We negate resolved: The benefits of the United States Federal Government's use of offensive cyber operations outweigh the harms.

Our Sole Contention is Escalation.

Historically the US's cyber policy has largely been defensive, developing offensive capabilities but limiting its use to avoid escalation.

However, Dilanian of CNBC '19 writes that new policies passed under Trump have shifted the focus of US cyber ops to constantly engaging our enemies rather than sitting on the sidelines.

This is extremely dangerous. Jensen of the Cato Institute '19 cautions that this divergence of US policy risks upsetting the peace of the past, and increasing the risk of escalation.

This happens for three reasons.

First is through inadvertent signaling.

Jensen furthers that preemptive cyber warfare risks overreaction. Limited operations like espionage would be seen as a sign of the US preparing to follow-up with more offensive strikes.

Ellers of National Interest '19 furthers that countries who perceive US operations as escalatory would be incentivized to attack the US first to maintain the upper hand.

Through the new offensive strategy Ellers concludes that countries will be locked in permanent tit-for-tat conflict with the US that could quickly spiral out of control.

As our use of OCOs increases, the problem only gets worse.

Healey of Oxford '19 writes that an aggressive US stance on cyber ops would trigger a positive feedback loop where countries would feel forced to create their own cyber commands, thus justifying a US increase in capabilities and resources.

Already, the AMSP '19 writes that use of OCOs will accelerate the cyber war with Russia until one side retaliates in a dramatic way to signal its resolve.

Second is revealing our strength.

As the US uses its offensive capabilities we risk our weapons being hacked and used against us.

This has already happened before.

Shane of New York Times ‘19 writes that in 2017 the NSA was hacked, releasing a weapon called EternalBlue. Since then hackers from Russia, China, and North Korea have used the weapon to cause billions in damages, including attacks on American cities.

Overall, historically, as we have shown our cyber-capabilities, other countries are now incentivised to attack us and gain those capabilities for themselves.

For example, Singer of Foreign Policy writes that when Snowden leaked the United States' offensive cyber capabilities, attacks on the US increased by 55% with severity also increasing.

Once countries have these weapons, they can use them with zero accountability.

Detsch of CSmonitor ‘17 writes that countries like China and Russia outsource their operations to large groups and companies, allowing them to launch large attacks and deny responsibility for any harm caused.

Aside from state actors, Jones of Financial Times ‘17 finds that through black markets, leaked weapons can quickly spread to unwanted groups and nations.

Even worse, after being attacked, the United States would lash out at perceived perpetrators.

The DOD'15 writes that as non-state entities and proxies launch attacks on the US it would make it harder for the US to identify the attackers, spiking the risk of miscalculation.

Third is by ending cooperation.

By constantly using offensive cyber operations against other countries, we decrease their incentive to cooperate with us.

Mussington of the CIG ‘18 finds that because cyber weapon capabilities are hard to gauge and are used to directly confront other countries, they corrupt cooperation by breeding mistrust.

Farell of CFR ‘15 furthers that rules for cyber engagement can only be formed if the US limits its ability to use operations that contradict their own demands.

Clarifying Cyber Conflict is crucial as Infosec ‘18 writes absent clear guidelines for cyber engagement countries will be uncertain in terms of how and when to respond to cyber attacks. They conclude that this ambiguity greatly increases the risk of conflict erupting as cyber engagement becomes more aggressive.

The impact is cyberwar in two ways.

First, on our infrastructure.

Straub of the SA in 2019 corroborates that because cyber attacks have the ability to destroy infrastructure that is vital for providing necessities like food, water, and energy, the effects of a cyber war can quickly jeopardize life for millions.

Indeed, the University of Cambridge finds that just one cyberattack on the US power grid would leave 93 million people in the dark and cost hundreds of billions in damages to the economy.

Second, on our financial institutions.

Additionally, because of rampant escalation caused by our use of OCOs, Politico in 2019 writes that the financial industry is preparing for U.S. banks to be hacked.

Pisani of CNBC in 2018 writes that because the global economy is largely determined by the success of the US market, a major cyber attack that would collapse our financial systems would quickly spread around the world.

The IMF concludes that the next economic shock would push 900 million people into poverty worldwide.

Thus, we negate.

Recession o/w terrorism two warrants

1. When we have a recession politicians are more incentivised to pull troops out of areas like Afghanistan, Time 08' writes that the recession put hella pressure on obama to decrease troop presence in these areas, which stops the military from being in the region which is responsible for most ISIS loss, also means less funding for the ISIS cyber task force
2. Recruitment doesn't matter if no one wants to join ISIS, FP: when econ downturn ppl in marginalized communities and emerging economies are much more likelier to join terrorist orgs

This is because Waldron of the National Interest '18 finds that the US has terrible cyber vulnerabilities.

And Martin of Jask '16 finds that as cyber weapons are spread around the world, groups could utilize them to launch "doomsday" attacks on the US.

a/t incentive to attack us is NU (2nd link)

1. Countries have limited resources on attacking,we have to demonstrate a specific capability before they start attacking. Singer clearly indicates that we had to reveal shit for countries to come attack us, seeing a 55% increase in stealing after we revealed weapons.
2. His response concedes the warrant that after things like Stuxnet and Eternal blue now people think the US has the best capability, which is why the sanger ev indicates that when we revealed our weapons we saw a 55% increase in stealing.
    a. The warrant for why our frontline is true is because there is an iherent high risk in attacking the US, so countries can only take that chance if they KNOW we have unique capabilities.

Cards

Dilanian of CNBC ‘19

https://www.cnbc.com/2018/09/21/trump-cybersecurity-policy-offensive-hacking-nsa-russia-china.html

The White House released a new cybersecurity strategy today, with several important changes in direction meant to give government agencies and law enforcement partners a greater ability to respond to cybercrime and nation-state attacks. The 40-page document mostly stays the course for past initiatives -- like working to strengthen the organizations that make up the country’s “critical infrastructure” industries, including electrical operators and financial institutions.

But some of **the changes emphasize a shift toward a more offensive cybersecurity posture**, a longtime request fromm the National Security Agency and cybersecurity branches of the U.S. Armed Forces.

The strategy codifies the ability of agencies aligned with the Department of Defense, like the NSA and military branches, to conduct offensive actions in cyberspace.

This means these agencies will be able to go after the overseas sources of attacks more proactively.

These activities can be risky, as cybercriminals may position their attacks from a neutral third party or a non-hostile country, making it more complicated for the U.S. to engage in cyber battles. These back-and-forth attacks can also cause damage to the infrastructure that supports the internet, particularly telecommunications providers.

This strategy gets the agency and law enforcement partners closer than ever to being allowed to make these offensive bids, which could include dismantling “botnets” — which are collections of compromised computers and devices used to attack corporate or government targets — underground cyber black markets, or other sources of cyberattacks.

Jensen of the Cato Institute ‘19

https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint

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**

Ellers of National Interest '19
https://nationalinterest.org/blog/skeptics/how-americas-cyber-strategy-could-create-international-crisis-90526

Buchanan argues that Washington's poor understanding of the indistinguishability between offense and defense is the pitfall in current American cyber strategy and that the utilization of traditional militaristic concepts in the cyber domain prevents the United States from identifying how intelligence collection can create unintended escalation. Buchanan remains skeptical that states will be encouraged to self-regulate their behavior in cyberspace. He worries that **America's cyber strategy may actually incentivize conflict escalation. Countries that perceive America's defensive strategy to be offensive in nature would be encouraged to attack the United States in order to retaliate or acquire intelligence of their own to ensure their defense in the future. Healey describes this as a tit-for-tat response. Should the United States continue to utilize these strategies, then states will find themselves in a position of "not just persistent, but permanent conflict,"** according to Healey. Though a defensive strategy of retaliatory countermeasures may be intended to avoid escalation, friction may instead lead to increasing instability in the cyber realm which could quickly spiral out of control.

Healey Oxford 2019
https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878

The posture and organizational dynamics feedback loops also overlap in their effects**. It is possible there is a positive feedback loop of policy isomorphism if the act of declaring an "offense is the best defense" posture (backed by perceived capability) shoves adversaries into adopting the same posture.** It may be stabilizing if adversaries believe they cannot (or ought not) respond. **It is likewise possible that as nations create commands to conduct offensive cyber operations, and delegate authority to conduct such operations, other nations will do the same. The global proliferation of cyber commands suggests some such dynamic, and China's seems purpose-built to match or "supersede" US Cyber Command** [84]. Once created, **these military cyber commands may feel an organizational imperative to engage in offensive cyber operations, whether to justify budgets or respond to operational contact with adversaries. US forward defense might cause headwinds to adversary operations, only to see that counteracted by the tailwinds of additional resources flowing to adversary cyber commands using the US posture to justify their own larger budgets.**

Mussington of the CIG '18
https://www.cigionline.org/articles/strategic-stability-cyber-operations-and-international-security

Tools of cyberwar are largely non-physical and therefore easier to conceal than conventional forces, making it difficult for actors to assess each other's capabilities. Offensive military cyber doctrines in the United States, Russia, China and elsewhere show that states are imitating neighbours and competitors when they develop their own cyber capabilities. However, these doctrines are not widely understood, feeding mistrust and the perceived need to gain a "first mover advantage" (ibid.). This in turn heightens the danger of escalation and reduces stability. Under the circumstances, a stable and persistent advantage in cyberspace seems unattainable.

Farell of CFR ‘15

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

If the United States is serious about promoting a normative approach to interactions in cyberspace, it will have to undertake some difficult reforms. First, the NSA, the Central Intelligence Agency, and Cyber Command should adopt a fundamental change of mind-set, abandoning what legal scholar Margo Schlanger calls "intelligence legalism." Most U.S. intelligence officials pride themselves on obeying the law, but their understanding of the law sometimes depends on strained and secret interpretations that push the envelope of what is possible. As argued in President Barack Obama's Review Group on Intelligence and Communications Technologies, the review process for signal collection must be more clearly weighed against the potential damage to the normative commitments to an open and secure Internet held by the United States, its allies, and those whom the United States wishes to persuade. **If the NSA wants to help develop strong norms, it will have to limit its own freedom to carry out operations that contravene the norms that the United States seeks to establish**. Second, if the U.S. government wishes to use naming and shaming tactics to develop norms, it will need evidence to support its claims. Shaming tactics face their own version of the attribution problem and the Snowden affair makes the U.S. government less inclined to share sensitive information, while some parts of the technical community are more likely to question the veracity of the information and less willing to cooperate.

Infosec ‘18

https://resources.infosecinstitute.com/the-time-has-come-for-rules-of-engagement-for-cyberwarfare/#gref

The United States and the other large international players are not the only ones with the skills, resources, technology and motivation to contend in the cyber arena. Countries around the world have taken large steps to begun to build their cyber warfare capabilities. According to Peter Singer, director of the Center for 21st-Century Security and Intelligence at the Brookings Institution, more than 100 nations now have a cybercommand or a special military unit assigned to fighting and winning wars in cyberspace. Put simply, the global stage is nearly set for cyber-based conflict. If one occurs, it could be — as Pulitzer Prize winner Robert Kaplan noted in a 2016 speech at the University of North Carolina — not a cat and mouse game, but “a cat and a cat game. If you’re ever seen two cats fighting…it’s a dangerous game to get into.**” Without established rules, conflict can quickly escalate with unexpected initial and follow-on consequences.**

Straub of the SA in 2019

https://www.sciencealert.com/a-major-cyber-attack-could-be-just-as-damaging-as-a-nuclear-weapon

As someone who studies cybersecurity and information warfare, I'm concerned that **a cyberattack with widespread impact, an intrusion in one area that spreads to others or a combination of lots of smaller attacks, could cause significant damage, including mass injury and death rivaling the death toll of a nuclear weapon.**

Unlike a nuclear weapon, which would vaporize people within 100 feet and kill almost everyone within a half-mile, the death toll from most cyberattacks would be slower. **People might die from a lack of food, power or gas for heat or from car crashes resulting from a corrupted traffic light system. This could happen over a wide area, resulting in mass injury and even deaths.**

This might sound alarmist, but look at what has been happening in recent years, in the US and around the world.

University of Cambridge

https://fas.org/sgp/crs/homesec/R45312.pdf

The NRC report further commented on the potential effects of a combined cyber and physical attack on the grid: If they could gain access, hackers could manipulate SCADA systems to disrupt the flow of electricity, transmit erroneous signals to operators, block the flow of vital information, or disable protective systems. Cyber attacks are unlikely to cause extended outages, but if well coordinated they could magnify the damage of a physical attack. For example, a cascading outage would be aggravated if operators did not get the information to learn that it had started, or if protective devices were disabled.26 **Similar conclusions were reached in a 2015 report from the University of Cambridge and Lloyds of London, which stated that a targeted cyberattack could leave 15 states and 93 million people from New York City to Washington, DC, without power. The scenario estimated the total impact to the U.S. economy at between $243 billion and $1 trillion, resulting from "direct damage to assets and infrastructure, decline in sales revenue to electricity supply companies, loss of sales revenue to business and disruption to the supply chain."** 27 The 2013 attack on the Metcalf substation in California further cast light on the physical vulnerabilities of the grid. After someone broke into a nearby underground vault to cut telephone cables, snipers opened fire on the substation, knocking out 17 large power transformers sending power to Silicon Valley. A blackout was averted by rerouting power around the substation, and local power plants were called upon to produce more electricity. It took the local utility 27 days to restore the substation. The Federal Energy Regulatory Commission's (FERC's) chairman at the time reportedly said that "if [the attack] were widely replicated across the country, it could take down the U.S. electric grid and black out much of the country."

The shift to become more offensive makes the problem of stealing even worse.

Wolff of the New York Times '19 writes that as we become more offensive we shift attention and resources away from cyber defense making it much easier for others to get into our systems.

Overall, Jones of Financial Times '17 finds that through black markets, leaked weapons can quickly spread to unwanted groups and nations.

This restrained stance kept tensions low, as Jensen of the Cato Institute finds that between 2000 and 2016, only 33% of cyber operations saw any retaliatory reactions, with most being mild responses.

Already, the AMSP '19 writes that use of OCOs will accelerate the cyber war with Russia until one side retaliates in a dramatic way to signal its resolve.

This is disastrous as Martin of Jask '16 finds that as cyber weapons are spread around the world, groups could utilize them to launch "doomsday" attacks on the US.

Farell concludes that norms will only be developed if countries stop viewing them as projections of US national interests, and rather ones developed out of a general consensus.

The Brookings Institution writes in 2018 that because the US OCO's would force countries into a "use it or lose it" posture, situations could quickly escalate to levels of all-out war.

Shrewd of Digit in 2019 corroborates that because of rampant escalation we face an upcoming cyber-cold war in which financial attacks will increase in amount and severity.

Establishing these norms is crucial as Kessler of the Harvard Political Review '17 finds that these norms can help define appropriate cyber behavior that could prevent major actors from launching devastating attacks.

Frontlines:

Critically, the Independent writes in 2019 that in a Russia-US Nuclear war 90 million people would die, and the

a/t stealing is not topical

a. 'use' of OCOs only accelerates the development of them

so EternalBlue is more likely to exist in a world in which we use more OOCs

OCOs*

b. even if we didn't use EternalBlue specifically, our use of OCOs in general highlighted our capabilities, which makes us an attractive hacking target

C.offense/defense argument links into this as well

1/ fix in LT by knowing weapon

1. No one patches shit, that's why Eternal blue is still hurting people
2. Don't develop weapons with the mindset of how to stop it, that's two different weapons

2/ weapons are specialized for an enemy

1. Not true, enemies re-engineer it against the united states, in fact the ___ finds the weapons actually become deadlier afterwards

Magnitude before probability weighing:

1. We have very good probability on our side, the AMSP 19' ev indicates that conflict with Russia is happening in squo and on our second link eternal blue indicates our link is happening too, they don't do comparative
2. No historical proof of end impact - isis may decrease but just like al qaeda led to ISIS we don't know their net impact
3. Uniqueness weighing is on our side - the strength from resolution is higher, OCO's clearly led to hacked and retal, whereas other factors may disturb their uniqueness like our military presence

https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-66/jfq-66_15-21_Olson.pdf?ver=2017-12-06-115540-947-cyberweapons are getting more aggressive
Change in the character of war is always noticeable after the fact, but the development of the technologies and methods that are the basis of the change is not. The roots of shifts in warfare are often present and undergoing development for years prior to their first decisive employment. Use of railroads, telegraphic communications, and headlong assaults into fortified positions during the Civil War foreshadowed operations in World War I.6 The Germans tested coordination of ground and air elements in the Spanish Civil War, years before it was employed on a large scale against the Polish and French in World War II.7 Similarly, the Yom Kippur War in 1973 used airpower to pin and hammer ground formations—a technique that would be used nearly 20 years later in Operation Desert Storm. 8 In each example, the years between initial development and large-scale implementation served only to increase the lethality of the final product. Cyber warfare has been developed and tested in a similar manner to these examples, and reports have consistently warned of the danger such warfare poses.

https://outline.com/2FGrwr

Yet despite this offensive capability and the demonstration of its potency, attacks on the United States have only grown, in both number and intensity. In the year after the Snowden leaks proved the United States' offensive prowess, there was 55 percent more confirmed data breaches than the year before — and that doesn't even include the operations targeting major government sites like OPM or the Pentagon's Joint Staff network.

https://outline.com/2FGrwr

The problem is that the evidence disproves this link between building up more cyber-offensive capability as the way to scare off the other side. There is not yet any direct pathway to deterrence the way building up nuclear capability yielded it back in the day. Unlike concerns over bomber and missile “gaps” during the Cold War (which notably turned out to be wrong), the United States’ hugely superior position in cyberspace has never been in question. And for anyone somehow in doubt, there were the series of Washington policymakers’ leaks designed to take credit for Stuxnet, the cyberattack that successfully slowed Iran’s nuclear program and showed off a whole new class of cyberweapon. Then came Edward Snowden’s dump of thousands of NSA documents**.** While Snowden’s disclosures obviously angered his former employers, they also show that the folks at Fort Meade have much to be proud of. They have developed unmatched, amazingly exotic capabilities, from a mindboggling scale of global monitoring devices to new classes of cyberweapons that use radio signals to jump software over the previously protective physical divides between systems. And the leaks show the capability is not mere lab work, but that the NSA has used them in operations against targets ranging from Iranian nuclear research facilities to Chinese command networks.

https://www.sandiegouniontribune.com/news/science/sd-me-cyber-warfare-20161014-htmlstory.html - attack on grid = 93 mil in dark https://www.independent.co.uk/news/world/americas/us-russia-nuclear-war-trump-putin-simulation-europe-nato-a9109116.html - 90 mil in russia-us cyber war people instantly dead

https://www.sciencealert.com/a-major-cyber-attack-could-be-just-as-damaging-as-a-nuclear-weapon - cyber war just as damaging as nuclear war

Indeed, Lindsey of CPO magazine '19 writes that leaking stockpiles of cyberweapons would be akin to letting nukes fall into the wrong hands.

Brookings below

U.S. attempts to compromise the North Korean missile development program and noting that cyber capabilities depend on concealing information
about cyber vulnerabilities from the other side, they argue that if the latter
has nuclear capabilities its confidence in its ability to use those capabilities
may be excessively high, and that it will be less likely to back down in a
crisis—thus increasing the likelihood that nuclear war will break out.

https://www.cfr.org/blog/theft-and-reuse-advanced-offensive-cyber-weapons-pose-growing-threat - other examples of weapons getting hacked, wannaCry and Petra

https://www.theamericanconservative.com/articles/why-u-s-cyber-sneak-attacks-wont-work-against-iran/

TAC 2 days ago -

Our OCOs vs Iran have forced them to upgrade their own forces and escalation has occurred, making it impossible for peace to happen

1/ doing a ton more attacks these days
2/ wolf: LT defense weakens so in the future more attacks

https://www.dailymail.co.uk/news/article-2751896/Islamic-State-jihadists-planning-encryption-protected-cyber-caliphate-carry-hacking-attacks-West.html - terrorist have intent to attack us + infra

https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf
In addition to state-based threats, non-state actors like the Islamic State in Iraq and the Levant (ISIL) use cyberspace to recruit fighters and disseminate propaganda and have declared their intent to acquire disruptive and destructive cyber capabilities. Criminal actors pose a considerable threat in cyberspace, particularly to financial institutions, and ideological groups often use hackers to further their political objectives. State and non-state threats often also blend together; patriotic entities often act as cyber surrogates for states, and non-state entities can provide cover for state-based operators. This behavior can make attribution more difficult and increases the chance of miscalculation."

Baram of CFR '19 writes that less sophisticated countries focus their resources on stealing more sophisticated weapons, as they allow them to launch effective attacks without having a lengthy R&D process.

War Stuff
https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf
In addition to state-based threats, non-state actors like the Islamic State in Iraq and the Levant (ISIL) use cyberspace to recruit fighters and disseminate propaganda and have declared their intent to acquire disruptive and destructive cyber capabilities. Criminal actors pose a considerable threat in cyberspace, particularly to financial institutions, and ideological groups often use hackers to further their political objectives. State and non-state threats often also blend together; patriotic entities often act as cyber surrogates for states, and non-state entities can provide cover for state-based operators. This behavior can make attribution more difficult and increases the chance of miscalculation."

.
https://www.ft.com/content/a7a6c91c-3a35-11e7-ac89-b01cc67cfeec

For the most part, such exploits are valuable as a means of espionage because they offer ways to hack into systems without detection. But **these tools can often be repurposed with ease**. **On the dark web** — the parts of the internet that are not reachable through regular search engines and often require specialist knowledge to access — **there is a thriving trade in exploits, and a community of hackers, criminals and activists that develop and repurpose them for malign ends. EternalBlue is just one of a trove of high-grade exploits that in recent months have been stolen from the US government and which can now be found online.** Some have emanated from WikiLeaks, the whistleblowing site, which is gradually releasing what it calls "vault 7", a cache of CIA cyber tools, so that tech companies can patch the software flaws these target. An even greater number may be in the hands of an anonymous group western intelligence officials believe is a front for Russian spy agencies, known as the ShadowBrokers. "WannaCry is just the latest in a series of events that should have been wake-up calls over this problem," says Toni Gidwani, director of research operations at the Washington-based cyber intelligence firm ThreatConnect. **"The characteristics of the attack and how quickly it spread were a progression . . . they showed how we have seen the cyber crime environment evolve. Groups have become more sophisticated, and they are adapting more and more tools. When you have vulnerabilities leaked like those by the ShadowBrokers — when things like that become public knowledge — you very quickly see weaponisation."**

https://outline.com/F4LUhz

Another problem is that the attack tools developed by our intelligence agencies tend to become sought-after targets for other nations that don't have the technical depth to develop their own. This has been the case with past tools, such as Eternal Blue, developed by the National Security Agency, which was stolen and leaked by a hacker group and subsequently used by North Korean hackers to create WannaCry — the massive ransomware attack in 2017 that crippled millions of computers in more than 150 nations in a matter of hours. That desire to match U.S. capabilities will only be worse after an officially confirmed attack.

https://www.forbes.com/sites/thomasbrewster/2019/05/07/chinese-hacker-crew-stole-nsa-cyber-weapons-in-2016--a-year-before-they-were-leaked-online/#128a6523237b

A Chinese group of hackers managed to get hold of cyber weapons from the U.S. National Security Agency's arsenal of digital weapons and were using them as far back as 2016.

Researchers at American cybersecurity giant Symantec claimed in a report released Tuesday that a group dubbed Buckeye had used a pair of tools called "Bemstour" and "DoublePulsar," which exploited weaknesses in Microsoft Windows, back in March 2016. Symantec didn't name Buckeye as a Chinese espionage unit, but U.S. government and private industry have previously tied the group to China's intelligence apparatus.

A year later, a group calling itself the Shadow Brokers started releasing versions of tools from a cyber-espionage operator called the Equation Group, which was swiftly revealed to be the NSA. The identity and provenance of the Shadow Brokers remains a mystery.

https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html

Until a decade or so ago, the most powerful cyberweapons belonged almost exclusively to intelligence agencies — N.S.A. officials used the term “NOBUS,” for “nobody but us,” for vulnerabilities only the agency had the sophistication to exploit. But that advantage has hugely eroded, not only because of the leaks, but because anyone can grab a cyberweapon’s code once it’s used in the wild.

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

The new element in the story is that an organization has reverse-engineered a deployed US cyber tool and reused it; previous cases involved the theft or loss of a tool,” agreed Bryan Clark of the Center for Strategic & Budgetary Assessments. “This would be similar to the Chinese finding a Tomahawk missile that had failed to detonate and using it to build their own.” The difference, Clark continued, is that physical bombs and missiles automatically destroy themselves in the course of an attack, unless they’re duds. Cyber weapons don’t.During war games, the cyber teams often assume that a weapon will only be used once, for precisely this reason. “The solution is to make cyber weapons tamper resistant,” he said, “which means their code cannot be determined without proper encryption, or the code rewrites itself after use, ‘dudding’ the weapon.” But even self-destructing code doesn’t *guarantee* a target of our cyber weapons can’t copy them, Clark warned: “They will still run the risk of being detected and characterized by a defensive system before the tamper resistant features activate.”

https://jask.com/cyber-weapon-proliferation/

Government grade cyber weapons with dramatic real world consequences like STUXNET not only exist but have long been feared by experts due to their ability to be acquired and repurposed by others. For example, a terrorist organization like ISIS, wielding a tool like STUXNET, could aim it at Western power grids or nuclear plants. While STUXNET did actually leak un-intendedly to the public through a bug in the propagation code and some mis-guided upload tests to services like VirusTotal, it’s risk was mitigated by the fact that the source code did not leak. Even in this circumstance the leaked weapon posed a real threat, as it was quickly reverse engineered and new concepts taken, but was still very difficult to re-purpose or “weaponize” the tool to attack others. Fortunately, in the case of STUXNET, it was designed for one very specific purpose and thus it’s usage elsewhere was largely minimized . Now on the other hand, if the source code of a sophisticated cyber weapon ever leaked out to the public it could allow any group, including a terrorist one, to quickly weaponize and use it at their own will, significantly raising the stakes to alarming levels.

This leaked source code scenario described above would be a security risk to all, and unfortunately as of last week’s Shadow Brokers event leaking NSA hacking toolset, this potential “doomsday” event is now a reality. For the first time ever, government grade (multi-million dollar) cyber weapon has leaked in source code form to the general public giving dangerous groups control of said weapon…

https://www.cfr.org/blog/theft-and-reuse-advanced-offensive-cyber-weapons-pose-growing-threat

First, are states going to start reusing each other’s leaked cyber tools as a matter of course? The ability to reuse stolen cyber tools may signal the beginning of a shift in the distribution of international cyber power, as weaker actors (including non-state actors) become increasingly able to use sophisticated malware to cause global damage and possibly target the cyber weapons’ original designers. Countries that are less technologically advanced and less vulnerable to cyberattacks might find the reuse of stolen vulnerabilities appealing for their own offensive activity. Second, is it possible to prevent the leaking of cyber tools from occurring in the first place? There aren't many reasons to be optimistic. First, there’s the insider threat problem—a particularly thorny issue given the extensive use of contractors and the risk that they steal or mishandle sensitive information that they were exposed to during their service. A second and possibly more problematic reason is that it is cheaper to use stolen vulnerabilities than finding new ones. As new vulnerabilities like EternalBlue get exposed, the costs of using stolen cyber vulnerabilities and conducting attacks are being consistently lowered while benefits remain high. States with offensive capabilities know that putting their hands on unique vulnerabilities developed by their adversaries will enable them to more easily launch sophisticated attacks without the need pursue a lengthy and costly R&D process. This makes the reuse of cyber tools especially appealing and may motivate different actors to concentrate their efforts in this direction. As long as the benefits of using the stolen vulnerabilities are higher than the costs, these vulnerabilities will remain an attractive target.

Third is

Apart from having ours weapons stolen, the actual use of offensive cyber operations also spreads our capabilities to unwanted actors.

Hitchens of Breaking Defense ‘19 writes that whenever we conduct offensive operations we leave behind traces of information and code allowing our adversaries to reengineer our own weapons.

Hitchens furthers that China has already been making cyberweapons based on the US’s past operations.

https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878#140575448 -FIRE ESCALATION EVIDENCE

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.**

https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878#140575448- New Strategy means others will follow suit and cause global escalation

The posture and organizational dynamics feedback loops also overlap in their effects**. It is possible there is a positive feedback loop of policy isomorphism if the act of declaring an "offense is the best defense" posture (backed by perceived capability) shoves adversaries into adopting the same posture.** It may be stabilizing if adversaries believe they cannot (or ought not) respond. **It is likewise possible that as nations create commands to conduct offensive cyber operations, and delegate authority to conduct such operations, other nations will do the same. The global proliferation of cyber commands suggests some such dynamic, and China's seems purpose-built to match or "supersede" US Cyber Command** [84]. Once created**, these military cyber commands may feel an organizational imperative to engage in offensive cyber operations, whether to justify budgets or respond to operational contact with adversaries. US forward defense might cause headwinds to adversary operations, only to see that counteracted by the tailwinds of additional resources flowing to adversary cyber commands using the US posture to justify their own larger budgets.**

https://nationalinterest.org/blog/skeptics/how-americas-cyber-strategy-could-create-international-crisis-90526

Buchanan argues that Washington's poor understanding of the indistinguishability between offense and defense is the pitfall in current American cyber strategy and that the utilization of traditional militaristic concepts in the cyber domain prevents the United States from identifying how intelligence collection can create unintended escalation. Buchanan remains skeptical that states will be encouraged to self-regulate their behavior in cyberspace. He worries that **America's cyber strategy may actually incentivize conflict escalation. Countries that perceive America's defensive strategy to be offensive in nature**

would be encouraged to attack the United States in order to retaliate or acquire intelligence of their own to ensure their defense in the future. Healey describes this as **a tit-for-tat response. Should the United States continue to utilize these strategies, then states will find themselves in a position of "not just persistent, but permanent conflict,"** according to Healey. Though a defensive strategy of retaliatory countermeasures may be intended to avoid escalation, friction may instead lead to increasing instability in the cyber realm which could quickly spiral out of control.

https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint-
ESCALATION EVIDENCE

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

https://www.csmonitor.com/World/Middle-East/2019/0701/US-Iran-clash-enters-cyber-realm-and-tests-a-Trump-strategy-

A more assertive and intrusive U.S. military approach to going after cyberthreats overseas – wherever malicious code exists – could lead other countries to respond in kind, causing unwanted escalation. While the U.S. is considered the world's most capable cyber power, it is also one of the most vulnerable because of its advanced digital economy.

“The U.S. is in a very precarious situation where it needs to project some amount of power, to show other countries that you can't just walk in and do what you want, but also respond in a very restrained manner,” says Mr. Caltagirone.

“What the U.S. does now is going to set the tone for the next five years.”

http://mil-embedded.com/articles/cyberwarfare-battlefield-precursor-for-kinetic-attacks/
-precursos for other attakcs