A/2: AFF

Overviews

Defense Prereq.

1. Wolff of New York Times finds: Our current shift to an offensive approach is detracting resources and attention from defense and risk management, which is why only 2% of our personnel work in defense right now. Problematically, Donnelly just a few weeks ago

indicates that offense is not sustainable without a proper defense, because it's the only way that you can protect the systems that sustain our offense in the first place. Offense just isn't sustainable in the long term.

Ineffective/Perception

1. OCOs might sound very appealing, but all of their arguments are purely hypothetical. Valeriano indicates that only 4% of OCOs produced even just a temporary concession, and that operations don't ever truly change the behavior of a target state because there are no long-lasting effects. However, the perception of the US attacking prompts retaliation. Garrett of IndustryWeek reports that last year, there was a 350% increase in ransomware attacks against the US. If you look at the empirics, OCOs just do not deter conflict, but they make things worse.

Going in Circles

1. Goldsmith of the New Republic finds that the US operations pioneered and was the root cause of cyber warfare normalizing. Because of this, Garrett of IndustryWeek reports that last year, there was a 350% increase in ransomware. Thus, it's counterintuitive to vote for them and try and solve back for the problem that they themselves are causing. The best way to actually prevent any more attacks is to negate and actually have cooperation, but that can only happen if we tone down our offense.

A/2: Preemptive Strikes

1. Valeriano indicates that only 4% of OCOs produced even just a temporary concession. He concludes that operations don't ever truly change the behavior of a target state because there are no long-lasting effects.
2. Turn. Defense works better. Maness of Northeastern University finds that Russian cyberattacks against the US declined significantly during the Obama administration when we focused on defense to the point where there were no credible cyber threats from any country.

A/2: Deterrence

1. Lynch of Fifth Domain explains that it's impossible to prove that deterrence is ever causing an effect. Our opponents cannot prove that [country] will not attack specifically because of the deterrent effect caused by the US. There are a ton of alt causes to why a country does not want to attack.
2. Delink. Singer of Foreign Policy explains that deterrence only existed in the Cold War because both the US and Russia had about the same weapons. However, the status

quo is different because the US is uniquely the most vulnerable to cyber attacks due to our dependence on the internet.

3. Attacks are mostly from individual attackers--they are not conducted through a nation's consensus. This means that even if it goes against the target country's interests to retaliate, it is impossible to deter an entire administration because all it takes is one person.
4. Historical precedence proves otherwise. Fazzini of CNBC reports Israel bombed Hamas as a direct means of retaliating against their OCOs. Deterrence didn't work here.
5. Stuxnet
6. Turn. Singer continues, that attempts at cyber deterrence are even worse, because there are over 60 countries conducting attacks and it's impossible to identify all the actors. Thus, because countries do not get exposed, and because it only takes mere seconds, they are even more willing to conduct attacks without risk.
7. Turn. Net Politics in 2019 finds that China and Russia will always see any attack from the United States as preemptive, leading to misinterpretation which will forever cause a cyber warfare. That's exactly why attacks are still increasing as we speak.

A/2: Russia

1. Delink. European Leadership Network in 2018 explains that deterrence only works if the country is willing to back down after the US attacks it, but Russia will never be willing to do so because of three reasons:
    a. Russia has already spun the narrative that the West is unceasingly attacking them and they need to fight back
    b. Russia doesn't believe in deterrence and isn't willing to just accept it and compromise its own capabilities
    c. Russia is geopolitically realist and wants room to maneuver because it uses its own OCOs and espionage attacks to project power, capture Western attention, and deter NATO

    That's why even after US attempts to deter Russia with OCOs, Russia continued to lead the biggest ever hack against the US during the 2016 elections.
2. Delink. Wired in 2019 writes that Russia is exceptionally good at covering their tracks, so they have nothing to lose. In fact, Russia has used Iranian proxies and impersonated Iranian hackers in the past which confused the US.

A/2: China

1. Segal of the Council on Foreign Relations reports that China literally stated that US "deterrence" doesn't deter them because, despite US advantages, China can easily recover from US attacks at any time, and US defense is so weak that China could always hit it equally as hard.

A/2: North Korea

1. Delink. Thompson in 2018 writes that because the US needs North Korea to sign a denuclearization deal, they know they have leverage over the US so no cyber operation will ever be damaging enough to deter North Korea in case it endangers chances of a denuclearization deal. That's why he concludes that US efforts to deter North Korea have largely failed.
2. Turn. Vishwanath in 2019 explains that North Korea has the capability to steal US cyber operations and use them for itself. Our OCO's won't deter, but it instead it'll cause even more harm. For example, in 2017 North Korea crippled millions of computers in more than 150 nations in a matter of hours.

A/2: MAD

1. Briens of the Medium explains that nuclear terms such as mutually assured destruction can't be applied to cyber warfare because attacks are anonymous and can happen in mere seconds. He concludes that good defense is the only way to truly deter nations.

A/2: FoPo

A/2: Iran

1. Alt causes as to why Iran won't attack. In fact, Giglio 19 of the Atlantic reports that Iran only backed down in a military conflict when the U.S. military heavily retaliated with Operation Praying Mantis, sinking five Iranian vessels and America's downing of the civilian airliner Iran Air Flight 655.
2. Delink. Schneider 19 of the Washington Post writes OCOs are unlikely to deter Iran because the costs to Iran are not significant enough to deter them from targeting US infrastructure.
3. Delink. Doffman in 2019 explains that deterrence only works if the US can strike back against attacks harder than the other country can but Iran and China are starting to cooperate against US cyberattacks and the US doesn't have the power to take on two countries at once
4. Delink. Lawson 19 of FifthDomain reveals that we've been in a cyber conflict with Iran for nearly a decade, yet we have not seen them deterred at all. They keep retaliating.
5. Turn. Lawson of the Fifth Domain in 2019 writes American OCOs in Iran only create more detrimental outcomes. After the US launched OCOs in response to Iran's downing of our drones and disruptions in the Strait of Hormuz, American cybersecurity companies reported spikes in cyberattacks against the US government and critical infrastructure.

6. Turn. Abdollah 19 furthers that because of our escalatory actions towards Iran, the number of attacks on all sectors of the US economy have increased, creating devastating outcomes in fields such as oil and gas.
    a. The reason is because Iran themselves have come out and declared that they will always pursue any aggressor.

A/2: NATO

1. The Department of Defense constructed the Cyber Mission Force in 2015 to be able to carry out OCOs for security interests even when focusing on defense. Voting neg does not mean that all OCOs go away, it's just that there will be a better balance of offense and defense. The second implication here is that if OCOs are inevitably going to exist in both worlds, then their argument is nonunique because relationships should go up regardless.
2. Trump has literally lifted all regulations to heavily focus on OCOs against adversaries. He's been doing so for three years now, we should've seen some semblance of their impacts triggering.
3. Nonunique. Tucker of CDN writes in 2019 that NATO is already building a cyber command to be fully operational in 2023, and will integrate OCOs regardless of what America does.
4. Turn. NATO creating its own cyber force is on-net better because the US is extremely aggressive under Trump, but Tucker of DefenseOne in 2019 explains the only way NATO is allowed to respond to a cyberattack is by getting a collective approval from all its members which has only happened once in the history of NATO. This means that the alternative has much less chance of conflict and escalation.

A/2: Prevent Proliferation

1. They can't prove that without cyber attacks, Iran would've nuclearized and they can't prove intent of use on the nuclear war.
2. There is no uniqueness on their case as Brewer in 2019 finds that no country that is absent nuclear power is currently developing nuclear technology and **the only country that has the capability is Iran.** The reason this is true is because many countries are part of international treaties that have political barriers and harsh penalties.
3. Turn on Iran. OCOs result in direct economic retaliation. After the Stuxnet attacks, Glaser in 2017 finds Iran was motivated to launch multiple waves of cyber-attacks against American banks and Saudi Arabia's Aramco oil company. These attacks were devastating as Glaser concludes Iran's retaliatory cyber-attacks were "probably the most destructive attack the private sector has seen to date."
4. Turn on Iran. Offensive Cyber Operations expose vulnerabilities that make institutions more likely to place better protection on nuclear and weapons facilities. This is empirically true in Iran as Blaustein in 2013 writes that after Stuxnet, Iran was more cautious with overall protection on nuclear facilities, leading to increases in nuclear

capacity. He concludes that Stuxnet was of net benefit to Iran if its government wants to build a bomb or increase its nuclear-weapons potential

A/2: ISIS

A/2: General

1. No long term solvency. Raston of NPR in 2019 reports each time American OCOs take down one ISIS server, they simply restart a new server elsewhere. He continues ISIS is a consistent moving target and has sufficient resources to ensure they always find ways around US operations.
2. Delink. Michaels 18 of USA Today finds that ISIS has lost 98% of its land due to US military successes. However, he concludes that this was due to the US backing local fighters with airstrikes and advisors, NOT because of OCOs.

A/2: Leadership Decap Uniqueness

A/2: Take Down Operations

1. There are alternative reasons as to why ISIS went on the decline, such as the Kurdish rebellion, other nations taking action, and US troops and drone strikes. That's exactly why ISIS lost 96% of land under Obama, when we didn't focus on OCOs.
2. Valeriano indicates that only 4% of OCOs produced even just a temporary concession. He concludes that operations don't ever truly change the behavior of a target state because there are no long-lasting effects.
3. Delink. Finley of Wired finds that it's impossible to selectively shut down ISIS's internet systems unless they cut off an entire region. That's exactly why the US has been unable to shut down their access even with our current technology.
4. Turn. Davis of Business Insider explains that our constant efforts have forced ISIS to decentralize and expand to new locations around the world, killing thousands in over twenty countries. Prefer our evidence because it analyzes the whole region.

A/2: Propaganda

1. Delink. Katz of Wired this year explains that OCOs were only able to take down the biggest media platforms like Facebook, Twitter, and Youtube. She concludes that ISIS just switches to lesser-known messaging apps to continue to proliferate propaganda.
2. Delink. David of Time reports that propaganda is literally still increasing, even though we keep deploying OCOs. The reason is because the US can only do so much against the sheer volume of their propaganda. We can't take down all of them.
3. The Wall Street Journal reports that in response to American efforts to take down their propaganda outreach, ISIS has turned to encrypted communication networks that the US can't take down, providing them a new avenue to funnel propaganda

4. ISIS will always try to keep their numbers high. This means that even if we take away one small sector of their recruitment process, they'll just pivot to other means of recruitment. They don't tell you why slashing propaganda is the choking point.
5. Turn. The alternative is more traditional methods of recruitment through kidnapping children and purchasing people, which is on-net worse.

A/2: Disrupting Transactions

1. Kenner of the Atlantic finds that as ISIS is adapting, they are switching to cash and brokers to become more discreet with their transactions.
2. The internet does not matter because a vast majority of ISIS capital comes from acquiring new territories and taking over capital systems. This means that fund transfers don't matter in the first place if you don't have land, which is their primary means of acquiring revenue.

A/2: Coercive Diplomacy

A/2: Israel

1. Carey of CNN just three days ago writes that Israel has been actively militarizing, continuing to use air strikes and rocket fire to carry out assassinations.
2. Doffman of Forbes finds that when Hamas sent in cyber operations against Israel, they retaliated by sending drone strikes. He concludes that quote, "a precedent has now been set for immediate military retaliation against cyber attacks [in Israel].
    a. This means that retaliation has happened and there's no reason why they won't ever do it again since their geopolitical agenda remains the same
    b. It proves that the realm of cyber warfare is forever changing which is why you can't just vote off of some past examples

A/2: Other

A/2: Economy

A/2: Norms

1. Finnemore of Carnegie explains that a norm only exists when the countries agree with the same particular beliefs, and that the US's strategy of just announcing a norm does not actually create one. That's why they failed in the past when trying to create a norm against cyber espionage. Voting for the aff doesn't change the ideology of these countries.
2. Finnemore concludes that the only time a norm actually started taking shape was when countries signed onto deals through cyber cooperation. The reason is because the

countries have no obligation to follow the norms insofar as states always prioritize their own self interests. History is on our side and we solve better.

A/2: Replace Conventional War

1. It's not like if we didn't have OCOs we would be solely using conventional warfare. It's extremely politically unpopular, and the federal government would probably be using alternative means to combat our geopolitical rivals. They can't prove the inherent tradeoff, even if their evidence says OCOs led to the decreased usage of conventional warfare.
2. Even if the US substitutes conventional war with OCOs, the increased use of cyber offense triggers conventional war in other parts of the world. For example, Fazzini of CNBC reports Israel bombed Hamas as a direct means of retaliating against their OCOs.
3. Their argument just assumes the US is gonna wage war against all other countries without OCOs. To some extent, cyber operations will always exist in either world, which means there's never an incentive for the US to suddenly resort to conventional warfare.
4. The reason conventional war isn't happening right now, is because the dynamic has changed, is because every country has decreased their conventional warfare. Switch to nukes, that's why people don't invade the US right now.

A/2: Hormuz/Oil

1. Nonunique. Vivian Yee of New York Times reports in 2019 that Trump has already sent warships and bombers to the Persian Gulf and has eliminated waivers that allow other countries to purchase Iran's oil. Essentially, Iran cannot export to other countries with or without OCOs.
2. Delink. Ratner of the Congressional Research Service reports in 2018 that in the event of an oil disruption, the US has held 660 million barrels of crude oil in a government held stockpile of crude oil to be used to offset supply disruptions. Their argument doesn't really lead to the disastrous effects that they talk about. We've already planned for this.
3. Delink. Jonathan Saul of Reuters explains that Iran cannot close the Strait of Hormuz for three reasons.
    a. The cost of closing the strait would hurt Iran's economy more than anyone else. 2/3 of Iran's government's budget comes from exports from the strait.
    b. Closing the strait would reduce the leverage Iran has over the region as it pushes Persian Gulf countries to the US. Iran gets more from threatening to close the strait than closing it.
    c. In order to close the strait, Iran would be forced to place mines in the sea lanes every day in order to maintain the disruption. However, Iran's navy does not have the confidence nor the capability for prolonged submarine operations.

A/2: Flexibility/Gray Zone

1. Turn. This effect for countries to respond without causing any material conflicts discourages diplomacy. Marks of NextGov in 2018 explains that offensive cyber operations are seen as an easy way out. They can ratchet up tensions without causing conventional war, which discourages diplomacy and negotiations.

A/2: Hospitals

1. This is being solved for in the status quo. The Hipaa Journal writes in 2019 cybersecurity budgets have increased, new technology has been purchased, and healthcare organizations are getting better at blocking cyberattacks and keeping their networks secure.

A/2: Protecting the EU

1. No need. The Global Commission on the Security of Cyberspace finds that the EU in May of 2019 adopted the EU Cybersecurity act, dedicated to protecting the public core internet that controls infrastructure.

A/2: NEG

Overviews

Correlation Not Causation

1. Their arguments are purely correlation not causation. Lotriionte explains that the world is constantly gravitating more towards efficient means of geopolitical projection. For example, we went from bayonets to tanks and now to cyber warfare, which is why Suman 16 writes that the overall amount of cyberattacks around the world went up by 1300% even under the Obama administration when we focused on defense. Thus, their arguments about countries using more cyber offense is not a direct cause of our federal government's usage, but rather just a general global trend.

A/2: Economy

A/2: Costs

A/2: Hurting Relations

A/2: Economic Ties

1. Some countries will never truly sever ties with America because the nations are too economically interdependent on each other. They're merely just forms of power projection in order to gain some concessions.
2. Alt causes as to why their relationships are worsening, they cannot give evidence that says OCOs are the sole reason.

A/2: Treaties

1. Delink. Mazanec of Strategic Studies finds that it's not in Russia and China's best interest to agree to such treaties because they are geopolitically realist nations and use cyber operations to power project by compromising the US.
2. The Council on Foreign Relations reports that after negotiating for almost ten years, the cyber treaty between US, China, and Russia collapsed because of their differing ideologies. That's exactly why these countries are still attacking to this day.
3. Their argument is that our focus on offense is the reason why countries are not signing onto deals and treaties. However, it's not like offense goes away when you vote for the neg. If countries really wanted the US offense to die down, they would've just signed onto the treaties by now.

A/2: Escalation

1. Nonunique. Countries will always deploy OCOs to try and gain a geopolitical advantage. That doesn't change when you negate.

A/2: Retaliation [General]

1. Delink. Jensen of Washington Post writes that actors always seek to limit the risk of escalation, and that countries are more likely to use economic or diplomatic alternatives before cyber responses.
2. Delink. Valeriano of Cato Institute this year finds that 67.4% of cyber operations don't see any cyber-retaliation within one year. Even if they do go through, the cyber-attacks were substantially less severe than before.

2. Delink. Borghard of Strategic Studies in 2019 finds that no one has ever died from the last 30 years of cyber operations and that even in the worst case hypothetical scenario, the casualties would be minimal. He even takes into account attacks on power grids and says the worst possible cyber attack is still nothing compared to a basic conventional attack.
3. Delink. Healey of the Journal of Cybersecurity finds that offensive cyber operations are actually stabilizing because we bring the fight to our adversaries, which isn't escalatory because countries know they do the same thing to us. By bringing the fight to our enemies we force them to spend on defensive cyber operations which in turn limits the amount of offensive operations committed on the United States.
4. Barnes of New York Times writes that the US conducted OCOs on Iran in June to stop their attacks on oil tankers, and Iran has not retaliated because they're still recovering. He concludes that our attacks signal our enormous capabilities and show to Iran that they could never possibly match us. Their argument doesn't align with reality.
5. Turn. Intent does not equal capability. Goodman of Strategic Studies explains that preemptively taking down our adversary's military systems is better because it means they can't retaliate, no matter how pissed off they get.
6. Turn. Even if retaliation happens, we provide a valve for de-escalation through flexible responses. Jensen of the Cato Institute writes in 2019, cyber operations act as a release valve for current crises. Rival states use cyber operations as a substitute for riskier military action, which reduces tensions. They allow us to do something without utterly crippling the other country and provoking war.

A/2: Repurposing

1. Jinghua of Carnegie in 2018 explains that the US is always growing faster than these other countries, so it doesn't matter if the countries copy an outdated piece of technology.
2. By the time other countries have taken US cyber capabilities and adapted them, our cyber operations would have advanced so much that their attacks are useless.
3. If the US is able to develop the technology, they probably know how to defend against it as well. It's literally their technology.
4. Borghard explains in 2019 that OCOs are inherently specialized to the weaknesses of specific countries. This is important because for example Person A insults a specific characteristic of Person B. Person B cannot repeat the same insult back at Person A because it doesn't apply. The same idea applies to OCOs as they are targeting specific characteristics of their target.
5. Incentive-wise if it was this simple, the US gov would never deploy an OCO that could destroy itself. Let's go back to the previous analogy of the insults. Deploying an OCO which could be reverse engineered and target the US is like Person A insulting Person B's shoes while they are both wearing the exact same pair. That insult could so obviously be hurled back and would completely backfire.

A/2: Chinese Backlash

A/2: North Korea

1. Mariani of the International Affairs Institute explains in 2017 that North Korean nuclear weapons are for political purposes of deterrence and negotiation only, similar to the United States' strategy. They are merely a bluff for nuclear diplomacy, as the nukes are their only source of international legitimacy and the only reason countries sit at the table with them.
2. A North Korean attack assumes that they are an irrational actor. Mark Bowden of the The Atlantic explains in 2017 that Kim Jong Un is not stupid and strategically places missiles to control over his people as a dictator. They will only attack when there is a rational reason to do so, such as a last ditch effort to save the regime. Our OCOs don't push them to the extremes like that.
3. Thomas Lee of CNN furthers this in July of 2017 finding that Kim knows launching a nuke would mean certain annihilation, and he values his rule above everything else, so he would never actually launch his nukes. He isn't suicidal.

A/2: Kinetic Warfare

1. Illogical. Lewis '18 finds that the whole point of engaging in cyberattacks is to increase deterrence through the cost of conflict. The whole point of cyber attacks is to pivot away from conventional war and avoid losses and casualties.
2. No Probability: Lonergan '19 finds that the vast majority of malicious cyber operations occur well below the threshold of physical war or impacts. No kinetic war will be triggered specifically because of an OCO.

A/2: Grids Impact

1. What Sagenweil in 2019 finds is that the scenario of our grids being attacked was literally a doomsday opinion piece that got misconstrued by media headlines. He concludes that squirrels, cats, and raccoons have a worse effect on power grids.
2. Not true. It's not like one grid controls all of US's infrastructure and the flip can just be switched off. Baker of the University of Kansas explains that electrical system experts are aware of the risk but say the attacks just won't happen because the grids are extremely diversified and chock-filled. That's exactly why there has never been a successful grid hack that caused a blackout.
3. Mitigate. Even if they do attack, Preston in 2016 finds that US electricity systems are already equipped with the tools to recover from sudden disruption and damages, which is why he concludes US energy grids are some of the most reliable around the world. Even further, NCLS in 2018 finds that the US has been increasing legislation in order to prepare for grid repair in the face of disasters.

A/2: Arms Race

1. Borghard in 2019 explains that all claims of cyber operations leading to the escalation of conflict are greatly exaggerated. He furthers that despite widespread use of offensive cyber operations among world powers instances of escalation are literally nowhere to be seen.
2. Delink. Arms races only happen in theory, but some countries just aren't able to keep up with the race. For example, Mugg of National Interest writes that after economic sanctions and a collapse in oil prices, Russia's economy sank which led to a 12% nominal reduction in defense spending by 2018.
3. Nonunique. Griffiths contends that 120 countries were developing cyberweapons, which means that the United States was not the root cause of countries expanding their arsenal. It was inevitable due to the nature of global warfare shifting to cyber.

A/2: China

1. Delink. Even if China increases spending, the funds only go to defense. Jinghua in 2019 finds that China does not want to engage in an arms race with the US. They have adopted an ideology of "active defense" where they will only attack if attacked first. All current cyber upgrades are only to keep up with military trends and to ensure that China can check back on local conflicts. Despite previous US OCOs, China still maintains a strict defensive strategy showing that they don't want to respond offensively.

A/2: Russia

A/2: 331% Impact

1. Indict. The 331% increase in probability of war is only going from .01 to .03%. It's a drop in the bucket.
2. Indict. The evidence is analyzing two countries going from a rivalry without an arms race to a rivalry with an arms race. However, we still have arms races in other fields, such as missiles and technology development, so this impact still materializes regardless.

A/2: Arms Race

A/2: Miscalc

A/2: Russia

1. Delink. We have mechanisms to prevent this escalation. Banco in 2019 writes that the US and Russia have diplomatic hotlines with one another, which can be used if the two countries are ever on the brink of a war.

A/2: North Korea

1. Sanger of the NYTImes reports that Trump has opened a diplomatic hotline with North Korea to maintain communication and prevent escalation. This means the risk of conflict or miscalculation is low because both sides can talk to each other.

A/2: Trade-Offs

A/2: DCOs

1. Literally no examples or empirics of DCOs working historically
2. Jacob Olcott, a former counsel to the Security Committee, has come out and stated that more bad things happened than good under Obama and that making everything more secure changed nothing.
3. The Fiscal Times corroborates that cyber attacks drastically increased during Obama's presidency by 448%.
4. Marks of Georgetown University explains that some of the worst cyber attacks in history happened under our focus on defense. For example, North Korea dismantled Sony, China stole 22 billion IP patents, and Russia hacked our power grid, killing thousands. Which is why the Guardian writes that Obama switched to OCOs in 2013 because of repeated failures with defense.

A/2: Other

A/2: PMCs

1. Loven from the University of Nebraska finds that statistically, PMCs have little to no statistical impact on the duration of a war. The reason is because governments generally choose the corporations they believe can solve military conflicts quickly and efficiently

This paper examines the effect of private soldiers, both Mercenaries and Private Military Contractors (PMC), on the duration of civil wars in Africa from 1960 to 2003. **Linear regression is used to determine if private soldiers increase or decrease the duration of** civil **wars. Ultimately** ***it is*** **found they have little to no statistical impact. This is contrary to the expectations of the theoretical literature on private military contractors, some of which expects private soldiers to profit from war and seek to lengthen duration**, and some of which expects the use of additional private soldiers to shorten the duration of wars.

PMCs might be expected to want to profit from a civil **war,** particularly a long civil war. The longer a war, the longer contractor's services will be needed and this provides job security and a steady paycheck. **However, those looking to hire PMCs will look for those who have the best reputation for achieving** the desired result of **victory, which will bring an end to the** civil **war, and can do so most efficiently**. As utility maximizes, **PMCs** might **decide it is better to end wars quickly and therefore ensure future contracts rather than drag out a current conflict. The cost/benefit analysis would indicate a preference for long term goals rather than short term goals.** Continuing in business and developing the reputation needed to be competitive would be a key business strategy.

2. PMCs only bad if there are troops on the ground. OCO PMCs preferable to conventional PMCs.

A/4: NEG

A/4: Obama Switched to OCOs

1. The Council on Foreign Relations in 2017 explains that Obama's attempts at offensive deterrence failed, and Russia's hacking episode proves offense is ineffective. They conclude that improvements in cyber defenses were the apex of our program, and the transition was an embarrassing symbol of public failure to protect against threats.