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

Contention One is Deescalation.

The existence of Offensive Cyber Operations, or OCOs, gives the US military flexibility during confrontations.

Jensen of the Washington Post '19 writes that OCOs allow the US to respond to provocations effectively without using the military which is highly escalatory.

For example, Smeets of Air University '18 writes that when Bush was contemplating using military force against Iran in 2006, cyber operations provided him with a 3rd option to attack Iran without causing war.

The impact is entrenching conflict.

Just look at Iran. If we were forced to physically intervene, Ward of Vox '19 finds that hundreds of thousands of people would die in a war between both countries.

Even if a kinetic strike doesn't occur, inaction still begets conflict.

Barnes of the New York Times '19 writes that offensive cyber operations signal to other countries that the US will respond to provocations and impose costs decreasing their incentive to be more aggressive, writing that after the recent attack on Iran, escalation was non-existent.

This is key, as Rogin of the Washington Post '19 concludes that failing to respond to Iranian aggression will only embolden them to be more provocative as they perceive the US is less willing to engage, eventually leading to conflict.

Contention two is Shaping the Future.

Recently the US has taken steps to deregulate their cyber command allowing them to initiate attacks with much higher frequency. This new strategy is a drastic shift from the old policies of cyber deterrence and restraint.

This increase in use of OCOs will stabilize the cyber domain in 2 ways.

First is through trial and error.

Pollard of Lawfare '19 writes that our use of OCO's provides a platform for adaptive learning, where over time we can communicate the acceptable range of attacks.

The CFGR '19 finds that this is because the new US strategy would enable our ability to precisely target countries for specific actions to signal our stance on cyber activity.

Overall, Pollard concludes that through persistent engagement we can clarify dangerous misperceptions in cyber conflict. He finds that even if there is a short term increase in provocation, in the long term a greater US cyber-presence will reduce the risk of escalation causing some sort of break out conflict.

Second is by norm setting.

The use of offensive cyber operations allows the US to leverage other nations into stopping their hacking.

Smeets 18 of Stanford explains that unlike dropping a missile, the damage of a cyber attack can be reversed at any time. This enables the use of leverage to punish actors that violate our cyber norms by withholding reversal until conditions are met.

Indeed, this method has been extremely effective. **Maness 18** of Northeastern finds that 4/6 US cyber coercion attempts are successful in invoking political concessions with countries such as China and North Korea.

Overall, without actively engaging in the cyber domain, Harknett of the Foreign Policy Institute '17 writes that the United States would be unable to push good practices and achieve peace, concluding that actors who are able to use OCOs to leverage others and dominate the cyber realm, will be in the strongest position to advocate for norms supporting their positions.

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.

Overall on both links, without the United States involved in the cyber domain, escalation will rise with no end.

Goldsmith of Brookings '16 finds that a cyber policy of inaction would only embolden our enemies to be more aggressive in the long term as they perceive they have a blank check. Indeed Schneider of LB '19 furthers that the 2011 strategy of restraint lead to an exponential increase in the scope and severity of cyber attacks on the US.

The impact is preventing cyber-catastrophe.

Infosec '18 continues that 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 a dangerous cyber attack as cyber engagement becomes more aggressive.

The Internet Society '17 furthers that as time goes by more and more of the world's vital infrastructure and economic systems will become connected to the internet.

For example, University of Cambridge concludes that a cyberattack on the US power grid would leave 93 million people in the dark and cost hundreds of billions in damages to the economy.

And Pisani of CNBC in 2018 writes that a major cyber attack on our financial systems would quickly spread around the world causing a world wide recession, pushing hundreds of millions of people into poverty.

Thus, we affirm.

Aff First Link

On our first link - we say that without OCOs, countries think that they can get away with anything. So they will keep attacking us until they eventually take one wrong step that risks real conflict. Using OCOs can help draw a line in the sand that tells other actors what is and isn't okay.

And going into the future, this risk of such conflict will only increase, as Coats of the UIC in 2019 writes that billions of unsafe devices will become connected to the internet and nation-states will have access to increasingly advanced cyber-weapons.

This conflict would be disastrous. For example, the San Diego Tribune finds that attacks on the US power grid would put 93 million people in the dark instantly, and the Pisani of CNBC in 2018 writes that attacks on the sector could send shockwaves throughout the rest of the sector leading to the next financial crisis, pushing hundreds of millions into poverty.

The Medium '19 writes that cyber attacks could serve as warnings that there is worse to come in the future if countries don't cease their actions.

For example, Wired '19 writes that in response to Russian hacking our cyber attacks were able to send the signal that the US has the ability to retaliate to any harmful action taken against it, deterring future aggression.

Indeed Pollard of LF '19 finds that these attacks were able to take out russian capabilities without any significant blowback.

Nye of the WEF '15 concludes that similar to nuclear weapons over time we can help to develop norms that limit the use of cyber weapons for malicious and escalatory purposes.

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.

https://www.weforum.org/agenda/2015/05/why-we-need-global-rules-to-prevent-cyber-war/- good norms evidence use for the link

Similarly, the most promising areas for early international cooperation on securing cyberspace are problems posed by third parties such as criminals and terrorists. Russia and China have sought a treaty for broad United Nations oversight of the Internet. Though their vision of "information security" could legitimize authoritarian governments' censorship, and is therefore unacceptable to democratic governments, it may be possible to identify and target behaviors that are illegal everywhere. Limiting all intrusions would be impossible, but one could start with cyber crime and cyber terrorism. Major states would have an interest in limiting damage by agreeing to cooperate on forensics and controls

It is likely to take longer to conclude agreements on contentious issues such as cyber intrusions for purposes like espionage and preparing the battlefield. Nonetheless, the inability to envisage an overall cyber arms-control agreement need not prevent progress on some issues now. International

norms tend to develop slowly. It took two decades in the case of nuclear technology. The most important message of the recent Dutch conference was that massive cyber vulnerability is now nearing that point.

It's imperative we build these best practices now as Hanson of Brookings '15 writes that as countries around the world start to advance their cyber capabilities, a lack of established and enforceable international norms will greatly increase the risk of miscalculation.

Morris of Rand '16 finds that although conflict isn't occurring now, as countries ability to attack the US becomes more effective the risk of aggressive confrontation greatly increases.

It is imperative we create these norms now as the Council onForeign Relations '18 writes that a lack of a mechanism to shape future cyber engagement would allow malicious actors to be aggressive without repercussions.

Existence of cyber operations

w/ out response→ countries perceive they can do bigger attacks → triggers miscalc eventually OCO show in future countries can't cross threshold

1. Shaping Global Norms

2. As we develop more capabilities that means they come to the table because we are stronger, we are weaker rn so obviously they won't do it
    a. Might in the future use bigger weapons against other countries-->hiroshima example we only did one attack but they always want to stop nuclear weapons
    b. Stuxnet is a good example of showing we have strengthened, ocos are a good way to signal strength
3. Come to mutual agreements that's how negotiations work so Russia and the US can agree to something

A2 attribution
https://www.belfercenter.org/sites/default/files/files/publication/isec_a_00266.pdf
Attribution is a matter of degree. Despite the problems of proxies and false ºags and the difªculty of obtaining prompt, high-quality attribution that would stand up in a court of law, there is often enough attribution to enable deterrence. Three major audiences are relevant. A defending government will want relatively high assurance from its intelligence agencies in order to avoid escalation and catalytic entrapment by a malicious third party, but it can rely on all-source intelligence in addition to network forensics. Second, the attacking government or nonstate actor knows what its role was, but it cannot be sure how good the opposing forensics and intelligence are. It can deny involvement, but it will never know how credible its deception was. Conversely, as suggested above, in some cases it may deliberately leave clues for signaling purposes while maintaining the ªction of plausible deniability

Prompt, high-quality attribution is often difªcult and costly, but not impossible. As Rid and Buchanan note, "[T]he larger a government's technical prowess, and the larger the pool of talent and skills at its disposal, the higher will be that state's ability to hide its own covert operations, uncover others, and respond accordingly."26 Not only are governments improving their capabilities, but many nonstate private-sector companies are creating a market in attribution, and their participation reduces the costs to governments of having to disclose sensitive sources. Many situations are matters of degree, and as technology improves the forensics of attribution, the strength of deterrence may increase. The problem of attribution should not be belittled, but imperfect attribution does not prevent some degree of cyber deterrence by punishment. At the same time, attribution is not a large factor in the denial, entanglement, and normative taboo means of cyber deterrence and dissuasion discussed below.

Absent our able to attack other actors they would be much more emboldened. As they continually conduct illegal operations, a lack of a US response would send a signal to these countries that they can attack the US and not face any meaningful retaliation. This would only incentivize them to be more aggressive in the future.

http://cs.brown.edu/courses/csci1800/sources/2019_01_22_JFQ_CyberRoleForPersistentOperations_Nakasone.pdf

Finally, we are ensuring our capabilities, operational tempo, decisionmaking processes, and authorities enable continuous, persistent operations. Adversaries and competitors have responded to our restrained and episodic engagement with cyber aggression that has eroded U.S. military, economic, and diplomatic advantages. Strategic effects in cyberspace come from the use—not the mere possession—of cyber capabilities to gain the initiative over those who mean us harm

http://cs.brown.edu/courses/csci1800/sources/2019_01_22_JFQ_CyberRoleForPersistentOperations_Nakasone.pdf

History cautions that we should expect the use of new capabilities to evolve as they are introduced in conflicts. Tanks, for instance, developed from infantry support to deep penetration roles, while aircraft progressed from tactical reconnaissance to strategic bombing to unmanned intelligence, surveillance, and reconnaissance. With battlefield experience comes the evolution and maturation of operational concepts and strategic insights. Carl von Clausewitz noted that the "knowledge basic to the art of war is empirical," meaning theory must conform to experience.

https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2942/RAND_RR2942.pdf

This study does not proceed from an assumption that either of these views is correct. Although our research highlights the limits of the effectiveness of gray zone strategies, these tactics clearly represent a threat to U.S. and allied interests, especially as techniques and technologies evolve over time.7 Indeed, the greatest danger may be in the future, when the impulse to achieve aggressive gains short of major war is married to dramatically improved means of doing so—in such disparate areas as information warfare and swarming drone technology. This strategy begins from the claim that it is strongly in the U.S. interest to constrain the growth of gray zone conflict, even if it is not currently posing an imminent, existential threat to U.S. interests

https://cgsr.llnl.gov/content/assets/docs/CGSRCyberWorkshop2019SummaryReport.pdf

Looking back at developments since 9/11, participants acknowledged major progress in reduction of threats to the homeland. Stuxnet was seen as having had significant influence on cyber strategic thought, orienting U.S. strategists around a target-based view (i.e. what targets can be affected through cyber means) and prioritizing the discussion of kinetic effects on targets. This occurred to the exclusion of an objective-based view and produced a focus on protecting critical infrastructure within the United States from cyberattacks with kinetic effects. Defending Department of Defense (DoD) and government networks and deterring cyber adversaries were also emphasized in the 2015 U.S. DoD Cyber Strategy. This approach came to appear inadequate, however, as the U.S. and allies were regularly targeted by adversaries with significant campaigns of cyber aggression below the threshold of armed conflict. These included major data breaches and persistent espionage campaigns, cyber-enabled influence campaigns

and election meddling, and intrusions into critical networks—potentially preparing conditions for future attacks.

https://www.zdnet.com/article/understanding-the-military-buildup-of-offensive-cyberweapons/

Despite the increased risk brought about by cyberwarfare, some experts would argue that there is an intrinsic value that comes with its rise. Both Gourley and Kindervag made the argument that the use of Stuxnet possibly saved the involved parties from a ground war. One could hypothesize, Kindervag said, that Israel might have felt it necessary to attack the nuclear refineries in Iran if they hadn't first been disabled by Stuxnet.

An additional argument would be that, if war has to happen, it would be better if it was perpetrated in cyberspace instead of the real world.

"If we're going to have warfare, the cyber world is a pretty bloodless place to do it," Kindervag said.

https://outline.com/2FGrwr

This dynamic makes reaching a formal prohibition on cyberattacks between the 21st-century powers unlikely. It does not mean, however, that there is no value in engagement and norm building. Rather than a treaty or agreement that unrealistically tries to create a Cold War-style regime of deterrence or arms control, the two sides need to flesh out a mutual understanding of the new rules of the game. Each side must understand that its opponent will continue to conduct cyber-activities ranging from espionage to theft. The most important goal is not to stop every cyberattack, but to keep them from escalating into something far more dangerous.

Shaping the perceptions of other countries--->
basically because we persistently engage with other countries those countries know the acceptable boundaries i.e what is wrong and right thing to do→
stops miscalculation from happening won't escalate because they know what to do

https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation/d-9076.ashx
Intensification is a necessary condition for escalation, and when the "way" employed causes physical damage, intensification results in an escalatory breakdown of the agreed competition space as described in this article. In 60 Garrett M. Graff, "A Guide to Russia's High Tech Toolbox for Subverting US Democracy," op. cit. 61 This is a modification of Kahn's definition of escalation to include escalation from agreed competition. 16 what may appear counter-intuitive to conventional wisdom, the more competitive interaction occurs within the agreed competition space, the more clarity will emerge on the demarcations of illegitimate or legitimate cyber operations and what are outside or within the "rules" of agreed competition and thus, may or may not lead to escalation.62 To help ground the concept of intensification in actual events, a few examples follow.
https://i.blackhat.com/USA-19/Thursday/us-19-Healey-Rough-and-Ready-Frameworks-to-Measure-Persistent-Engagement-and-Deterrence-wp.pdf-We need to actually use not just sit on our weapons
The threat of using something in cyberspace is not as powerful is actually using it."4 The mere possession of cyber capabilities is not enough, Nakasone argues, because adversaries are actively engaging the U.S. in cyberspace every day.5 If an adversary is actively stealing U.S. data, merely possessing the capability to disrupt them, but not using it, does nothing to improve the U.S. position. The use of cyber capabilities allows the U.S. to both demonstrate its capability and directly impose costs on an adversary.

https://www.fifthdomain.com/dod/cybercom/2018/11/26/why-cyberspace-demands-an-always-on-approach/There is still restraint-with perissitant engagement

Hager also noted that the mission in cyberspace might be enduring, much like the counterterrorism mission or general defense of the homeland. In other words, there is no immediate conclusion in sight. "All we're trying to do is go, 'Hey there's going to be a cost to doing this.'" But he added that that despite expanded authorities, Cyber Command has not been provoking other nations wherever it wants around the world."We still have a number of checks and balances through the interagency and higher-level authorities above the military chain of command because we do operate within the legal confines that the U.S. government has put on us," he said. "We're not just a bunch of

cowboys running out there and I can't necessary say some of our adversaries follow those rules."

https://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870
Norms can develop in a variety of ways, particularly through habit and entrepreneurship. Some norms emerge spontaneously without any particular actor having any particular intent and then become entrenched through habit. **In any group that interacts regularly, norms develop simply through expectations shaped by repeated behavior. Much of the foundational engineering of the internet involves this kind of path-dependent norm development. For example, the widespread preference for using a Simple Network Management Protocol to manage devices on a network arose from repeated use.** Policymakers understand this power of unchallenged repetition and often seek to shape it. For instance, the U.S indictment of five Chinese hackers in May 2014 partly aimed to dispel expectations that state-sponsored cyber espionage for commercial advantage is acceptable.

Hathaway 12 (Oona A. Hathaway the Gerard C. and Bernice Latrobe Smith Professor of International Law and director of the Center for Global Legal Challenges at Yale Law, Rebecca Crootof, pursuing a PhD in Law at Yale Graduate School of Arts and Sciences, Philip Levitz, Yale Law School Princeton University, Haley Nix, Research Assistant at Yale Law School Aileen Nowlan, William Perdue, Julia Spiegel (Forthcoming in the California Law Review, 2012), "THE LAW OF CYBER-ATTACK")

Changes in domestic law and policy, such as adding extraterritorial ¶ applicability to criminal laws and planning for the use of countermeasures, are ¶ valuable legal responses to the threat of cyber-attack. *Yet* "cyberspace is a ¶ network of networks that includes thousands of internet service providers ¶ *across the globe*; no single state or organization can maintain effective cyber ¶ defenses on its own."280 Given the transnational nature of the challenge, ¶ international cooperation is likely to be necessary to provide a solution ¶ commensurate to the problem.281 The *U*nited *S*tates has already committed itself to working "with like-minded states to establish an environment of expectations or norms of ¶ behavior, that ground foreign and defense polices and guide international ¶ partnerships."282 While the development of international norms is useful, *it ¶ will not provide governments and private actors with the clarity of a codified ¶ definition of cyber-attack or written guidelines on how states should respond to ¶ certain types of challenges*. For this reason, we recommend that the ¶ international community create a multilateral agreement. The agreement ¶ should have two central features. First, it must offer a shared definition of ¶ cyber-attack and which cyber-attacks constitute armed attack—"cyber-warfare"—under the U.N. Charter.283 Second, it should offer a framework for ¶ more robust international cooperation in evidence collection and criminal ¶ prosecution of those participating in cross-national cyber-attacks. That ¶ framework should be attentive to the challenges of over-criminalization, ¶ maintaining room for individuals to use the Internet and related technologies to ¶ engage in lawful dissent. Such a treaty would serve both international aims and ¶ national interests of participating countries.284 Any international resolution defining when a cyber-attack rises to the ¶ level of an armed attack should follow the effects-based approach described ¶ above.285 In other words, a cyber-conflict should be defined to escalate into a ¶ conventional conflict only if the cyber-attack causes physical injury or ¶ property damage comparable to a conventional armed attack. Although the ¶ framework of jus in bello *is of limited usefulness in evaluating the lawfulness ¶ of cyber-attacks because of its ambiguities*, it would not be appropriate for this ¶ definitional treaty to attempt to articulate the content of jus in bello norms for ¶ cyber-attack. Rather, the jus in bello challenges articulated above—such as ¶ proportionality of non-lethal or temporary harm and the definition of direct ¶ participation for civilians working alongside military cyber-attackers—*are ¶ likely to be clarified through state practice*. In any resolution or agreement on ¶ cyber-attacks, but

especially in the Security Council, the international community should ensure that the accepted definition of cyber-attack does not ¶ quell legitimate dissent and other legitimate expressive activities in ¶ cyberspace.

https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace

Persistent engagement has the major upside of encouraging adaptive learning by U.S. adversaries in cyberspace. As the USCYBERCOM vision statement notes, "Through persistent action and competing more effectively below the level of armed conflict, we can influence the calculations of our adversaries, deter aggression, and clarify the distinction between acceptable and unacceptable behavior in cyberspace." U.S. adversaries will also make mistakes—overreacting to U.S. actions, underestimating U.S. resolve or simply being slow to learn from experience. However, this learning process can help mitigate the larger risk in cyber conflict of escalation to armed conflict via a fundamental lack of understanding among adversaries about what targets and attacks are acceptable in cyberspace. Miscalculation—for example, underestimating how highly an adversary values a target that is attacked via cyberspace—will remain a risk and could lead to unintended escalation. However, the process of adaptive learning, explicit communication of limited intent, and effective signaling through military actions and inaction in other domains (e.g., avoiding contemporaneous large-scale military exercises near the adversary's border, or increased nuclear alert levels) should ultimately reduce the risk for dangerous escalation.

https://www.washingtoninstitute.org/policy-analysis/view/iran-crisis-moves-into-cyberspace

As the United States used cyber means to respond to a kinetic attack, Iran's leadership may see little reason for strategic restraint in cyberspace. Indeed, the restrained U.S. response may

embolden Tehran to move aggressively in that domain, believing Washington has reinforced its reluctance to take action in other military domains.

https://www.zdnet.com/article/cyber-attribution-isnt-so-important-even-for-nation-states/

Australia can pinpoint the individual humans responsible for a cyber attack, according to foreign minister Julie Bishop. You can assume that the other Five Eyes nations -- the US, UK, Canada, and New Zealand -- have access to that same capability.

"Depending on the seriousness and nature of an incident, Australia has the capability to attribute malicious cyber activity in a timely manner to several levels of granularity -- ranging from the broad category of adversary through to specific states and individuals," Bishop said at the launch of Australia's International Cyber Engagement Strategy last Wednesday.

DETERRENCE

[EVIDENCE ABOUT US OCOS SHOWING US RESOLVE AND DETERRING MORE ATTACKS IN THE LONG TERM]

https://www.jstor.org/stable/26271529#metadata_info_tab_contents

If we fail to take these actions, alternative avenues will be pursued and leave offensive cyber operations behind. In fact, this is already happening as frustrated commanders rely on relatively simple and quick kinetic solutions. Agencies are also using different authorities to accomplish the same results without having to battle the same restrictions. If faced with a choice—destroy it

now via a kinetic strike or wait some days, weeks, or perhaps even months for a cyber operation to potentially achieve the same effects—it seems clear which choice commanders will make. It does not have to be this way. If the proposals discussed above are implemented, offensive cyber operations can actually begin to move at the speed of light and benefit the commanders who most need them.

Kevin **Freiburger**, August 27 **2019** On the offense: How federal cybersecurity is changing, GCN, https://gcn.com/articles/2019/08/27/cybersecurity-offense.aspx,
Offensive cybersecurity means planting cyber "weapons" deep within adversaries' networks. The U.S. doesn't need to actually use cyber weapons for the strategy to work. Instead, the mere presence of a cyber weapon shows adversaries that the U.S. has the capability to inflict damage. Offensive cybersecurity tactics act as deterrents, reminiscent of gunboat diplomacy or the mutually assured destruction scenarios contemplated in conventional nuclear weapons war games. **The U.S. currently deploys offensive cybersecurity strategies with Russia. In what is a more aggressive strategy for the U.S., officials confirmed that they have placed the equivalent of digital land mines into Russia's electric power grid to serve as a warning to President Vladimir Putin and as a demonstration of Cyber Command's power.** This particular effort adds to a previous cyber strategy already in place meant to overwhelm the computer systems at Russia's Internet Research Agency -- the entity responsible for the 2016 election meddling. O**ffensive cyberattacks are conducted remotely, shortening the time for deployment and costing less than conventional weaponry and military infrastructure.** And in some ways, offensive cyber strategy has the potential to save lives. In June of this year, the U.S. called off a conventional weapons counterattack on Iran due to the high potential of human casualties. The DOD chose to instead move forward with an unnamed cyberattack

https://medium.com/@z3roTrust/projecting-military-power-through-cyberspace-using-offensive-cyber-attacks-2b602e6c1df1- send a signal evi

Or, a cyber attack could also serve as a warning to a foe that there is more of this to come if they do not cease their actions and change course in the same way economic sanctions do. Following a well-executed and time-coordinated cyber attack, there may not be ships off the coast line or American troops kicking down doors, but the adversary has a clear message from the American government and there was no collateral damage loss of life or cost to the environment.
https://www.cgai.ca/offensive_shifts_offensive_policies_cybersecurity_trends_in_the_government_private_sector_relationship

But most of the former intelligence and cybersecurity officials who spoke to WIRED about Cyber Command's operation say that the key significance of turning off the IRA's internet access was not the immediate outage it created,

but the larger message it communicated to the Kremlin—amplified further by the classified operation now having leaked to the *Post.* The mere action of demonstrating that level of control over the IRA's network makes clear that the US government could have done worse, such as destroying computers or leaking the IRA's internal communications.

"This operation was nothing more than a signal to the Russians that what you did was not acceptable, and we'll take action and use some element on the spectrum of force to counter that," says Sergio Caltagirone, a former technical lead at the NSA who has since worked in threat intelligence at Microsoft and security firm Dragos. "You start small to get the message across: If you do this, we will do something. If they do it again, you ratchet up the pain a little more."

Time will tell if the signal has any long-term effect. But Kenneth Geers, a cybersecurity-focused fellow at the Atlantic Council, argues that it's just the first step in establishing an "escalatory ladder" that's understood by US adversaries, with increasing responses for every violation. "It says,'We're going to hinder your ability to do this. We know who the people are, where the network is, how they're doing it, and we can stop you,'" Geers says. "This is a message that will be heard loud and clear in the Kremlin."

Smeets 18 of Stanford University notes that offensive capabilities expand military options and allow more flexibility.

For example, **Doffman 19** of Forbes writes that Trump was able to pull back from a retaliatory military strike against Iran and instead used a cyber operation.

The reason is clear, as **Smeets** continues that in cases when force is required, offensive operations offer a flexible, minimal, and precise way to quell tensions.

In a world without cyber operations, the United States would be forced to take costly and escalatory measures, which **Dilanian** finds would trigger immediate Iranian retaliation to the global economy through the escalation of conflict in the Middle East and blocking trade in the Strait of Hormuz.

This would have a devastating impact for the entire world.

Tan 19 writes that increased tensions from the strike Trump canceled on Iran would have raised the prices of oil by $5-$10 per barrel - a drastic shift.

As a result, **Westhoff 19** explains that an increased oil price increases the cost of transportation and production, ultimately leading to higher food prices.

Unfortunately, higher food prices can have adverse outcomes on impoverished people, as **Anderson**, director general of the International Food Policy Research Institute finds that even short term spikes in food prices can put food necessities out of reach for 1.1 billion people in developing countries.

Our Sole Contention is reducing conflict.

Subpoint A is de-escalation.

The existence of Offensive Cyber Operations, or OCOs, gives the US military flexibility during confrontations.

Jensen of the Washington Post '19 writes that OCOs allow the US to respond to provocations effectively without using the military which is highly escalatory.

For example, Smeets of Air University '18 writes that when Bush was contemplating using military force against Iran in 2006, cyber operations provided him with a 3rd option to attack Iran without causing war.

The impact is entrenching conflict

Absent the ability to use OCOs, the US would be forced to use its military increasing the likelihood of conflict.

Just looking at Iran.

War of Vox '19 finds that hundreds of thousands of people would die in a war between both countries.

Apart from stopping escalation OCOs also allow the US to send credible signals to other countries.

The Medium '19 writes that cyber attacks could serve as warnings that there is worse to come in the future if countries don't cease their actions.

For example, Wired '19 writes that in response to Russian hacking our cyber attacks were able to send the signal that the US has the ability to retaliate to any harmful action taken against it, deterring future aggression.

Indeed Pollard of LF ‘19 finds that these attacks were able to take out russian capabilities without any significant blowback.

Fl to trump won’t intervene
https://www.outsidethebeltway.com/trump-abandons-restraint-in-foreign-policy-in-favor-of-interventionism/
https://www.outsidethebeltway.com/trump-taking-ill-advised-militaristic-position-regarding-iran/
https://theintercept.com/2019/09/17/saudi-arabia-oil-field-attack-trump/

za/t Iran/anyone fcking retaliated

1. Better than a physical war
2. And again, iran’s retaliation was significantly less w OCOs, we aren’t saying it creates a positive result, it takes a middle position that provides the best outcome

Second link is more about general they are emboldened to do more bad shit before Trump's new policies changes

1. Defense is hella hard because they can find on exploits--->
2. Does Not help with iran-->cyber defense can stopping attack on us
3. Cyber offense-->now know we know how to defend
4. Cyber defensive sucks

a/t norms not working yet

Well yeah we haven’t had hella good OCO’s yet - no one listens to NK bc their nuke programs trash

a/t US are low threshold so why would russia/china care