secretary of State for Arms Control and International Security. Dr. Robock has written to me that, after these meetings, he and Dr. Toon were left with the impression that neither Holdren nor Gottemoeller think the nuclear winter research “is correct.” But it is not only Holdren and Gottemoeller who reject the nuclear winter research. Greg Mello, of the Los Alamos Study Group, cites a source who confirms that the group that determines the “full range of activities related to the development, production, maintenance (upkeep) and elimination (retirement, disassembly and disposal) of all United States nuclear weapons — the members of the U.S. Nuclear Weapons Council — have stated that “the predictions of nuclear winter were disproved years ago.” The members of the U.S. Nuclear Weapons Council include: Under Secretary of Defense for Acquisition, Technology, and Logistics Vice ~~Chairman~~ [Chairperson} of the Joint Chiefs of Staff Under Secretary for Nuclear Security of the Department of Energy Under Secretary of Defense for Policy Commander of the United States Strategic Command It is important to understand that some members of this group — especially the Commander of the U.S. Strategic Command (USSTRATCOM) — also develop the policies that guide the use of nuclear weapons. Perhaps General John Hyten, Head of USSTRATCOM, who is in charge of the U.S. nuclear triad, and General Paul Selva, Vice ~~Chairman~~ [Chairperson] of the Joint Chiefs of Staff, the second highest ranking officer in the United States, have never seen or heard of the 21st century nuclear winter studies. Perhaps when they hear a question about “nuclear winter,” they only remember the smear campaigns done against the early studies. Or, maybe, they just choose not to accept the new scientific research on nuclear winter, despite the fact that it has withstood the criticism of the global scientific community. Regardless, the rejection of nuclear winter research by the top leaders of the United States raises some profoundly important questions: Do U.S. military and political leaders fully understand the consequences of nuclear war? Do they realize that even a “successful” nuclear first-strike against Russia could cause most Americans to die from nuclear famine? In 2010, Drs. Toon and Robock wrote in Physics Today: We estimate that the direct effects of using the 2012 arsenals would lead to hundreds of millions of fatalities. The indirect effects would likely eliminate the majority of the ~~human~~ [humyn] population. In 2013, Drs. Toon and Robock wrote in the Bulletin of Atomic Scientists that: A nuclear war between Russia and the United States, even after the arsenal reductions planned under New START, could produce a nuclear winter. Hence, an attack by either side could be suicidal, resulting in Self-Assured Destruction. RENEWED COLD WAR Although president-elect Trump appears to favor a return to the policy of détente with Russia, many if not most U.S. political leaders appear to support the Obama administration’s policies of direct confrontation with Putin’s Russia. Mainstream corporate media, including the editorial boards of The New York Times and The Washington Post, routinely engage in anti-Russian and anti-Putin rhetoric that surpasses the hate speech of the McCarthy era. Under President Obama, the United States has renewed the **Cold War** with Russia, with little or no debate or protest, and has subsequently engaged in **proxy wars** with Russia in **Ukraine and Syria,** as well as threatening **military action against China** in the **South China Sea**. In response to what NATO leaders describe as Russia’s “dangerous and aggressive actions,” NATO has built up a **“rapid-response force”** of 40,000 troops on the Russian border in the Baltic States and Poland. This force includes hundreds of tanks, armored vehicles, and heavy artillery. NATO troops stationed in Estonia are within **artillery range of St. Petersburg**, the second largest city of Russia. The United States has deployed its **Aegis** Ashore Ballistic Missile Defense (**BMD**) system in **Romania** and is constructing another such BMD system in **Poland**. The Mark 41 launch system used in the Aegis Ashore systems can be used to launch a variety of missiles, including **long-range nuclear-armed cruise missiles**. In other words, the United States has built and is building **launch sites for nuclear missiles on the Russian border**. This fact has been widely reported on Russian TV and has infuriated the Russian public. In June, Russian President Putin specifically warned that Russia would be **forced to retaliate** against this threat. While Russian officials maintain that its actions are normal and routine, Russia now appears to be **preparing for war**. On October 5, 2016, Russia conducted a nation-wide civil defense drill that included 40 million of its people being directed to fallout shelters. Reuters reported two days later that Russia had moved its Iskander nuclear-capable missiles to **Kaliningrad**, which borders Poland. While the United States ignores the danger of nuclear war, Russian scholar Stephen Cohen reports that the danger of war with the United States is the leading news story in Russia. Cohen states: Just as there is no discussion of the most existential question of our time, in the American political class — the possibility of war with Russia — it is the only thing being discussed in the Russian political class . . . These are two different political universes. In Russia, all the discussion in the newspapers, and there is plenty of free discussion on talk show TV, which echoes what the Kremlin is thinking, online, in the elite newspapers, and in the popular broadcasts, the number 1, 2, 3, and 4 topics of the day are the possibility of war with the United States. Cohen goes on to say: I conclude from this that the leadership of Russia **actually believes** now, in reaction to what the United States and NATO have said and done over the last two years, and particularly in reaction to the breakdown of the proposed cooperation in Syria, and the rhetoric coming out of Washington, that **war is a real possibility**. I can’t remember when, since the Cuban Missile Crisis, that the Moscow leadership came to this conclusion in its collective head. Perhaps this narrative will change under president-elect Trump. However, he is inheriting a situation **fraught with danger**, which retains the possibility of **direct military conflict** with **Russia in Ukraine and Syria**, as well as increasingly militarized confrontation with **China in the South China Sea**.

### 1AC – Solvency

**But the plan solves**

**NW**, **2011**, “Ban on offensive cyber operations needed”, NATO Watch, https://natowatch.org/default/2011/ban-offensive-cyber-operations-needed/ceng

Russia’s call for NATO to launch an investigation into the computer worm that targeted a Russian-built Iranian nuclear power plant deserves a response. Claims that the incident could have triggered a new Chernobyl are probably exaggerated, but an investigation is certainly warranted. Indeed, a joint Russia-NATO investigation might be beneficial, especially if it were also to review the 2007 cyber attacks against Estonia (2007) and Georgia (2008). The New York Times has reported that US and Israeli intelligence services collaborated to develop the destructive computer worm in a bid to sabotage Iran's efforts to make a nuclear bomb. No smoking Russian state gun has ever been found in relation to the attacks on Estonia, although evidence points to coordination among Russian professional computer specialists and chat sites that were exhorted on the blogosphere to attack Estonian sites. The question of who masterminded the attack itself has been reverberating for several years, with many fingers pointing at the Kremlin, but without any evidence to substantiate these claims. A joint NATO-Russian analysis of both the Stuxnet and Estonia/Georgia cyber attacks would be an exemplary case of cooperative security in action. But don’t expect it to happen any time soon. The rattling of cyber skeletons inside both the Kremlin and Pentagon will see to that. In addition, the opinion pages in America have been full of praise for the “bloodless cyber warfare attack” on Iran, which is hardly surprising given the domestic support for other remote technological fixes in the US arsenal, such as armed drones. But just as those have blowback consequences, the moving of malware from the domain of civilian black-hats to full-bore military weaponry also has the potential to threaten us in return. As the Los Angeles Times points out “it's hard to ignore the signs that a new kind of arms race has started”. This is troubling for at least two reasons: **we don't know how existing international laws and treaties that govern conventional conflicts would apply to cyber war, if at all, and second, our crucial infrastructure is highly vulnerable to attacks from cyberspace. In an increasingly interconnected world, it's hard to tell where the cyber battlefield begins and ends.** It is clear, however, that the US Defence Department is carrying out clandestine cyber activities with very little oversight by lawmakers, a situation that is almost certainly mirrored across several other NATO member states as well as other major powers, like Russia, India and China. The US military's use of offensive cyber warfare has only rarely been disclosed, the most well-known instance being the electronic jamming of Iraqi military and communications networks in advance of the ‘shock and awe’ attack in 2003. It seems highly likely that the US military is also involved in offensive military cyber activities in Afghanistan, Yemen and several other countries where it is supporting counterinsurgency or counterterrorism operations. The Pentagon has also centralized its cyberspace operations within a Cyber Command that became fully operational in October last year. It is also clear that the US is making most of the running in developing cyber security partnerships with NATO and the EU. Hungary's Gabor Iklody is the point person on emerging security challenges for NATO, including cyber security, heading up a new office opened last August. The Lisbon Summit in November and NATO’s new Strategic Concept also identified cyber security as a priority and commit the Alliance to bringing a NATO cyber-incident response organization fully online by 2012 and to centralize NATO cyber security. The declaration also included commitments to develop an in-depth cyber defence policy by June 2011 and prepare an action plan for its implementation. One of Ambassador Iklody’s first tasks should be to clearly define the parameters of offensive and defensive cyber operations and explore how NATO might contribute towards an international ban on offensive cyber attacks, or at minimum, a ‘no-first use policy’ akin to that adopted by some nuclear weapon states (but not NATO). He will first be required to remove the blinkers and address a significant obstacle to international cooperation in this area: that a major source of cyber attacks and a major spur to the cyber arms race resides within NATO itself.

## 2AC

### 2AC---OCOs Fail

#### OCOs fail---too costly

Smeets ’22, Max; Feb 23; Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich, co-founder and Director of the European Cyber Conflict Research Initiative (ECCRI.eu), an organization promoting the interdisciplinary study of cyber conflict and statecraft in Europe and beyond, also an Affiliate at Stanford University Center for International Security and Cooperation; Security Studies, “Cyber Arms Transfer: Meaning, Limits, and Implications,” vol. 31/ceng

An offensive cyber organization will also need attack tools to achieve a certain effect or goal. Payloads greatly vary in size. On one end of the spectrum, they can come as very lightweight files that are easy to distribute, but once executed they will trigger the download of a much larger piece of malware.43 On the other end of the spectrum, payloads can be multiple megabytes (MBs) in size. A multipurpose toolkit was discovered in 2012 by researchers from Kaspersky Lab, which they called Flame. Whereas the Stuxnet code is “only” about 1 MB in size, Flame’s malware code is about twenty times larger—and still not fully understood.44 It is difficult—and cost inefficient—to build an arsenal of tools for a more mature cyber command or intelligence agency. Although early development and stockpiling would be desirable to ensure swift deployment if the need arises, tools often must be tailored to the target and desired effect (especially if the actor desires stealth and stability), which means that in-time development is often necessary. Consider, for example, a case in which the leadership of a command decides there is a need to target a specific programmable logic controller (PLC) used to run a certain manufacturing process. The developers will likely have to build tools that can work on that particular PLC model. If leadership subsequently decides to target a different process, developers will have to deploy a new toolset. Finally, the more features of the target you can use, the less you need yourself. Napoleon was famous for making sure his troops were living off the land through which they moved. It allowed his army to travel light and march long distances. This notion of living off the land is also commonly applied to cyber operations. The attacker may use something exotic to get into a target’s network, but it makes a lot of sense to subsequently use the target’s existing infrastructure to gain further network access. For example, existing communication lines to push out notifications can be used to move through an organization’s network. Living off the land is not merely done for cost-efficiency benefits. The practice is equally, if not more, important for remaining undetected. Fourth, to effectively run cyber operations an organization requires infrastructure, broadly defined as the processes, structures, and facilities needed to pull off an offensive cyber operation. This element can be split into two categories: control infrastructure and preparatory infrastructure. Control infrastructure refers to processes directly used to run an operation. This is also the type of infrastructure that is generally burned down after a failed operation. It includes domain names of phishing sites, leaked email addresses, or other abused technologies.45 It also concerns C&C infrastructure used in remotely conducted operations to maintain communication with compromised systems within a target network. Depending on an operation’s goal and resources, the C&C infrastructure might be as basic as a single server operating on the external network.46 At the same time, an organization may run a whole set of operations simply to compromise legitimate web servers to use them for C&C later.

### 2AC---OCOs cause miscalc

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

Brandon Valeriano and Benjamin Jensen, 19, (Brandon Valeriano and Benjamin Jensen, Brandon Valeriano Senior Fellow, Cato Institute Benjamin Jensen Professor of Strategic Studies, School of Advanced Warfighting at the Marine Corps University, 1-15-2019, Cato Institute, The Myth of the Cyber Offense: The Case for Restraint, https://www.cato.org/policy-analysis/myth-cyber-offense-case-restraint#notes, 6-26-2022) SCade

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

### 2AC---Use of Force

#### Response to cyber operations as a “use of force” creates disproportionate military actions – that escalates to war

Wenqing Zhao, 20, (Wenqing Zhao, 2020, A New Paradigm of Non-Intervention, https://jilp.law.ucdavis.edu/issues/volume-27-1/27.1\_ZHAO.pdf, 6-25-2022) SCade

\*CDOs = cyber disinformation operations

A. Victim States of CDOs Have No Legal Recourse in the United Nations Charter Article 2(4) The lawfulness of resorting to military measures, the jus ad bellum, is regulated by the Charter of United Nations Article 2(4). Article 2(4) provides that “all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state.”48 No definitions are provided in the Charter, however, for the key terms, “use of force” and “political independence,” except for a mentioning in the preamble that one purpose of the Charter is to “ensure…that armed force shall not be used, save in the common interest.”49 It is altogether unclear if “use of force” in Article 2(4) implies a use of armed force, and it would be imprudent to draw such a definite conclusion as arguments were made that use of force is “a large category of activities containing a smaller subset of events that qualify as armed subset.”50 CDOs, while capable of asserting broad influence on the target states, can hardly fall under the category of armed force. Furthermore, a CDO rarely amount to a “use of force,” even when the term arguably covers operations less grave than armed force. Regardless of the scope of use of force, incursions into a nation’s political independence in the form of CDOs have an “ostensibly peaceful” façade that is non-belligerent in nature, and therefore are “seldom broadly accepted as uses of force.”51 The worry of counting CDOs as “use of force,” other than it is counter-intuitive to the plain language, is that the effect of CDOs might be disproportionate to that of belligerent military actions (the traditional understanding of “use of force”). Consequently, counting CDOs as “use of force” might trigger a state’s countermeasures disproportionate to what CDOs deserve, in forms of draconian economic sanctions or even military actions, especially when the effect of CDOs is extremely hard to measure as I will discuss in later sections.

#### Attacks ensures tit-for-tat retaliation – that creates nuclear escalation---both sides retaliate.

Michael T. Klare, 19, (Michael T. Klare, Michael T. Klare is a professor emeritus of peace and world security studies at Hampshire College and senior visiting fellow at the Arms Control Association. This is the fourth in the “Arms Control Tomorrow” series, in which he considers disruptive emerging technologies and their implications for war-fighting and arms control., 11-1-2019, Arms Control Association, Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation, https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#bio, 6-26-2022) SCade

The danger here is that economic attacks of this sort, if undertaken during a period of tension and crisis, could lead to an escalating series of tit-for-tat attacks against ever more vital elements of an adversary’s critical infrastructure, producing widespread chaos and harm and eventually leading one side to initiate kinetic attacks on critical military targets, risking the slippery slope to nuclear conflict. For example, a Russian cyberattack on the U.S. power grid could trigger U.S. attacks on Russian energy and financial systems, causing widespread disorder in both countries and generating an impulse for even more devastating attacks. At some point, such attacks “could lead to major conflict and possibly nuclear war.”14

### 2AC: AT: Regulate CP

#### Setting a standard for cyberattacks greenlights lower level attacks that escalate

Michael Horowitz, 10, (Michael Horowitz, Horowitz is an Assistant professor of political science at the University of Pennsylvania and a senior fellow at the Foreign Policy Research Institute. He has also held fellowships at the Olin Institute for Strategic Studies at Harvard, the Belfer Center for Science and International Affairs at Harvard, and the Weatherhead Center for International Affairs at Harvard, October 2010, “A Common Future? NATO and the Protection of the Commons”. Transatlantic Paper Series No. 3, https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/Trans-Atlantic\_Papers\_3-Horowitz.pdf, 6-26-2022) SCade

One option is to lay out a specific policy that would be a part of the Strategic Concept and that describes the sort of cyber attack that is damaging enough to trigger an Article 5 commitment from other NATO member states. The risk of such a specific declaration is that it could “green light” lower level attacks by guaranteeing that they would not trigger a NATO response. The advantage of a specific policy is that it sets up a clear red line for potential adversaries and potentially deters more dangerous types of cyber attacks. Bureaucratically, clear guidance about responding to cyber attacks could facilitate rapid responses in a crisis and prevent dangerous delays that place the security of member states at risk. While individual NATO member states are capable of acting quickly, NATO as an institution, like many institutions, works more slowly. Having preset procedures in place to govern the response to a cyber attack could help NATO members effectively coordinate in a crisis.

### 2AC---Expansion

#### Ukraine is a result of NATO expansion – further expansion to cyber or AI would result in further Russian war---the aff is key to deescalating

Ted Galen Carpenter, 22, (Ted Galen Carpenter, Ted Galen Carpenter is senior fellow for defense and foreign policy studies at the Cato Institute. Carpenter served as Cato’s director of foreign policy studies from 1986 to 1995 and as vice-president for defense and foreign policy studies from 1995 to 2011, 2-28-2022, Guardian, Many predicted Nato expansion would lead to war. Those warnings were ignored, https://www.theguardian.com/commentisfree/2022/feb/28/nato-expansion-war-russia-ukraine, 6-25-2022) SCade

Russia’s military offensive against Ukraine is an act of aggression that will make already worrisome tensions between Nato and Moscow even more dangerous. The west’s new cold war with Russia has turned hot. Vladimir Putin bears primary responsibility for this latest development, but Nato’s arrogant, tone‐​deaf policy toward Russia over the past quarter‐​century deserves a large share as well. Analysts committed to a US foreign policy of realism and restraint have warned for more than a quarter‐​century that continuing to expand the most powerful military alliance in history toward another major power would not end well. The war in Ukraine provides definitive confirmation that it did not. Thinking through the Ukraine crisis – the causes “It would be extraordinarily difficult to expand Nato eastward without that action’s being viewed by Russia as unfriendly. Even the most modest schemes would bring the alliance to the borders of the old Soviet Union. Some of the more ambitious versions would have the alliance virtually surround the Russian Federation itself.” I wrote those words in 1994, in my book Beyond Nato: Staying Out of Europe’s Wars, at a time when expansion proposals merely constituted occasional speculation in foreign policy seminars in New York and Washington. I added that expansion “would constitute a needless provocation of Russia”. What was not publicly known at the time was that Bill Clinton’s administration had already made the fateful decision the previous year to push for including some former Warsaw Pact countries in Nato. The administration would soon propose inviting Poland, the Czech Republic and Hungary to become members, and the US Senate approved adding those countries to the North Atlantic Treaty in 1998. It would be the first of several waves of membership expansion. Even that first stage provoked Russian opposition and anger. In her memoir, Madeleine Albright, Clinton’s secretary of state, concedes that “[Russian president Boris] Yeltsin and his countrymen were strongly opposed to enlargement, seeing it as a strategy for exploiting their vulnerability and moving Europe’s dividing line to the east, leaving them isolated.” Strobe Talbott, deputy secretary of state, similarly described the Russian attitude. “Many Russians see Nato as a vestige of the cold war, inherently directed against their country. They point out that they have disbanded the Warsaw Pact, their military alliance, and ask why the west should not do the same.” It was an excellent question, and neither the Clinton administration nor its successors provided even a remotely convincing answer. George Kennan, the intellectual father of America’s containment policy during the cold war, perceptively warned in a May 1998 New York Times interview about what the Senate’s ratification of Nato’s first round of expansion would set in motion. “I think it is the beginning of a new cold war,” Kennan stated. ”I think the Russians will gradually react quite adversely and it will affect their policies. I think it is a tragic mistake. There was no reason for this whatsoever. No one was threatening anybody else.” He was right, but US and Nato leaders proceeded with new rounds of expansion, including the provocative step of adding the three Baltic republics. Those countries not only had been part of the Soviet Union, but they had also been part of Russia’s empire during the Czarist era. That wave of expansion now had Nato perched on the border of the Russian Federation. Moscow’s patience with Nato’s ever more intrusive behavior was wearing thin. The last reasonably friendly warning from Russia that the alliance needed to back off came in March 2007, when Putin addressed the annual Munich security conference. “Nato has put its frontline forces on our borders,” Putin complained. Nato expansion “represents a serious provocation that reduces the level of mutual trust. And we have the right to ask: against whom is this expansion intended? And what happened to the assurances our western partners made after the dissolution of the Warsaw Pact?” In his memoir, Duty, Robert M Gates, who served as secretary of defense in the administrations of both George W Bush and Barack Obama, stated his belief that “the relationship with Russia had been badly mismanaged after [George HW] Bush left office in 1993”. Among other missteps, “US agreements with the Romanian and Bulgarian governments to rotate troops through bases in those countries was a needless provocation.” In an implicit rebuke to the younger Bush, Gates asserted that “trying to bring Georgia and Ukraine into Nato was truly overreaching”. That move, he contended, was a case of “recklessly ignoring what the Russians considered their own vital national interests”. The following year, the Kremlin demonstrated that its discontent with Nato’s continuing incursions into Russia’s security zone had moved beyond verbal objections. Moscow exploited a foolish provocation by Georgia’s pro‐​western government to launch a military offensive that brought Russian troops to the outskirts of the capital. Thereafter, Russia permanently detached two secessionist‐​minded Georgian regions and put them under effective Russian control. Western (especially US) leaders continued to blow through red warning light after a red warning light, however. The Obama administration’s shockingly arrogant meddling in Ukraine’s internal political affairs in 2013 and 2014 to help demonstrators overthrow Ukraine’s elected, pro‐​Russia president was the single most brazen provocation, and it caused tensions to spike. Moscow immediately responded by seizing and annexing Crimea, and a new cold war was underway with a vengeance. Could the Ukraine crisis have been avoided? Events during the past few months constituted the last chance to avoid a hot war in eastern Europe. Putin demanded that Nato provide guarantees on several security issues. Specifically, the Kremlin wanted binding assurances that the alliance would reduce the scope of its growing military presence in eastern Europe and would never offer membership to Ukraine. He backed up those demands with a massive military buildup on Ukraine’s borders. The Biden administration’s response to Russia’s quest for meaningful western concessions and security guarantees was tepid and evasive. Putin then clearly decided to escalate matters. Washington’s attempt to make Ukraine a Nato political and military pawn (even absent the country’s formal membership in the alliance) may end up costing the Ukrainian people dearly. The Ukraine tragedy History will show that Washington’s treatment of Russia in the decades following the demise of the Soviet Union was a policy blunder of epic proportions. It was entirely predictable that Nato expansion would ultimately lead to a tragic, perhaps violent, breach of relations with Moscow. Perceptive analysts warned of the likely consequences, but those warnings went unheeded. We are now paying the price for the US foreign policy establishment’s myopia and arrogance.

### 2AC---AI Arms Race Bad

#### The narrative of an AI arms race is false and actively perpetuates increased risks of unsafe AI being launched

Paul Scharre, 19, (Paul Scharre, 6-1-2019, Foreign Affairs, Killer Apps, https://www.foreignaffairs.com/articles/2019-04-16/killer-apps?check\_logged\_in=1&amp;utm\_medium=promo\_email&amp;utm\_source=lo\_flows&amp;utm\_campaign=registered\_user\_welcome&amp;utm\_term=email\_1&amp;utm\_content=20220626, 6-26-2022) SCade

The nation that leads in the development of artificial intelligence will, Russian President Vladimir Putin proclaimed in 2017, “become the ruler of the world.” That view has become commonplace in global capitals. Already, more than a dozen governments have announced national AI initiatives. In 2017, China set a goal of becoming the global leader in AI by 2030. Earlier this year, the White House released the American AI Initiative, and the U.S. Department of Defense rolled out an AI strategy. But the emerging narrative of an “AI arms race” reflects a mistaken view of the risks from AI—and introduces significant new risks as a result. For each country, the real danger is not that it will fall behind its competitors in AI but that the perception of a race will prompt everyone to rush to deploy unsafe AI systems. In their desire to win, countries risk endangering themselves just as much as their opponents. AI promises to bring both enormous benefits, in everything from health care to transportation, and huge risks. But those risks aren’t something out of science fiction; there’s no need to fear a robot uprising. The real threat will come from humans. Right now, AI systems are powerful but unreliable. Many of them are vulnerable to sophisticated attacks or fail when used outside the environment in which they were trained. Governments want their systems to work properly, but competition brings pressure to cut corners. Even if other countries aren’t on the brink of major AI breakthroughs, the perception that they’re rushing ahead could push others to do the same. And if a government deployed an untested AI weapons system or relied on a faulty AI system to launch cyberattacks, the result could be disaster for everyone involved. Policymakers should learn from the history of computer networks and make security a leading factor in AI design from the beginning. They should also ratchet down the rhetoric about an AI arms race and look for opportunities to cooperate with other countries to reduce the risks from AI. A race to the bottom on AI safety is a race no one would win.

#### AI is already being misused – further rushed development only hampers it more

Paul Scharre, 19, (Paul Scharre, 6-1-2019, Foreign Affairs, Killer Apps, https://www.foreignaffairs.com/articles/2019-04-16/killer-apps?check\_logged\_in=1&amp;utm\_medium=promo\_email&amp;utm\_source=lo\_flows&amp;utm\_campaign=registered\_user\_welcome&amp;utm\_term=email\_1&amp;utm\_content=20220626, 6-26-2022) SCade

AUTOCRATIC INTELLIGENCE

Harm from AI misuse isn’t hypothetical; it’s already here. Bots are regularly used to manipulate social media, amplifying some messages and suppressing others. Deepfakes, AI-generated fake videos, have been used in so-called revenge porn attacks, in which a person’s face is digitally grafted onto the body of a pornographic actor. These examples are only the start. Political campaigns will use AI-powered data analytics to target individuals with political propaganda tailored just for them. Companies will use the same analytics to design manipulative advertising. Digital thieves will use AI tools to create more effective phishing attacks. Bots will be able to convincingly impersonate humans online and over the phone by cloning a person’s voice with just a minute of audio. Any interaction that isn’t in person will become suspect. Security specialists have shown that it’s possible to hack into autonomous cars, disabling the steering and brakes. Just one person could conceivably hijack an entire fleet of vehicles with a few keystrokes, creating a traffic jam or launching a terrorist attack. AI’s power as a tool of repression is even more frightening. Authoritarian governments could use deepfakes to discredit dissidents, facial recognition to enable round-the-clock mass surveillance, and predictive analytics to identify potential troublemakers. China has already started down the road toward digital authoritarianism. It has begun a massive repression campaign against the Muslim Uighur population in Xinjiang Province. Many of the tools the government is using there are low tech, but it has also begun to use data analytics, facial recognition systems, and predictive policing (the use of data to predict criminal activity). Vast networks of surveillance cameras are linked up to algorithms that can detect anomalous public behavior, from improperly parked vehicles to people running where they are not allowed. The Chinese company Yuntian Lifei Technology boasts that its intelligent video surveillance system has been deployed in nearly 80 Chinese cities and has identified some 6,000 incidents related to “social governance.” Some of the ways in which Chinese authorities now use AI seem trivial, such as tracking how much toilet paper people use in public restrooms. Their proposed future uses are more sinister, such as monitoring patterns of electricity use for signs of suspicious activity.

#### China AI norms are being exported – must be countered

Paul Scharre, 19, (Paul Scharre, 6-1-2019, Foreign Affairs, Killer Apps, https://www.foreignaffairs.com/articles/2019-04-16/killer-apps?check\_logged\_in=1&amp;utm\_medium=promo\_email&amp;utm\_source=lo\_flows&amp;utm\_campaign=registered\_user\_welcome&amp;utm\_term=email\_1&amp;utm\_content=20220626, 6-26-2022) SCade

AI’s power as a tool of repression is even more frightening. Authoritarian governments could use deepfakes to discredit dissidents, facial recognition to enable round-the-clock mass surveillance, and predictive analytics to identify potential troublemakers. China has already started down the road toward digital authoritarianism. It has begun a massive repression campaign against the Muslim Uighur population in Xinjiang Province. Many of the tools the government is using there are low tech, but it has also begun to use data analytics, facial recognition systems, and predictive policing (the use of data to predict criminal activity). Vast networks of surveillance cameras are linked up to algorithms that can detect anomalous public behavior, from improperly parked vehicles to people running where they are not allowed. The Chinese company Yuntian Lifei Technology boasts that its intelligent video surveillance system has been deployed in nearly 80 Chinese cities and has identified some 6,000 incidents related to “social governance.” Some of the ways in which Chinese authorities now use AI seem trivial, such as tracking how much toilet paper people use in public restrooms. Their proposed future uses are more sinister, such as monitoring patterns of electricity use for signs of suspicious activity. China is not just building a techno-dystopian surveillance state at home; it has also begun exporting its technology. In 2018, Zimbabwe signed a deal with the Chinese company CloudWalk Technology to create a national database of faces and install facial recognition surveillance systems at airports, railway stations, and bus stops. There’s more than money at stake in the deal. Zimbabwe has agreed to let CloudWalk send data on millions of faces back to China, helping the company improve its facial recognition systems for people with dark skin. China also plans to sell surveillance technology in Malaysia, Mongolia, and Singapore. China is exporting its authoritarian laws and policies, too. According to Freedom House, China has held training sessions with government officials and members of the media from over 30 countries on methods to monitor and control public opinion. Three countries—Tanzania, Uganda, and Vietnam—passed restrictive media and cybersecurity laws soon after engaging with China.

#### The best move is to not play in the arms race at all

Paul Scharre, 19, (Paul Scharre, 6-1-2019, Foreign Affairs, Killer Apps, https://www.foreignaffairs.com/articles/2019-04-16/killer-apps?check\_logged\_in=1&amp;utm\_medium=promo\_email&amp;utm\_source=lo\_flows&amp;utm\_campaign=registered\_user\_welcome&amp;utm\_term=email\_1&amp;utm\_content=20220626, 6-26-2022) SCade

THE ONLY WINNING MOVE IS NOT TO PLAY Today’s AI technologies are powerful but unreliable. Rules-based systems cannot deal with circumstances their programmers did not anticipate. Learning systems are limited by the data on which they were trained. AI failures have already led to tragedy. Advanced autopilot features in cars, although they perform well in some circumstances, have driven cars without warning into trucks, concrete barriers, and parked cars. In the wrong situation, AI systems go from supersmart to superdumb in an instant. When an enemy is trying to manipulate and hack an AI system, the risks are even greater. Even when they don’t break down completely, learning systems sometimes learn to achieve their goals in the wrong way. In a research paper last year, a group of 52 AI researchers recounted dozens of times when AI systems showed surprising behavior. An algorithm learning to walk in a simulated environment discovered it could move fastest by repeatedly falling over. A Tetris-playing bot learned to pause the game before the last brick fell, so that it would never lose. One program deleted the files containing the answers against which it was being evaluated, causing it to be awarded a perfect score. As the researchers wrote, “It is often functionally simpler for evolution to exploit loopholes in the quantitative measure than it is to achieve the actual desired outcome.” Surprise seems to be a standard feature of learning systems. Machine-learning systems are only ever as good as their training data. If the data don’t represent the system’s operating environment well, the system can fail in the real world. In 2018, for example, researchers at the MIT Media Lab showed that three leading facial recognition systems were far worse at classifying dark-skinned faces than they were at classifying light-skinned ones. When they fail, machine-learning systems are also often frustratingly opaque. For rules-based systems, researchers can always explain the machine’s behavior, even if they can’t always predict it. For deep-learning systems, however, researchers are often unable to understand why a machine did what it did. Ali Rahimi, an AI researcher at Google, has argued that much like medieval alchemists, who discovered modern glassmaking techniques but did not understand the chemistry or physics behind their breakthroughs, modern machine-learning engineers can achieve powerful results but lack the underlying science to explain them. Every failing of an AI system also presents a vulnerability that can be exploited. In some cases, attackers can poison the training data. In 2016, Microsoft created a chatbot called Tay and gave it a Twitter account. Other users began tweeting offensive messages at it, and within 24 hours, Tay had begun parroting their racist and anti-Semitic language. In that case, the source of the bad data was obvious. But not all data-poisoning attacks are so visible. Some can be buried within the training data in a way that is undetectable to humans but still manipulates the machine. Even if the creators of a deep-learning system protect its data sources, the system can still be tricked using what are known as “adversarial examples,” in which an attacker feeds the system an input that is carefully tailored to get the machine to make a mistake. A neural network classifying satellite images might be tricked into identifying a subtly altered picture of a hospital as a military airfield or vice versa. The change in the image can be so small that the picture looks normal to a human but still fools the AI. Adversarial examples can even be placed in physical objects. In one case, researchers created a plastic turtle with subtle swirls embedded in the shell that made an object identification system think it was a rifle. In another, researchers placed a handful of small white and black squares on a stop sign, causing a neural network to classify it as a 45-mile-per-hour speed-limit sign. To make matters worse, attackers can develop these kinds of deceptive images and objects without access to the training data or the underlying algorithm of the system they are trying to defeat, and researchers have struggled to find effective defenses against the threat. Unlike with cybersecurity vulnerabilities, which can often be patched once they are uncovered, there is no known way of fully inoculating algorithms against these attacks. Governments already have plenty of experience testing military, cyber-, and surveillance tools, but no testing method can guarantee that complex systems won’t experience glitches once they’re out in the real world. The first time F-22 fighter jets crossed the International Date Line, their computers crashed and the aircraft were nearly stranded over the Pacific Ocean. Testing AI systems often takes even more time and money than testing traditional military hardware. Their complexity, which makes them more capable, also creates more opportunities for unexpected glitches. Imagine that a government develops an AI system that can hack into its adversaries’ computer networks while avoiding detection. The first government to deploy such a system would gain a huge advantage over its competitors. Worried that an adversary was developing a similar tool, the government might feel compelled to cut testing short and deploy the system early. This dynamic has already played out in other industries, such as self-driving cars. The consequences of accidents caused by national security AI tools could be far worse. AI wouldn’t be the first case of governments relying on a powerful but unsafe technology. That’s exactly what happened with computers, which play critical roles in everything from trading stocks to guiding missiles even though they suffer from enormous vulnerabilities. In 2018, investigators at the U.S. Government Accountability Office found that U.S. weapons systems were riddled with cybersecurity loopholes that could be exploited with “relatively simple tools and techniques.” Even worse, Defense Department program managers didn’t know about the problems and dismissed the GAO’s findings, claiming the tests were not realistic. Computer security vulnerabilities aren’t limited to government-run systems. Company after company has suffered major data breaches. Digital security is already too often an afterthought. A world of widespread, unprotected AI systems isn’t just a possibility; it’s the default setting.

### 2AC---AT: OCO Intel & OCO Good

#### US pledging OCOs for NATO military use disrupts their intelligence gathering capabilities – makes them exclusively used to hack targets not gather intel

Trey Herr, 18, (Trey Herr, Trey Herr is a 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., 10-10-2018, Council on Foreign Relations, Sharing is Caring: The United States’ New Cyber Commitment for NATO, https://www.cfr.org/blog/sharing-caring-united-states-new-cyber-commitment-nato, 6-26-2022) SCade

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.

### 2AC---AT: AI Arms Race Fake

#### Even if AI doesn’t reach the level of an Arms Race – their author concedes there are risks in investing into AI more

Paul Scharre, 21, (Paul Scharre, 6-29-2021, Center for New American Security , Debunking the AI Arms Race Theory, https://www.cnas.org/publications/commentary/debunking-the-ai-arms-race-theory, 6-26-2022) SCade

In 2015, a group of prominent AI and robotics researchers signed an open letter warning of the dangers of autonomous weapons. “The key question for humanity today,” they wrote, “is whether to start a global AI arms race or to prevent it from starting. If any major military power pushes ahead with AI weapon development, a global arms race is virtually inevitable.”1 Today, many nations are working to apply AI for military advantage, and the term “AI arms race” has become a catchphrase used by both critics and proponents of AI militarization. In 2018, then-Under Secretary of Defense Michael Griffin, calling for the United States to invest more in AI, stated, “There might be an artificial intelligence arms race, but we’re not yet in it.”2 In a 2020 Wired article, Will Roper, then chief acquisition officer for the U.S. Air Force, warned of the risks of falling behind in a “digital arms race with China.”3 The so-called AI arms race has become a common feature in news headlines,4 but the arms race framing fails to match reality. While nations are clearly competing to develop and adopt AI technology for military use, the character of that competition does not meet the traditional definition of an arms race. Military AI competition nevertheless does pose risks. The widespread adoption of military AI could cause warfare to evolve in a manner that leads to less human control and to warfare becoming faster, more violent, and more challenging in terms of being able to manage escalation and bring a war to an end. Additionally, perceptions of a “race” to field AI systems before competitors do could cause nations to cut corners on testing, leading to the deployment of unsafe AI systems that are at risk of accidents that could cause unintended escalation or destruction. Even if fears of an “AI arms race” are overblown, military AI competition brings real risks to which nations should attend. There are concrete steps nations can take to mitigate some of these dangers.

### 2AC – Russian Deterrence Disad Answers (Impact Defense)

#### No meltdowns impact

Shellenberger 19 – Michael, author, environmental policy writer, cofounder of Breakthrough Institute and founder of Environmental Progress, Time Magazine “Hero of the Environment”. “It Sounds Crazy, But Fukushima, Chernobyl, And Three Mile Island Show Why Nuclear Is Inherently Safe”, Forbes, <https://www.forbes.com/sites/michaelshellenberger/2019/03/11/it-sounds-crazy-but-fukushima-chernobyl-and-three-mile-island-show-why-nuclear-is-inherently-safe/#5b4a65ff1688>, 03-11-2019

In other words, **the main lesson** that should be drawn **from the worst nuclear accidents is that nuclear energy has always been inherently safe**. The truth about nuclear power’s safety is so shocking that it’s worth taking a closer look at the worst accidents, starting with the worst of the worst: Chernobyl. The nuclear plant is in Ukraine which, in 1986, the year of the accident, was a Soviet Republic. Operators lost control of an unauthorized experiment that resulted in the reactor catching fire. There was no containment dome, and the fire spewed out radioactive particulate matter, which went all over the world, leading many to conclude that Chernobyl is not just the worst nuclear accident in history but is also the worst nuclear accident possible. Twenty-eight firefighters died after putting out the Chernobyl fire. While the death of any firefighter is tragic, it’s worth putting that number in perspective. Eighty-six firefighters died in the U.S. in 2018, and 343 firefighters died during the September 11, 2001 terrorist attacks. Since the Chernobyl accident, 19 first responders have died, according to the United Nations, for ”various reasons” including tuberculosis, cirrhosis of the liver, heart attacks, and trauma. The U.N. concluded that “the assignment of radiation as the cause of death has become less clear.” What about cancer? By 2065 there may be 16,000 thyroid cancers; to date there have been 6,000. Since thyroid cancer has a mortality rate of just one percent — it is an easy cancer to treat — expected deaths may be 160. The World Health Organization claims on its web site **that Chernobyl could result in the premature deaths of 4,000 people**, but according to Dr. Geraldine Thomas, who started and runs the Chernobyl Tissue Bank, that number **is based on a disproven methodology**. “**That** WHO **number is based on LNT,”** she explained, using the acronym for the “linear no-threshold” method of extrapolating deaths from radiation. LNT assumes that there is no threshold below which radiation is safe, but **that** assumption **has been discredited over recent decades by multiple sources of data.** Support for the idea that radiation is harmless at low levels comes from the fact that people who live in places with higher background radiation, like Colorado, do not suffer elevated rates of cancer. In fact, **residents of Colorado, where radiation is higher because of** high concentrations of **uranium in the ground, enjoy** some of **the lowest cancer rates in** the U.S. Even relatively high doses of radiation cause far less harm than most people think. Careful, large, and long-term studies of survivors of the atomic bombings of Hiroshima and Nagasaki offer compelling demonstration. **Cancer rates were just 10 percent higher among atomic blast survivors, most of whom never got cancer**. Even those who received a dose 1,000 times higher than today’s safety limit saw their lives cut short by an average of 16 months. But didn’t the Japanese government recently award a financial settlement to the family of a Fukushima worker who claimed his cancer was from the accident? It did, but for reasons that were clearly political, and having to do with the Japanese government’s consensus-based, conflict-averse style, as well as lingering guilt felt by elite policymakers toward Fukushima workers and residents, who felt doubly aggrieved by the tsunami and meltdowns. The worker’s cancer was highly unlikely to have come from Fukushima because, once again, the level of radiation workers received was far lower than the ones received by the Hiroshima/Nagasaki cohort that saw (modestly) higher cancer rates. What about **Three Mile Island?** After the accident in 1979, Time Magazine ran a cover story that superimposed a glowing headline, “Nuclear Nightmare,” over an image of the plant. **Nightmare? More like a dream. What other major industrial technology can suffer a catastrophic failure and not kill anyone?** Remember when the Deepwater Horizon oil drilling rig caught on fire and killed 11 people? Four months later, a Pacific Gas & Electric natural gas pipeline exploded just south of San Francisco and killed eight people sleeping in their beds. And that was just one year, 2010. The worst energy accident of all time was the 1975 collapse of the Banqiao hydroelectric dam in China. It collapsed and killed between 170,000 and 230,000 people. **Nuclear’s** worst **accidents show** that **the technology has always been safe** for the same, inherent reason that it has always had such a small environmental impact: the high energy density of its fuel. **Splitting atoms to create heat**, rather than than splitting chemical bonds through fire, **requires tiny amounts of fuel**. A single Coke can of uranium can provide enough energy for an entire high-energy life. **When the worst occurs, and the fuel melts, the amount of** particulate **matter that escapes** from the plant **is insignificant** in contrast to both the fiery explosions of fossil fuels and the daily emission of particulate matter from fossil- and biomass-burning homes, cars, and power plants, which kill seven million people a year. It's not that nuclear energy never kills. It's that **nuclear's death toll is vanishingly small**. Consider nuclear's global death toll in context. These are just annual deaths. - walking: 270,000 - driving: 1,350,000 - working: 2,300,000 - air pollution: 4,200,000 By contrast, **nuclear's death total is** likely to be **around 200**.

#### No Nuclear Meltdowns – countries have learned from Fukushima and Chernobyl implementing safety defenses – failure is increasingly unlikely because nuclear detonations are stopped – that’s Shellenberger

#### No risk of meltdowns.

ALEXANDER **SAMMON**, DECEMBER 5, 20**19**, [Alexander Sammon is a staff writer at The American Prospect.], “The Tantalizing Nuclear Mirage”, The American Prospect, <https://prospect.org/greennewdeal/the-tantalizing-nuclear-mirage/>, Xoxo 6/4/2020.

To hear Booker tell it, his evolution on the subject was the product of scientific rigor and anti-ideological clarity on decarbonization. He related this narrative during a media blitz, comparing anti-nuclear Democrats to Republican climate deniers over their rejection of an **incontrovertible science**, while pledging to usher in a nuclear future that no right-minded person could deny. “Where the science is going, to me, at first sounded like science fiction … **new nuclear actually portends** of exciting things where you have **no risk of the kinds of meltdowns we’re seeing**,” he proclaimed at CNN’s climate town hall. Grandiosity aside, Booker isn’t alone in his **nuclear embrace. He’s part of an unlikely pro-nuclear political alliance, an emergent accord that spans the centrist think tank Third Way**, Andrew Yang, Jay Inslee, environmental activists, and progressive commentators alike. “The left should stop worrying and **learn to love existing nuclear power plants**,” wrote New York’s Eric Levitz in a subsequent send-up of Bernie Sanders’s and Elizabeth Warren’s twin commitments to phase out the technology. In a world where the rapid deployment of zero-carbon energy production is urgent, nuclear power, the argument goes, represents the only proven bet. As **it stands, nuclear is currently the largest single source of near-zero-carbon energy generation in the United States, providing 20 percent of our total energy mix**. And **while the waste may be dangerous**, and th**e risks associated with meltdowns cinematically seared into our collective memory, the technology is actually safer than burning fossil fuels**—**one study found that per unit of electricity generated, oil is 263 times more deadly than nuclear,** on account of air pollution alone. With 11 years, per the U.N.’s 2018 IPCC report, to overhaul our energy system, to be serious about decarbonization is to find a place at the table for nuclear. It’s an alluring idea. Already, this logic has been embraced in states like Ohio and Booker’s New Jersey, which have been allocating green tax subsidies to nuclear projects. And while it’s largely played out in the background, the question of what to do about nuclear has vexed Green New Dealers since the rollout of Alexandria Ocasio-Cortez’s framework in February. While plane travel and hamburgers raised hackles in the press, one of the first clauses to be deleted from the initial proposal pledged to phase out the technology altogether. So does the Green New Deal need nuclear to achieve its lofty goals? Does zero-carbon energy infrastructure necessitate a nuclear buildout, or at least an embrace of already-existing nuclear as a bridge fuel, as countries like Sweden have done? Unfortunately, the case for nuclear as a green technology is not so simple—the technology faces a spate of environmental and economic challenges, while its track record as a bridge fuel shows it may be more rivalrous than concomitant with renewables. In fact, it may be the nuclear industry that needs the Green New Deal, not the other way around. DESPITE THE NEWFOUND exigency of overhauling the country’s energy mix, this is not the first time America’s energy system has arrived at a crossroads in the last ten years, nor is it the first time nuclear has been trotted out as its last, best hope. In the late aughts, with oil prices soaring and production stagnant, policymakers made a commitment to expanding American nuclear generation. An era of so-called “nuclear renaissance” began, with four **next-generation reactors commissioned** at two plants, one in Georgia and the other in South Carolina. Since nuclear energy was first announced as a civilian project in 1953, its promises of worldwide abundance have far outpaced its production. Now, over a decade later, that project managed to bankrupt its construction company, Westinghouse, nearly taking down the entire Toshiba conglomerate, Westinghouse’s parent company, with it. The two reactors in South Carolina were abandoned, while the Southern Nuclear and Georgia Power utility companies assumed control of the remaining two reactors in Georgia, the Vogtle 3 and 4. But even a cash infusion from Georgia ratepayers, who began subsidizing the completion of the project in 2011, was not enough to keep the project close to its budget or timeline. Initially expected to come online in 2016-2017, the Vogtle plant has run some $14 billion over budget. Its completion dates have been deferred to 2021-2022. There’s currently no other active nuclear development in the United States. That timeline should be particularly alarming for nuclear enthusiasts. If it’s going to take 10 to 15 years to see a plant through to completion, even with massive financial backing, that’s seemingly impossible to square with the 11 years to decarbonize. At the very least, we’d need hundreds, if not thousands of plants already under construction just to make a dent. Booker, Yang, and other advocates are betting that **R&D might accelerate that process,** but in a real sense it’s already too late. So if new construction can’t be counted on, and the window for adding new nuclear to the fleet has already shut, what about the reactors we currently have? Has their environmental potential gotten short shrift? While nuclear fission emits far less carbon dioxide than energy production by oil and gas, the process of getting to that energy generation complicates nuclear’s claim to zero-carbon status. Uranium mining, processing, and transport are all carbon-intensive procedures done by diesel-powered heavy machinery. Instead of carbon, the plants themselves emit heat, often in great quantities, which can warm nearby air and water dramatically, killing fish and wildlife and afflicting neighboring habitats. And while nuclear may maintain a cleaner sheet than fossil fuels when it comes to CO2, its record on H2O is less rosy. An American nuclear plant can require between 19 million and 1.4 billion gallons of water a day, just for purposes of cooling. Because of that implacable thirst, it’s imperative that **nuclear plants are constructed near major water sources.** Thus, nuclear plants dot our rivers and coastline, each of which carries with it its own climate-specific challenges. Plants built near abundant freshwater—rivers and lakes—have been forced to contend with the twin challenges of too much water and not enough. In recent years, nuclear reactors, like those on the Great Lakes, **have been forced to shut down when droughts have plagued rivers and lakes, reducing water levels to perilous lows.** Meanwhile, in places like Nebraska, flood risks have necessitated shutdowns. And in France, which sports one of the most robust nuclear programs in the world, heat waves have caused **water temperatures to surge to the point of shutdowns multiple summers in a row.**