General **3**

AFF **3**

A2: Preventing Israel from going to war 3
A2: Cyber Attacking Iran's Nukes 3
A2: Strait of Hormuz 4
A2: Preemptive Denial/Deterrence 5
A2: Deterrence by Capability 6
A/2: Russia 7
A/2: China 7
A/2: North Korea 7
A/2: Iran 7
A2: Creating Global Norms 8
A2: NK Nuke Program 10
A2: IP Theft/CH Hacking 11
A2: Substitutes for Intervention 12
A/2: Deters Aggression 12
A2: ISIS 12
A2: Boko Haram 15
A2: Strengthening NATO 15
A2: Satisfying Saudi Arabia 16
A2: NK Stealing money for Nukes 16
A2: Stuxnet works to reduce their OCO 17
A2: Drone strikes become more accurate 17
A2: Rohan aff 17
A2: Norm Setting 17
A2: Coercion 19
A2: Setting a threshold / Adaptive Learning 19
A2: Find Vulnerabilities to solve em 20
A2: Dark Web OCOs 20
A2: Shut Down Iran radars 21

A2: Evaluate Only Past Actions 21
A2: Persistent Engagement takes out Capabilities 21
A2: St. Johns Aff 22
A2: Ports 22

NEG **23**
A2: Direct Escalation 23
A2: Military Tradeoff 26
A2: Reengineering 26
A2: Normalizing OCOs 27
A2: Angering Iran / Cyber war 27
A2: Arms Race w Russia 28
A2: Taiwan Scenario 29
A2: Defensive Tradeoff 30
A2: OCOs Not Effective (general) 32
A2: Weapons get stolen 32
A2: OCO's disrupt norm breaking 33
A2: Provoking NK cyber weapons 36
A2: Trump hella more aggressive 36
A2: PMC 37
A2: Russia Leaves Internet 39
A2: Dumb Iran arg 39
A2: St. Johns Neg 41
A2: Left of Launch 41
A2: SMH intel link 42

General

AFF

A2: Preventing Israel from going to war

1. NI 19': OCO might alleviate it in the ST, but in the LT they will get it; the incentive to get a nuclear weapon still exists for Iran so Israel down the line will cause war.
2. US moving troops into the region so that assures Israel.
3. NI 19': Only do a preemptive strike if it was clear that confrontation was going to happen; we link in through escalation link.
4. Israel has no leader rn rlly so they can't even go to war rn.

Now, faced with the increasing likelihood of war, Israel seems to be heading again towards the conclusion that a preventive strike against Iran is inevitable, as Israel's operations against the Iranian nuclear project and its sporadic attacks on Iranian proxies in Syria and Iraq, while operationally successful, have not succeeded in deterring Iran from: (1) expanding "proliferation-sensitive activities [which] raises concerns that Iran is positioning itself to have the option of a rapid nuclear breakout"; (2) continuing its incursion into Iraq, Syria and Lebanon. Thus, "undermining the sovereignty of its neighbors"; (3) developing and transporting precision missile technology, principally to its Lebanese proxy, Hezbollah.

A2: Cyber Attacking Iran's Nukes

1. Cato Institute writes that Stuxnet failed to stop Iran's Nuclear program, writing that after Stuxnet their nuclear progress saw a 10x increase in growth. That's why despite our efforts the past 10 years cyber attacking Iran, their Nuclear program has continued to grow.
2. In fact, our cyber attacks on Iran are the reason why they continue to develop. Glaser in 2017 writes that Iran was willing to negotiate long before Stuxnet, yet after we attacked

them, they double downed on their Nuclear program in order to prove they wouldn't be bullied into stopping.

3. Stuxnet drew blowback. DO 17' finds that Stuxnet motivated Iran to launch devastating attacks on oil supplies and American banks.
    a. This links into their oil impact by disrupting major oil producers, at best its non-unique.
    b. Other banks are hit meaning that global financing of __ is harder to do.

In the aftermath of Stuxnet, and indeed right up until the November 2013 Joint Plan of Action interim agreement in which Iran agreed to temporarily freeze portions of the nuclear program as negotiations with the P5+1 continued, **Iran's number of operating centrifuges and stockpile of enriched uranium continued to grow.** From 2008 to 2013, Iran's stockpile of low-enriched uranium grew from 839 kilograms to 8,271 kilograms, **almost a ten-fold increase. "At best,"** according to the University of Toronto's Jon Lindsay, **"Stuxnet thus produced only a temporary slow-down in the enrichment rate itself." Other experts are even more skeptical.** Ivanka Barzashka, Research Associate at King's College London and a Fellow at Stanford, argues that "evidence of the worm's impact is circumstantial and inconclusive." Brandon Valeriano and Ryan Maness, in their book Cyber War Versus Cyber Realities contend, **"It is wholly unclear if the Stuxnet worm actually had a significant impact on Iran."**

Iran's willingness to make concessions in return for American accommodation makes the utility of Stuxnet seem dubious. According to Trita Parsi, the president of the National Iranian American Council who has interviewed Iranian officials on the issue at length, **Iran was deliberately doubling down on its nuclear program in order to show the West that the coercive approach would not work in the absence of diplomatic concessions.**

Second, Stuxnet drew blowback: it motivated Iran to launch multiple waves of cyber-attacks against American banks and Saudi Arabia's Aramco oil company. Then-Defense Secretary Leon Panetta, in a hyperbole typical of official statements on cyber security, said Iran's retaliatory cyber-attacks were **"probably the most destructive attack the private sector has seen to date."**

A2: Strait of Hormuz

1. OCOs are also just one use meaning that once we use cyber operations Iran can just patch those vulnerabilities once we use weapons which is why there is 0 long term closure.
    a. Furthermore because we are targeting suck specific systems they are not infinite vulnerabilities for these systems, over time as we patch those vulnerabilities the systems became generally unhackable.
2. Can just use ships don't need intricate technology to stop these ships.
3. Their end impact is also just a reason why Iran would never block the strait of hormuz in the first place.

A2: Preemptive Denial/Deterrence

1. This triggers the link in our first argument, when we persistently engage with our enemies they perceive it as the US trying to take out their capabilities, so rather than stopping their attack the Ellers evidence says that countries would realize this and have to strike back first to get the upper hand.
    a. The Iran example is good where; we attacked their electronics and stuff, but in return Iran even further developed their cyber weapons program and there was a marked spike in retaliation. Countries are always going to have this desire to stay ahead of the US, and developing our OCO's only pushed them to raise their capabilities to match.
2. Our second warrant also responds here because even if we use OCO's to destroy their weapons they just steal our weapons for them to use, take China for example we used Eternal blue to try to take out their weapons and in return they just took our weapons.
    a. On the net there's no difference because these countries still have weapons.
    b. It's worse because the threshold for them to use it is so much lower because they didn't spend anything to use it.
    c. The weapons that really matter are the ones we develop and then these countries reengineer to use against us, those are the most dangerous, the ones they have currently are super low level, the comparative is on our side
3. The ____ ev indicates that the cost to make OCOs is relatively low, so
    a. Even if we take out their weapons they'll always just make new ones
    b. The weapons can still be used, most of the cost is from r&d which is already done, so its just a matter of getting a computer
    c. They'll always have an incentive to go out there and use an OCO
4. Deustch of CSMoniter 17' ev is good here too because countries just outsource their OCO's to third parties who carry out the attack, preventing countries from being held accountable.
    a. [use example of CH not taking blame for an attack they did]
5. Cross apply the wolf evidence from our case about our defense getting worse. There are two reasons why maintaining our defense is better than deterrence by denial.
    a. It directly solves the problem of attacking rather than indirectly solving, higher probability of preventing attacks
    b. Zero risk of further attack, we develop defense no one feels threatened
    c. It actually decreases the incentive to attack because if countries perceive that their attacks aren't going to make actual damage they won't take the risk of escalating b/c they know they can't win in the long term.

https://cams.mit.edu/wp-content/uploads/2017-10.pdf-super cheap shit

Bill Woodcock, a research director at the Packet Clearing House, a nonprofit organization that tracks Internet traffic, once said, cyber-attacks are so inexpensive and easy to mount, with few fingerprints;they will almost certainly remain a feature of modern warfare. “It costs about 4 cents per machine,” Mr. Woodcock said [w9] “You could fund an entire cyber-warfare campaign for the cost of replacing a tank tread, so you would be foolish not to.” In developing a strategy to counter these dangers, the Pentagon is focusing on a few central attributes of the cyber-threat. First, cyber-warfare is asymmetric. The low cost of computing devices means that U.S. adversaries do not have to build expensive weapons, such as stealth fighters or aircraft carriers, to pose a significant threat to U.S. military capabilities. A dozen determined computer programmers can, if they find a vulnerability to exploit, threaten the United States' global logistics network, steal its operational plans, blind its intelligence capabilities or hinder its ability to deliver weapons on target.

A2: Deterrence by Capability

1. The reason why we need deterrence in the first place is because of our use of OCOs. The Ellers evidence says that countries perceive our use of OCO’s as the US trying to take out their capabilities or prepare for further war and as a result feel forced to strike back first to get the upper hand.
    a. The Iran example is good where; we attacked their electronics and stuff, but in return Iran even further developed their cyber weapons program and there was a marked spike in retaliation. Countries are always going to have this desire to stay ahead of the US, and developing our OCO’s only pushed them to raise their capabilities to match.
2. Deustch of CSMoniter 17’ ev is good here too because countries just outsource their OCO’s to third parties who carry out the attack, preventing countries from being held accountable.
    a. [use example of CH not taking blame for an attack they did] Countries are just gonna attack us and not take any blame they don’t solve.
3. Our second link applies here too because when these nation states and terrorist groups hack our weapons and stuff they can just decode it so they aren’t threatened by it. The deterrence effect goes away.
4. Don’t let them link in either because rogue states and terrorist groups don’t feel any deterrence effect because 1/ the US can’t retaliate really against terrorist groups and 2/ Rogue states know the US is going to be very hesitant about intervening in them.
5. The wolf evidence from our case is also responsive here because if our defense keeps getting traded off for offense then the incentive to attack us for other states will rise over time, just because now it’s so much easier to be successful. At worst there’s no net difference, at best because to end benefit matters much more to a state than the process the amount of hacks will increase.

A/2: Russia

1. Our first link is responsive nt he impact level where the AMSP ev indicates that we're locked into a cyber war with Russia because of the need for Russia to show their resolve.
2. Russia also hides their attacks, Wired 19' specifically looks at Russia's cyber attacks and concludes that Russia uses proxies to confuse the US, having no accountability.

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.
2. Deterrence is solving a problem they created. China won't develop unless they feel threatened. The Manes ev indicates that after we demonstrated our capabilities in the Iraq war they felt forced to match, same with OCOs.
    a. History proves. The LA Times in 2017 writes that under Obama's strategy of avoiding OCO's we signed an agreement with China that reduced their hacking of us by 90%. But since Trump's shift towards OCO's IJ 19' finds that hacking from China is now on the rise again.

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: Iran

1. Fifth Domain reports that just after we cyber attacked Iran in the Summer, there was a marked spike in Iranian cyber attacks against the US. Obviously deterrence doesn't work.

More recently, in June, the United States carried out cyberattacks against Iran in response to Iranian disruptions of shipping through the Strait of Hormuz and the downing of a U.S. surveillance drone. At the same time, two cybersecurity companies reported a spike in Iranian cyberattacks against U.S. government and critical infrastructure targets.

A2: Creating Global Norms

First let's discuss our case:

Both of our warrants link into the argument.

1. If there is tit for tat escalation which boils over into conflict then no one has an incentive for norm building. In fact the new US strategy runs counter to every norm the US propagates because if countries perceive the US as trying to preemptively strike them then of course they're not going to be willing to stand down and accept agreements.
2. If OCOs start getting leaked and used more in general then the US and other actors are going to become much more wary about being less offensive and agree to low-tension norms because they feel like they have to be actively engaged to stop threats.
    a. Furthermore third parties like non-state actors don't agree to norms so even if they are created our second link still triggers.
    b. If weapons are stolen and leaked then countries like China and Russia can give those weapons to third parties to cheat any agreements without having any accountability for actions.

This is why overall the Healy evidence, which is the only evi that looks at norms with our current usage of ops, indicates that the norms wouldn't happen because we keep violating it. The weighing for our warrants versus theirs is the Jensen evidence that says concessions and coercion were working before, but since the policy shift we've been seen as preemptive and countries are going to be retaliated against.

Then on specifics:

1. Cato Institute writes in 2018 that only 4% of OCO's have produced even a temporary political concessions, because they are so irrelevant and easy to block that they don't even work.

    a. But even on these concessions in the LT they've failed as well, they can agree to whatever they want, doesn't mean they follow through on it
2. Don't prove why we can't just use other methods like sanctions. In fact the **LA Times in 2019** writes that past cyber agreements with China have been because of sanctions and not cyber operations.
    a. OCO's aren't some unique form of threat. China can a)patch any hack b)take the hit c)retaliate very easily, OCO's are so irrelevant
3. Our Detsch evidence also responds, countries can just agree to a norm and then use third parties anyways to avoid they can't be held responsible for the OCO.

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

To date, c**yber operations do not appear to produce concessions** by themselves. **Offense,** whether disruption, espionage, or degradation, d**oes not produce lasting results sufficient to change the behavior of a target state.30 Only 11 operations (4 percent) appear to have produced even a temporary political concession, with the majority associated with sustained, multiyear counterespionage operations by U.S. operatives usually targeting China or Russia.**31 Furthermore, each of these operations involved not just cyber actions, but other instruments of national power, such as diplomatic negotiations, economic sanctions, and military threats. Under the Obama administration, these operations were calibrated to limit escalation risks and took place alongside a larger series of diplomatic maneuvers designed to manage great-power relationships. For example, the United States used an interagency response to Chinese hacking that included covert retaliation but also involved pursuing a 2015 agreement to limit cyber-enabled economic warfare.33 In response to Russian actions, the United States pursed a mix of sanctions, diplomatic maneuvers, and cyber actions.

https://www.latimes.com/politics/la-fg-us-china-cyber-20170403-story.html

For years, according to U.S. officials, Chinese-backed hackers repeatedly looted valuable intellectual property and other business secrets from U.S. manufacturers, drugmakers, financial institutions and other companies, often with the assistance or tacit approval of the Chinese government or military.

But a late nig**ht negotiation involving U.S. and Chinese officials in a Washington hotel in September 2015, days before Xi was due in Washington for his fir**st state visit, produced an accord with Beijing — the exact details of which remain secret — not to sponsor cyberattacks on U.S. corporations for commercial gain.

Chinese officials capitulated because they were afraid President Obama would impose economic sanctions against Chinese firms that benefited from the hacking, a

move that would taint Xi's high-profile visit, according to two former U.S. officials who participated in the talks who were not authorized to speak publicly.

ome adversaries and allies might theoretically accept a US forward defense but only if they trusted that the USA would not take advantage of the new equilibrium to engage in tactics such as widespread Internet surveillance or covert cyber actions. Unfortunately, with supremacy and overmatch in cyberspace the stated goals of the Department of Defense, Washington, DC is unlikely to take these measures off the table. Norms work better if they're not seen as mutual, restraining both sides, and if they don't change as a matter of whim or convenience. The USA has been inconsistent here, long insisting that its own espionage for geopolitical purposes was acceptable (and even stabilizing) then crying foul over similar behavior by China, claiming activity like the intrusion into OPM must be deterred. This would be less a mutually restraining "norm" than an asymmetric advantage to be imposed through power by one side on others. For persistent-engagement stability theory to bring equilibrium, adversaries need assurance that if they do adhere to US norms, they would not suffer some new (real or perceived) cyber insult from the USA. Amongst the reasons to believe this will not happen is that adversary operations that are within those norms should get a less aggressive response from the USA. As Max Smeets has written, "it is hard to see what exactly would be deemed as acceptable behavior" by the USA and there will be temptation to aggressively intercept and halt any potential attack on the homeland [68]. In addition, the DoD (and other US agencies, as will be explored in the next section) is bound to flex its new authorities regardless of the commitment of those adversaries to norms. These operations could well be perceived by as hostile actions and proof the USA is itself ignoring restraint.

A2: NK Nuke Program

1. Wired in 2019 writes that NK's nuclear program is wholly disconnected from the internet, finding that their intranet is never connected to the broader internet at the same time, and thus concluding that cyber attacking North Korea's nukes is impossible.
    a. That's why when we tried cyber attacking NK's nuclear program in 2010 it failed, cuz hackers can't reach their systems.
2. Even if they want to attack front-side missile launch systems, the NYT in 2019 writes that these attacks largely failed, as NK is now successfully launching ICBM's with no hampering.
3. A prereq to a cyber attack is having a planted spy in NK, with Wired in 2019 writes that would easily raise the risk of miscalculation, and force NK into a pre-emptive strike. We'd say keeping ships in the region and AMS is better because its clear who is where, and thus less chance of miscalc, whereas NK never knows when they're getting OCOd, and thus why the chance of war is much higher.

4. The report they sight about cyber operations causing NK's failure rate to go down is really bad. In fact what the NYT in 17' writes is that the rate drop is really because of manufacturing errors, and just NK being a bunch of idiots.
    a. In fact it also finds that attacking NK would trigger retal in nuclear form from Russia and China

Wired 19'

But despite the US government's dominating powers in the digital realm, security experts and former intelligence officials believe that battlefield favors North Korea. US hackers can take bites out of the edges of North Korea's infrastructure. **But getting to its core—and anywhere close to disrupting or even delaying its nuclear capabilities—will be extremely difficult, they say, if not impossible. In fact, the US did attempt Stuxnet-style sabotage against North Korea in 2010,** years before the Kim regime had the combined ability to create a nuclear weapon and launch it across the Pacific, according to a 2015 Reuters report. **The attempt failed. America's hackers simply couldn't reach the deeply isolated core computers that controlled North Korea's nuclear weapons program.**

NYT 19'

Much more recently, **The New York Times has reported that the US attempted supply-chain attacks that would corrupt the North Korean missile launches, perhaps by tainting software or hardware components.** In recent years, those missile launches have had failure rates as high as 88 percent, perhaps a sign that those programs worked at least in part. But **over the last several months, North Korea has had repeated successes in launching intercontinental ballistic missiles that could reach the United States. If supply-chain sabotage did work at some point, those tests suggest it may well have been overcome.**

Wired 19'

Planting a human agent in the heart of North Korea's most sensitive military facilities would be about as hard as it sounds, says Columbia's Healey, who also worked as the director for Cyber Infrastructure Protection under the Bush administration. **And he suggests that even if that moonshot sabotage operation were successful, it might not have the intended effect.** If North Korea believes its nuclear missile capacity is being threatened, he warns that the country could respond with a pre-emptive strike. **"This stuff is ripe for miscalculation,"** Healey says.

A2: IP Theft/CH Hacking

1. China always has a key incentive to steal tech insofar as it is key to their development and LT growth. Their uniqueness takes out their own argument, have to prove that at least some IP theft is being deterred but at the point where CH hacking is increasing means OCO's don't deter.
2. Other ways we can deter IP Theft. Breaking Defense in 2018 writes that expanding no fly lists and publishing warnings for IP theft would help solve the problem as well. Its' NU.
    a. In fact the USA Today in 18' confirms that the US's move towards actually criminally charging ppl who IP theft is solving the problem.

A2: Substitutes for Intervention

1. Our uniqueness takes out this argument. The cato evidence at the top of our case says that the new policy changes have destroyed the capability for oco's to act as de-escalatory mechanisms. This is because any attack now is just seen as preemptive act of hyper aggression just leading to more long term conflict in the long term.
2. Alt. reasons as to why the attack would never happen even if we didn't have offensive cyber weapons , political reasons mainly and the fact that no one wants another US intervention into another country.
    a. For example the reasons for Trump not doing the strike were because it was too escalatory, that view of strikes doesn't necessarily change with the absence of OCOs he could definitely do other things like increase sanctions.
    b. He has always campaigned on not getting in more conflicts, and the general consensus is that the US shouldn't get itself into more conflicts.
3. They have to win why is dropping a bomb necessarily leads to conflict it could be just tit for tat. Iran knows the US response is just the US feeling the need to posture in response to their aggression, it is not necessarily an act of war.
4. Weighing: escalation in the cyber domain is worse than with kinetic weapons.
    a. Iran is much more likely to escalate in response to cyber weapons, this is because they know they have asymmetric advantage in the cyber world because they are much less reliant on the internet than the US so if the US initiates cyber conflict they are much more willing to take the conflict further. However Iran knows the US has superior conventional advantage and advantage with alliances in the middle east, Iran is much more likely to sit back and not do anything if we launch a conventional strike.

A/2: Deters Aggression

1. The US not doing conventional strikes and favoring ocos just emboldens iran even more. This is because the Washington Institute in '19 finds that Iran sees this tradeoff as the US becoming less assertive to Iran so they perceive they can be more aggressive without facing major consequences. This is why the New York Times '19 finds that there is growing consensus that lack substantial action taken against Iran in June, the same time we retaliated with an oco, is the reason Iran became emboldened and attacked Saudi Arabia 3 months later.

A2: ISIS

Overarching responses

1. ISIS will reappear as someone else
2. Impact is so small; 8 mil not the impact, 98% loss bc of mil
3. OCOs literally don't contribute much

Recession o/w terrorism two warrants

1. Time 17': When we have a recession politicians are more incentivised to pull troops out of areas like Afghanistan and decrease international cooperation in general, which stops the biggest factor reducing ISIS, outweighing on magnitude.
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

On General

1. OCO's enable drone strikes; DS 18': OCOs enable broader conflict and intervention, root cause of terrorism
2. If we win our links then they don't access this contention; with escalation all resources are focused on cyber war; with weapon hacking all resources focused on developing new weapons since our current ones get stolen; either way, no focus on ISIS

On Infra

3. ISIS is adapting and going to new regions, NYT 19': ISIS in philippines, represents a new stage of terrorist orgs that are extremely nimble and require low resources, just moving around after attacks,
    a. This is why the WP 18' writes that after OCOs ISIS just switched servers or switching to other methods, and as a result left the impact of OCOs extremely short term, ISIS will just adapt, concludes can't take them out

On funding

4. Bitcoin switch; NYT 19': terrorist orgs just switching to cryptocurrencies that can hold money without having to liquidate it and are impossible for enforcement to track
5. ISIS doesn't get their money from online, they're diversified. NYT 18' writes that ISIS gets its money from wheat, sheep milk, watermelon sales, whatever they can find, which is why they conclude that the group is self-financed, not dependent on external donors.

ISIS is only able to stay alive because air strikes can't take out their revenue stream. Callimachi 18: Rukmini Callimachi 18, 4-4-2018, "The ISIS Files: When Terrorists Run City Hall," No Publication, https://www.nytimes.com/interactive/2018/04/04/world/middleeast/isis-documents-mosul-iraq.html *CC*

A little more than a decade later, after seizing huge tracts of Iraq and Syria, the militants tried a different tactic. They built their state on the back of the one that existed before, absorbing the administrative know-how of its hundreds of government cadres. An examination of how the group governed reveals a pattern of collaboration between the militants and the civilians under their yoke. One of the keys to their success was their diversified revenue stream. The group drew its income from so many strands of the economy that airstrikes alone were not enough to cripple it. Ledgers, receipt books and monthly budgets describe how the militants monetized every inch of territory they conquered, taxing every bushel of wheat, every liter of sheep's milk and every watermelon sold at markets they controlled. From agriculture alone, they reaped hundreds of millions of dollars. Contrary to popular perception, the group was self-financed, not dependent on external donors.

<u>On Recruitment</u>

6. Social Media doesn't apply because recruitment is local, for all attacks they recruit in the area of attack, so NYT 19' writes that for philippines its ppl in that country that are recruited
7. Even if SM doesn't exist there are other means to recruit, in 90s terrorism activity was much higher so obviously SM isn't some golden key
8. Any past drop in SM usage not bc of OCOs, WP 18' writes that isis lost key media personnel on the ground which is why SM usage dec, not OCOs.
9. In the past OCO's haven't decreased propaganda; Bashar 19' (strake reads this in case) despite taking out production of propaganda material, they still have so much online there was no impact.

In fact, in Bangladesh, a hot-spot for ISIS recruitment, almost all militants were recruited online – Bashar 19
(Iftekharul Bashar, Associate Research Fellow at the International Centre for Political Violence and Terrorism Research, "Islamic State Ideology Continues to Resonate in Bangladesh", https://www.mei.edu/publications/islamic-state-ideology-continues-resonate-bangladesh, MEI)IEA
Recruitment Pattern Islamic State in Bangladesh has been able to recruit both from existing terrorist groups as well as youth with no prior record of engagement in violence. According to Bangladesh's Cou**nter Terrorism and Transnational Crime Unit, 82 of the operatives were recruited online. Though there has been a significant decline in the production of propaganda materials in the local language, the existing materials available in the cyber domain are substantial and being frequently read, referred to and shared by the group's followers.** A significant strength of the group is its ability to recruit from a cross-section of the society. However, unlike any other Bangladeshi terrorist groups, IS has been able to recruit from the more educated, urban and privileged class of society. One other interesting recruitment pattern is its ability to recruit women and children. The group emphasizes family-based units to ensure secrecy and avoid detection. Women's role in IS cells in Bangladesh are still mostly passive, and often a result of persuasion by their radicalized

husbands. However, there are several cases where women have been self-radicalized and taken a more direct role. Momena Shoma is a case in point. She became radicalized in 2013 and in 2018 stabbed an Australian national in Melbourne for which she was given a 42-year jail sentence.16 Momena Shoma's sister, Asmaul Husna, who was also said to be radicalized, stabbed a Bangladeshi police officer in Dhaka.17
ISIS and Al Qaeda are recruiting jihadist computer experts with the expressed interest of launching hacking attacks on the U.S.

On Leader Decap

1. Will still take out leader, did so a few weeks ago
2. NYT writes that because there is so much popular support and strong infrastructure, taking out a leader isn't going to magically bring down the org.
    a. o/w prob, analyzes 20 years and concludes no success, concluding its counter productive bc its raises AMS

https://www.nytimes.com/2016/08/31/world/middleeast/syria-killing-terrorist-leaders.html

A2: Boko Haram

1. Ev prob indicates that just supporting them is enough, don't need to physically attack, just providing intel and drone coverage is enough to solve
2. Nigeria has already set up their own command and is doing OCOs, US isn't needed
3. The coop we can do is things like providing technology in squo, Spacewatch 18': US companies already helping carry out ops, don't prove u/q for federal government being key
4. We wouldn't use our ops in Nigeria and give them away, higher priorities for US military
5. Further US involvement is only going to fuel Boko Haram recruitment, literally means "western education is bad"
6. Our ops create dependency on us, means that in the future if our OCOs are disrupted in any way then nigeria has no capabilities to stop Haram
7. EU heavily investing in security and strengthening partnership with Nigeria against boko haram, don't prove why the US uniquely needs to help

A2: Strengthening 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.

    a. Voting neg does not mean that all OCOs go away, it's just that there will be a better balance of offense and defense.
    b. 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. Still have to prove intent. If Trump doesn't like NATO then even if we use OCOs generally that doesn't mean he will also use it to strengthen NATO.
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. CyberScoop 19' finds a couple problems with this argument.
    a. Others, specifically 9 other countries can do OCOs for NATO, and that the UK has been the most successful. Don't need the US.
    b. Don't have to respond in cyber means, in fact many may actually be responded to militarily.
        i. That means that we don't need OCO's to strengthen NATO
        ii. But also that this is a bad thing on net because it concedes that interventions would increase, which has been disastrous blah blah
5. Their impact is dependent on someone attacking NATO, but the only way this happens is if we escalate with Russia for example in the first place. We short circuit their impact.

A2: Satisfying Saudi Arabia

1. US is oil independent
    a. SA won't hoe the US bc the US doesn't care
    b. US wouldn't be affected if SA does hoe
2. SA hasn't gotten on anyone's case for criticizing anyone -- they prioritize profit over all else
    a. Ev says profit top incentive
    b. Only source talking abt is anonymous official - only example is 1973 yom kipper war
3. We have troops in SA, security is much more than just an OCO
4. Only ally in region, SA can't lose US
    a. Can't name any allies

A2: NK Stealing money for Nukes

1. Why would NK destroy financial sector if they need it stable to steal money from?

2. CNBC; 4 other sources for Nuclear weapons funding
3. They'll just put more money from their own gdp towards nuke program to make up for it

A2: Stuxnet works to reduce their OCO

1. CNBC in 19' asks every single expert and concludes stuxnet failed

https://www.cnbc.com/2019/09/21/saudi-aramco-attacks-could-predict-cyber-warfare-from-iran.html

A2: Drone strikes become more accurate

1. OCO enable more strikes so still worse even if they are precise
2. Bramlette is bad ev;
    a. The test was done w drones u can buy at kroger, not military drones that are already using gps/satellite tech, don't need OCOs
    b. concedes ¾ tests failed, and actually showed false targets thus increasing civilian deaths
    c. Concedes that the cyber additions can be easily blocked, it lists 4 countermeasures, one of which i learned 10 minutes before the round, ask me after i'll send it to you too
3. The impact is like 5 thousand people, meanwhile escalation pushes 90 million people to death from the grid shutting down and hundreds of millions from financial attacks

A2: Rohan aff

Crowther 17; they say OCO provide deterrence that doesn't exist rn, but it concedes that OCO's actually don't have any deterrence effect, they are misconstruing this evi so hard

A2: Norm Setting

1. Our use of OCO's is the reason why Norms are needed in the first place, for two reasons.
    a. **Goldsmith of NewRepublic** writes that our constant use of OCO's normalized the use of OCO's by other countries in the first place, the warrant being that other countries didn't feel a need to develop a program until the US did.

        i. This is why the Healy ev from case is very good in saying that our switch the offense allows other countries to justify creating their own commands. Historically this is true, Manes 19' finds that the US invasion of Iraq justified other countries to pursue intervention and that our OCO usage would have a similar effect.
    b. Our leaking of weapons by using them and developing them provides the weapons used in the first place. If we didn't create them, then there would be much less weapons and dangerous weapons available for others to create.
2. Avoiding OCO's is the way to set norms going forward. **Bonnie of the AC in 19'** writes that our constant usage of OCO's has pushed the chance to create norms with Iran off and instead has invited more escalation, not peace, which is obviously needed in order to create norms.
    a. History proves. The LA Times in 2017 writes that under Obama's strategy of avoiding OCO's we signed an agreement with China that reduced their hacking of us by 90%. But since Trump's shift towards OCO's IJ 19' finds that hacking from China is now on the rise again.
3. There are unintended consequences of coercion. What Manes in 19' writes is that even though we tried to use a virus to stop Iran's Nuclear program and cyber capabilities it spread around the world to 155 countries, who then change it up and attack other countries.
    a. This gets rid of any coercive powers because now everyone has it.
    b. It makes the incentive to sign on to any norm even worse because they fear attack from random groups that now have weapons.
4. Valerino in 2019 finds a couple problems with this argument.
    a. It's impossible to evaluate the role OCO's have because countries might be listening to us just because we have hella economic and political clout, not necessarily OCOs.
    b. Past norm setting campaigns have failed; we tried two different ops, one on NK and one on China, both failed.
5. **CSMoniter 17' ev** from case also applies here; countries just outsource their OCO's to third parties so no accountability. Even if they create norms, it's short circuited by countries just attacking and denying.
        i. This is why the CS 19' writes that countries like Russia and China have terrible track records when it comes to following norms.
6. The Council for Foreign Relations in 17' writes that even if the United States goes ahead to develop norms they won't gain long term legitimacy without other countries taking the lead, like the Netherlands. They have to prove that before they access their impact.
7. Norms in the neg world are always better than the ones they develop.
    a. This is because the CFR evi from our case finds that norms will only be successful if countries don't see it as a projection of US national interest. This makes sense, if you do what the aff is saying and just coerce countries into following what we want they don't see the norms as ones developed out of a general consensus and

ones that are generally accepted. That's why they conclude that they best way to develop norms is to have the US bring other actors to the table and then develop guidelines that are in line with all countries interests.

b. The norms they develop are extremely short term because they won't do anything to restrain themselves without the US first disarming themselves they simply don't trust them. This is why historically non-proliferation with nuclear weapons didn't work as countries just simply didn't trust that the other countries weren't planning to use or develop those weapons anyways. We have to disarm ourselves before even thinking about getting other countries to follow what we want them too. {also why every norm they can bring up failed, literally every country just stopped that one action for a while and then just resumed}.

https://www.cfr.org/report/promoting-norms-cyberspace

Third, to develop legitimate norms, the United States should let some of its partners take the lead. New norms will not be seen as legitimate if they are perceived to be solely a projection of U.S. interests. The Netherlands, for instance, has been active in promoting free expression on the Internet, and is hosting a Global Conference on Cyberspace in April 2015. A number of private groups and companies—the Global Network Initiative, Electronic Frontier Foundation (EFF), the Center for Democracy and Technology, and Microsoft—are working on norms of state behavior. The United States can exercise influence over norms, helping to convene initial groups, and perhaps imprinting the early process of debate with some of its core values. However, norms will only develop full legitimacy if they are associated with independent structures that evaluate them, debate them, and assess whether different actors are living up to them.

A2: Coercion

1. Coercion doesn't work because in order to force someone to comply you have to show them what they'll face if they don't listen, but WOT 16' writes that once you show your capabilities they patch it.

A2: Setting a threshold / Adaptive Learning

1. Only true if weapons don't get more sophisticated; we may avoid escalation with squo missiles, but when China releases even stronger weapons, then we have to learn those, and pose even new threats to escalation.

2. This argument is too idealistic. They are assuming that countries just see all our cyber operations as just ways to communicate in the cyber realm but our first link tells you that countries would just view US cyber operations as just preemptive strikes on their capabilities, and they would feel the need to attack first and in a bigger way. If anything the problem of communication gets worse because rather than signal resolve our operations signal aggression and escalation.
3. *Even if countries don't know what the US's "threshold is" we would argue that rules of engagement in other areas of conflict would dictate their cyber actions. Countries know if they do something to completely devastate the US economy or do something to threaten american lives it would result in full retaliation. There would be 0 incentive for them to just keep getting more aggressive with their attacks.*
    a. *That's why before Trump's policies there was no big attack or miscalculation.*
4. Even if the US is able to respond to these countries attacks, they would always have incentive to attack and continue to escalate. This is because actors such as Iran and North Korea know
    a. Its very hard to attribute complex attacks back to the source
    b. They have an asymmetric advantage in cyber conflict because the US is the country most reliant on the internet, so they have a strategic advantage of using cyber operations
5. Our second link also links into this argument. As long as third party actors get more weapons and can attack the US would be always be on edge and they would miscalculate and attack a country they think was responsible.
    a. This is better link into escalation as third party actors aren't bound to rules of engagement and geopolitical relations its always more important to stop escalation stemming from these actors rather than from countries like China and Russia who already who many preexisting reasons to not do the attacks they talk about.

A2: Find Vulnerabilities to solve em

1. [we don't patch shit]
2. [o/w, this goes to business]
3. [Don't link into OCO's]
4. [More we do this more we open them up into getting our weapons]
5.

A2: Dark Web OCOs

1. Dallas News 17': FBI setting up sites to catch criminals, don't need OCO's to stop Child porn viewers

2. Newsweek 17': Others taking down dark web, don't' need OCO's to do so

A2: Shut Down Iran radars

1. Its one time use; afterwards they can figure it out
2. If they wanted to close they'd do so without tech; can just blockade
3. Probably fine if they close the strait compared to other options if we're at this point of agression

A2: Evaluate Only Past Actions

Tense neutral -
You know for sure its not associated in past - resolution would have been said
Even if evaluating past - weapons in squo have led to an inc. risk of miscalc already in the future

A2: Persistent Engagement takes out Capabilities

Two key problems with this arg:

1. RCD writes that the US doesn't just run around launching operations, they take their time planning them out extensively. This means we cannot keep persistently engaging every day to take out their capabilities, it's impractical and render our weapons useless bc everyone patches them.
2. It's impossible to truly take out their capabilities. RCD also writes that the BEST CASE scenario is that we disable their computer systems to prevent an attack, leaving the attackers able to learn from what just happened and then launch an attack back, concluding that regeneration is always possible; it makes no sense how we can just take out someone's capabilities forever.

https://www.realcleardefense.com/articles/2018/10/09/a_new_more_aggressive_us_cybersecurity_policy_complements_traditional_methods_113879.html
Borghard and Lonergan also point out that cyber responses are limited in their destructive power. A best-case scenario for a cyberattack would be disabling computer systems and networks being

used against U.S. interests to prevent an attack from happening, or to disrupt an attack that is underway. While this is better than nothing, it still leaves the individuals behind the operation free to learn from their mistakes and mount another attack. While using cyber operations against known threats in conjunction with indictments that name and shame perpetrators — along with specific details on how they carried out their alleged crimes — would certainly make it harder for individuals to reuse the same infrastructure for a future attack, regeneration is always possible, especially with state support.

A2: St. Johns Aff

1. Their uniqueness ev is really bad
    a. We're locked into cyber war w russia and attacks on US banks are increasing, that's why their uniqueness ev is a) not specific to the US and b) doesn't even say OCO are stopping them, they're hella misconstruing
2. Their friedberg ev loses them the first link, they themselves concede don't have to use OCOs, just developing them is enough, its NU
3.

"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. "

A2: Ports

1. Defending forward not working, san diego port being attacked
    a. Incentive structure is where it matters bc we can't stop capability
2. Computing 18': AI can solve back, don't need OCOs

https://www.computing.co.uk/ctg/sponsored/3064194/troubled-waters-cyber-attacks-on-san-diego-and-barcelonas-ports-show-risk-of-it-ot-convergence

NEG

A2: Direct Escalation

1. First an overarching response. Inaction is just as bad. In fact, the Lawfare evidence indicates that in the four years after Obama released his 2011 strategy of not doing OCOs, the scope, severity, and diversity of cyber-attacks on the United States exponentially increased. The warrant being that countries always have an incentive to attack us, and not doing anything just invites them to do it more because we don't impose costs to their actions. The impact of escalation they give you is relatively non-unique, but importantly, our side controls the risk of offense by forcing countries to recalculate.
    a. ALSO can be implicated to say that we should be invading russia's stuff too to create MAD
2. Second, they don't prove why escalation only occurs through cyber operations. In their world, if someone attacks us, then, without OCOs, Trump would just retaliate in another form because the current administration is incredibly hawkish and prefers military responses. We say we're winning the comparative; that is, if he has to respond in either world, it's better for it to NOT be physical military strikes, which is something only we can guarantee. The analogy is clear; starting a physical on the ground war is much worse than a back-and-forth in the cyber domain. We're still accessing offense.
3. Don't prove why the US would escalate, adapative learning
4. Our link about adaptive learning short-circuits their argument in two ways. First, the NYT evidence from case indicates that in the short-term there may be some attacks and unusual responses but in the long term using OCOs will force them to settle out and de-escalate over time. Thus, we outweigh because they're impacting to a very temporary increase in tensions while we are defining international cyber conflict in order to constrain *other* actors, who even in their world would have an incentive to develop OCOs.
5. Our first link short circuits this again; the Lawfare evidence indicates that strong conflict is solved for by using OCOs and signaling the level you want to escalate like a hotline, that way if either side really wants to go to war they can signal it through cyber ops. In the neg world countries just escalate with no end, until we're triggered into full war. The Barnes ev indicates that there was no escalation w recent attack on iran, whereas the the lawfare ev indicates that in the

Our link outweighs on a couple levels:

1. Probability; historically our case has been true
2. Magnitude; we impact out to the entire world, not just specific to the US
3. Incentive Structure; their impact is non-unique, countries always going to want to attack, we change the incentive

Prefer Our First Contention over this for a couple of reasons

1. The escalation resulting from a conventional we strike just occurs much faster, historically it takes at max a couple of months for some kinetic strike to lead to some big conflict. However their cyber escalation arguments take a long time to fully manifest because its a series of conflicts leading up to some big attack. We would argue within that time period it takes to stop some escalatory conflict our impact would have triggered multiple times over.
    a. Also intervening factors weighing
2. Getting involved in conventional conflict also just leads to more spillover into areas so there would be more cyber retaliation on a large scale as well.
    a. This analysis doesn't go the other way because if there is an escalation in the cyber domain the provocations such as grid damage or financial attacks are just generally more reversible so the incentive to cross over to kinetic strikes is very low. Countries would just stay within the cyber domain.
3. A/2 Scope: Conventional conflict in small countries IS bad - and probably can be argued as worse. if we get involved in iran, so does russia - the same giant powers get in on a war but are proxies, which means that they don't have their own thresholds for when to stop escalating and just tear a country apart (see: syria)
4. The impacts of cyber warfare is just much more reversible. Things such as hacks on grids and hacks on business are short term effects that in the long term can be balanced out. However historically military intervention has severe long lasting effects on societies such as societal collapse and just also kill a lot of people.

1. Cato Institution writes in 2018 that rarely has a cyber operation provoked a more severe response, the warrant being that OCO help serve as a non-dangerous way to retaliate to show resolve. Prefer history, escalation never escalates.
2.
3. Our first link about global cooperation short circuits it; if we coerce countries into norms we stop any escalation from happening, not just with the US, but with the entire world.

4. Our second link also short circuits this; the NYT ev from case indicates that in the short term there may be some attacks and unusual responses but in the long term OCO's will settle out and de escalate over time. Pref the forward looking analysis over their past analysis that doesn't account for things in the future.
5. Our second link short circuits this again; the Lawfare ev indicates that strong conflict is solved for by using OCO's and signalling the level you want to escalate like a hotline, that way if either side really wants to go to war they can signal it through cyber ops. In the neg world countries just escalate with no end, until we're triggered into full war.

1. [ev about in short term being some attacks, but in the long term it'll settle out]
2. [much better w OCO's (ev abt it being bloodless) than physical]
3. [the lawfare ev solves back for strong conflict by acting like a hotline; if either side really wants to go to war then they can signal it through cyber ops, whereas in the neg world they just escalate with no end]
4. [Have hotlines to ensure it never goes to full scale]
5. [incentive to escalate is NU, the only risk to deter is OCO's]
    a. find some example from past two years

Link weighing:

1. Kinetic strikes larger magnifier
2. Inaction worse than escalation; if we don't do anything we embolden them to escalate further, for ex. If China thinks that we won't do anything they'll escalate and we'll go to war
3. Overarch: If we didn't have OCO's we are still seeing escalation; China can escalate unilaterally, so Neg's impact are NU to large extent, only difference is how we respond

[WRITE LINK WEIGHING SPECIFIC TO EACH NEG LINK]
https://www.cybintsolutions.com/cyber-security-facts-stats/ - hacking has been increasing for a long time

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

It is thus not surprising that given the limited objectives of most cyber operations, to date rival states have tended to respond proportionally or not at all.

Returning to the data, between 2000 and 2016, only 89 operations (32.72 percent) saw a retaliatory cyber response within one year. Of those, 54 (60.7 percent) were at a low-level response severity (e.g., website defacements, limited denial of service attacks, etc.). Table 1 in the appendix compares the

severity scores for cyber operations between rival states between 2000 and 2016.[37] **When rival states do retaliate, the responses tend to be proportional: that is, they tend to match the severity of the initial attack.[38]**

Low-level responses beget low-level counter responses as states constantly engage in a limited manner consistent with the ebbs and flows of what famed Cold War nuclear theorist Herman Kahn called "subcrisis maneuvering."[39] Rarely does a response include an increase in severity.

Instead, we witness counter responses of a similar or lower level than the original intrusion or a response outside the cyber domain (for example, economic sanctions or legal indictment of specific individuals). The engagement is persistent but managed, and often occurs beneath an escalatory threshold.[40] As seen in Table 2 in the appendix, this behavior appears to apply equally to each possible cyber strategy: disruption, espionage, and degradation. Espionage saw little retaliatory escalation, while disruption and degradation both exhibited more low-level responses.

A2: Military Tradeoff

1. Have incentive to build anyways there are so many complicated relationships so they will have to develop.
2. SAvsIran, conflict means that funding, absent ocos, the money will just go to funding other types of military spending.
    a. Cyber weapons are just generally more cost effective and cheap
3. Silence people brutally so that's not the reason they fund social security
4. Comparative is we have conventional conflict versus some decrease in social spending from cyber ops
    a. They would do things like the strait of hormuz and destroy their infra. capability and things like oil refinery so in the long run they lose the ability to get money for social security.

A2: Reengineering

1. ZDnet: China catching up to the US in terms of OCO capabilities
    a. Countries like China and Russia just have good stem foundations and the ability to innovate fast, we say that absent the use of US oco's those countries would get the same level of weapons anyways.
2. Inaction is still bad, if the impact is they attack the US more if we do nothing it just leads to more aggression and a higher risk one of their impact scenarios triggers the impact.
3. NU; still develop weapons, don't need to use it
4. Norms solve reengineering; Steven 17'
5. Better for them to reengineer weapons than just develop their own capabilities because we can
    a. Patch weapons we create

    b. Takes longer for them to develop than if they are pumping them out on their own
6. NYT/below the threshold of war so the weapon cannot be reengineered
    a. This is offense for us bc then its better to steal from us than other countries whose weapons are much higher than ours in terms of how provocative they are

A2: Normalizing OCOs

1/ lawfare: inaction is just as bad
2/

A2: Angering Iran / Cyber war

Adapat this shit for cyberwar, also read lawfare inaction

On link:
1. Other actors; CSI 19': Israel launching new OCOs against Iran, they have to develop their cyber program in any world. Also should have seen war against Israel.
2. Other things cause retaliation; RF 19' finds that sanctions/CEOs saying bad things about Iran caused a OCO against us, retaliation is coming regardless of whether we have OCOs or not
3. Physical Intervention would have been straight Nuclear War, much worse (win c1 in order to win their case)

On Impact:
1. CSIS writes in 2018 that Iran would never escalate beyond basic level responses. Make them give you one example in the past 14 years since we started cyber-attacking Iran that they have escalated.

https://www.csis.org/analysis/iran-and-cyber-power
How likely is an attack against the United States? A decision for a cyberattack on the United States will depend on Iranian calculations of the risk of a damaging U.S. response.

While the Iranians may appear hotheaded, they are shrewd and calculating in covert action and will consider how to punish the United States without triggering a violent response. If we look at Iranian cyber actions against U.S. targets—the actions against major banks or the more damaging attack on the Sands Casino—**Iranian attacks are likely to be retaliatory, intending to make the point that the United States is not invulnerable but without going too far.** Attacking major targets in the American homeland would be escalatory, something Iran wishes to avoid. It wants to push back on U.S. presence in the region and demonstrate, to both its own citizens and its Gulf neighbors, that the United States can be challenged. I**f Iran does act in the United States, crippling a casino makes a point. Blacking out the power grid or destroying a pipeline risks crossing the line.**

A2: Arms Race w Russia

1. Cyber escalation has never occurred with Russia despite constant attacks between the two. The warrant for why is 3 fold
    a. We stay low level, valaerino writes that attacks are proportional and below the threshold of war
    b. Cfr: The countries aren't dumb, they have constant meetings and hotlines to prevent escalation
    c. We coerce them into norms, squo cyber coop with russia, solving back for root harm

The United States and Russia recognize that despite their significant differences, they have to talk to each other to avoid uncontrolled escalation in cyberspace. That's why even after the 2014 Russian invasion of Ukraine, the United States kept meeting with Russian cyber experts despite having cut cooperation elsewhere. And the Kremlin reportedly used a dedicated hotline on cyber issues to raise concerns about malicious cyber activity emanating from the United States against the 2014 Sochi Olympics.

A2: Taiwan Scenario

1. Can't attribute it to the U.S.
2. Other stuff would trigger this; trade war displeasure, SCS, UN, other triggers for their supposed link.
3. China won't invade – 5 warrants

Maitreya Bhakal, 01-24-12 – analyst on Chinese relations. Article: "Five reasons why China will not invade Taiwan, and an analysis of Cross-strait Relations." Online: "http://blog.hiddenharmonies.org/2012/01/24/china-taiwan-america-us-cross-strait-relations-invade-five-reasons/"

-Economics

-Public Perception

-Threat of American intervention

-China wants peace

-Taiwan won't declare independence

Five reasons why China will not invade Taiwan Journalists and analysts never forget to dutifully remind us that China has not "ruled out" the use of force against Taiwan. What they do not remind us with such regularity however, is that the Chinese leadership has regularly stressed that they seek peaceful reunification of Taiwan with the mainland. China has deployed, they say, 1500 missiles targeting Taiwan (or 2000, if one is feeling so inclined), due to which Taiwan should be regularly supplied with US arms to enable it to defend itself. They find the subtle politics of China's missile deployments beyond the scope of their understanding. What they also fail to address is why China should redeploy or dismantle a major part of its defense arsenal (and one that faces the South China Sea and defends China's most populated areas) just to placate Taiwan and US hawks. Moreover, even if the missiles were withdrawn, they could be redeployed at any time. These missiles are seen as an important deterrent to Taiwan's independence and potential US intervention. Whatever the media wants its readers to believe, the only major reason why China would actually consider an invasion is if Taiwan declares independence. This is in no danger of happening in the near future. Especially given Ma's recent victory and his pledge of the "Three Nos" – "No independence, No unification, No use of force". It is reasonable to assume that the majority of the Taiwanese public agree with him, and are happy with the status quo (the latter has been demonstrated by numerous opinion polls as well). Here are five major reasons why a full-fledged Chinese invasion of the island is more suited for a video game rather than reality. 5. Economics: China has always placed economics at the forefront of most other matters. Despite the often-tumultuous state of Sino-Indian relations (and an unresolved border dispute), trade has touched $63 billion. China is India's second largest trading partner. In the Senkaku island dispute with Japan, Deng Xiaoping, as soon as he came into power in 1978, proposed that China and Japan jointly explore the oil and gas deposits near the disputed islands without touching on the issue of sovereignty. China has also sought joint exploration in the resource-rich Spratlys, a solution which is the right step forward and is in fact more urgent than sovereignty, which the Philippines and Vietnam and have so far been reluctant to do. China doesn't mind waiting and biding its time until sovereignty issues get resolved. As Deng Xiaoping famously remarked regarding the Senkaku dispute, "It does not matter if this question is shelved for some time, say, 10 years. Our generation is not wise enough to find common language on this question. Our next generation will certainly be wiser. They will certainly find a solution acceptable to all". Unlike his predecessor Jiang Zemin, Hu Jintao has used a softer approach towards Taiwan, promoting stronger economic and cultural ties, high-level official visits and direct flights in order to reduce tensions. This pragmatic approach is on display even in the Taiwan dispute. China is Taiwan's largest trading partner, and Taiwan is China's seventh largest. Two-thirds of all Taiwanese companies have made investments in China in recent years. In 2010, China (including Hong Kong) accounted for over 29.0% of Taiwan's total trade and 41.8% of Taiwan's exports. The ECFA was heavily tilted in Taiwan's favor. It cut tariffs on 539 Taiwanese exports to China and 267 Chinese products entering Taiwan. Under the agreement, approximately 16.1 % of exports to China and 10.5 % of imports to China will be tariff free by 2013. Taiwanese firms have invested $200 billion in the mainland, and trade between the two sides has exceeded $150 billion. Taiwanese trade with China. Source: Reuters Both China and Taiwan have a lot to lose by fighting with each other. Another factor to consider is the incalculable loss that an invasion will have on the Chinese economy, not to mention scaring away potential investors. 4. The Taiwanese public: China is, quite rightly, obsessed with "stability", President Hu's watchword. Analysts agree that this is one of the main reasons why it is not being "tough" on North Korea – that it wants a stable neighbor with no refugee spillover. With hundreds of protests happening in China every year, it most certainly wouldn't want yet another headache on its hands and alienate the island's inhabitants (even more than they are at the moment). There is very less support for reunification on the island, and opinion polls make clear that only a tiny minority of Taiwanese identify themselves as "Chinese". The Anti-Secession also explicitly states in Article 9: In the event of employing and executing non-peaceful means and other necessary measures as provided for in this Law, the state shall exert its utmost to protect the lives, property and other legitimate rights and interests of Taiwan civilians and foreign nationals in Taiwan, and to minimize losses. At the same time, the state shall protect the rights and interests of the Taiwan compatriots in other parts of China in accordance with law. A Chinese invasion might inevitably lead to riots and international condemnation. China would thus risk flushing down the toilet many years' hard work of patient diplomacy (in convincing other countries of its "peaceful rise"). This would in turn cause them to inch even closer to America, were they would be welcomed with open arms. 3. The threat of American intervention: The United States of America, the responsible superpower, has been engaged in more military conflicts around this world than any other. Since the Second World War, the US has: Attempted to overthrow more than 50 governments, most of them democratically-elected. Attempted to suppress a populist or national movement in 20 countries. Grossly interfered in democratic elections in at least 30 countries. Dropped bombs on the people of more than 30 countries. Attempted to assassinate more than 50 foreign leaders. Hence, the plain fact that needs to be realized is that the United States is more prone to violent outbursts than any other country. The PLA doctrinal textbook, Zhanyixue, explicitly states that China is not in the same league as "advanced countries" (The entire document never mentions the United States by name), argues Thomas J. Christensen in China's Revolution in Doctrinal Affairs: Recent Trends in the Operational Art of the Chinese People's Liberation Army (CNA, 2005). He further states, Moreover, unlike in the heady early days of the Great Leap Forward, PLA strategists do not envision China closing that overall gap anytime soon. There is no stated expectation of short-cuts or leapfrogging to great power military status. In other words, China will have to accept that its relative technological backwardness and weakness in power projection will persist for a long time. And then goes on to quote the text of Zhanyixue explicitly: "Our military equipment has gone through

major upgrading (很大提高) in comparison with the past, but in comparison to advanced countries, whether it be now or even a relatively long period from now, there will still be a relatively large gap (仍有较 大的差距).....The most prominent objective reality that the PLA will face in fighting future campaigns is that in [the area of] military equipment, the enemy will be superior and we will be inferior." As is clear, Chinese policy-makers are realists, and thus can be relied upon to heavily weigh the consequences of a possible US intervention. 2. China wants peace: China is one of the few rising powers in the whole of human history to announce peaceful intentions and no desire to rule or establish hegemony over the world. In what might come as a shock to most people who consider media reports as a textbook for Chinese foreign policy, China has, on the whole, been a peaceful nation and has not engaged in military action unless provoked. And the military action that it has been involved in in its modern history has been extremely limited in its duration and objectives. Barring a misadventure with Vietnam in 1979 (which was also quite limited), China has only used war as a last resort, when it was left with no other alternative. Resolutions of boundary disputes can be generally considered as a fundamental indication whether a country is pursuing expansionist or peaceful policies (which is one reason why a thorough analysis of China's border disputes has been neglected by almost all western media outlets and analysts). China has had the highest number of border disputes of any country in the world and with no intention of living in an unfriendly atmosphere over a peace of land, has successfully handled and offered substantial compromises (this is the other reason) in most of them. China borders 14 countries by land; and as a result of territorial dismemberment and unequal treaties, the PRC government, when it came into power, found itself involved in territorial disputes with all of them. The way in which China resolved those disputes stands as testimony to its desire of peace at any cost and serves as an example to other countries. China has, in the interests of peace and stability on its borders, adopted a negotiation tactic favorable to rival claimants that other countries would do well to emulate. Many of these claimants were countries much weaker than China. China was under no obligation to offer such substantial compromises. The portion of land that China received in border settlements with various neighbouring countries is as follows. Afghanistan – 0% Tajikistan – 4% Nepal – 6% Burma – 18% Kazakhstan – 22% Mongolia – 29% Kyrgyzstan – 32% North Korea – 40% Laos – 50% Vietnam – 50% Russia – 50% Pakistan – 54% Some of this land was strategically important (such as the Wakhan corridor that was disputed with Afghanistan) and extremely rich in resources (such as the Pamir mountain range in case of Tajikistan). China has also not reiterated its claims on a majority of the territory which was seized from it by the unequal treaties (even if it meant being cut off from the strategic Sea of Japan). In the map below, the gray area was part of China when the Qing dynasty was at its height, and then was snatched away from it due to unequal treaties. China has pursued claims on no more than 7% of these territories. China has generally been known to attack when it has been taken advantage of or construed as weak, or when the enemy was at its very doorstep, such as during the Korean war. The Sino-Indian war of 1962 stands as a textbook example of this strategy. Nehru, the then Indian PM, rejecting all Chinese offers for negotiations, constituted a "Forward Policy" of pushing forward to enemy lines and made belligerent statements about China ("I have ordered the army to throw the Chinese out"), implicitly announcing Indian intentions to attack. Some of the Indian outposts established under this policy went even further then Chinese ones. China, correctly interpreting these actions as hostile and viewing India through the prism of British imperialist intentions on Tibet (as India had made itself the British successor in all matters regarding Tibet and China), made multiple diplomatic protests against the Forward Policy, but Nehru ignored them and never thought that China would have the guts to attack. After China finally did attack and occupied the disputed areas, it declared a unilateral ceasefire and withdraw to pre-war status quo borders without occupying an inch of territory. Hence, Chinese intentions were just to just India a lesson. It had no interest in occupying any territory. Hence, a peaceful South China Sea and Taiwan strait is in China's interest. As China rises, the last thing it wants to do is anything that might be construed as provocative. It has indicated that it wants a peace treaty with Taiwan, and indeed, negotiating a peace agreement was one of the points that President Hu introduced as a blueprint for cross-strait relations in December 2008. Ma made a campaign promise to sign a peace treaty in the run up to the 2008 elections, but reneged on it after becoming president. Such a treaty will not only assure China's maritime neighbors (including rival claimants in the South China Sea) of China's peaceful intentions, but will have the effect of also formally ending the Chinese Civil War. 1. Taiwan is not going to declare independence: The most important reason why China has not yet considered an invasion. Ma has explicitly declared that he is not seeking independence, and the voters seem to be siding with him and are happy with the status quo. And so is China. Chinese leaders have a penchant for putting issues on the backburner. They adapt to changing situations and are happy to do what they can (business) and leave for future generations what they cannot (reunification). So what next? Chinese leaders will be happy to admit – they don't know. As long as both sides are happy with the status quo, there seems to be no reason to fret. As long as Taiwan does not declare independence, there seems to be no reason to worry about a military conflict. And since a majority of the Taiwanese people are happy to be were they are, rocking the boat is the last thing leaders on both sides of the strait would want to do. Both economies are growing, and people are living happily on both sides. Every generation of leaders thus hands over this problem to the next one, with the hope that they might one day either solve it, or preserve the status quo and hand the headache over to their successors. Hence, discussion of a Chinese invasion serves little purpose other than to be used by various "foreign-policy analysts" to justify their grants and pass their time. There ought to be no doubt that a full-blown invasion would be a nightmare for China, and it simply wouldn't do it. Or, as Jim Hacker would say, "Not just that it shouldn't, but it couldn't, and if it could, it wouldn't, would it?"

4.

https://www.scmp.com/week-asia/geopolitics/article/2156237/what-would-us-do-if-beijing-decided-take-taiwan-force - US would intervene

A2: Defensive Tradeoff

https://www.ibtimes.com/meet-cyber-industrial-complex-private-contractors-may-get-7b-windfall-pentagons-2329652

1. IB Times 19' finds two things:
    a. We always increase funding for both, so no reason why we can't just increase funding for defense.
    b. Most of the "offense" spending goes to defense anyways, so no real tradeoff, pref on historical precedent
2. Foreign Policy analyzes when we doubled the defense budget and personnel and found that our cyber security still was complete trash.
3. [know what we're going to be hit with, so know how to respond]
4. [take out enemies before they attack us]
5. [deterrence - general]

1. Second, focusing on offense prerequisites defense, as the Cato Institute writes in 2019 that the best defense is a good offense because we can stop the operation from targeting the US in the first place.

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

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

https://outline.com/2FGrwr

Unfortunately, despite the attention, rhetoric, and money the United States government spends on cybersecurity, it is still far from resilient against cyberattack. For every gain, there is still a major gap to be closed. In the military, the construction budget alone for Fort Meade, the combined headquarters of the NSA and Cyber Command, will reach almost $2 billion by the end of 2016, and the force will add another 4,000 personnel, yet the Pentagon's own tester found "significant vulnerabilities" in nearly every major weapons program. In the broader federal government, the cybersecurity budget for fiscal year 2016 is 35 percent higher than it was just two years ago, yet half of security professionals in these agencies think cybersecurity has not improved in that period. The reasons range from continued failure to follow basic measures — as of June 2015, only about 70 percent of federal employees, for example, have implemented a requirement for

personal identification verification cards that dates back to 2004 — to failing to take seriously the long-term nature of the conflict. The exemplar of these failures was the OPM, which dealt with some of the most sensitive government information, and yet outsourced IT work to contractors in China — despite warnings going back to 2009.

A2: OCOs Not Effective (general)

1. Air University finds that even if an OCO isn't perfectly effective is still deters aggression. For example, the OCO we launched on iran had plenty of errors and poor execution, but still deterred Iran forcing them to back down.

Cyber ops still have strategic value if not actually successful
https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Smeets.pdf

Similarly, an offensive cyber operation should not be considered by itself but with reference to both its direct and indirect effect upon conflict. This reveals an intricate relationship between mission excellence and strategic success. A well-written piece of code might provide great tactical value but does not guarantee strategic value, while failed usage of a cyber capability might provide strategic gains. An example of this seemingly counterintuitive logic might be Shamoon, the wiper malware that targeted the world's largest oil company, Saudi Aramco, in August of 2012.18 **The malware contained multiple coding errors and was badly executed.19 Yet, with reference to Iran's broader conflict situation and posture in the region, it might have had a positive contribution. Not least, Iran showed it was unwilling to immediately back down following others' usage of a capability it had hardly developed at the time. The deployment showed Iran's military perseverance and perhaps even enhanced its political standing relative to other states.**

A2: Weapons get stolen

1. ZDnet: China catching up to the US in terms of OCO capabilities
    a. Don't need to steal; have their own capabilities
    b. Other countries don't need to steal from US, they can steal from China too
2. We can OCO Cyber infra before they attack us, weapons irrelevant
3. Have to specify what weapons get stolen, most are just access to network, they don't actually do any damage
4. Since our weapons are below the threshold of war its better for countries to be stealing from us than russia/china who are much more aggressive with their weapons

5. Eternal Blue wasn't even that devastating because it was super specific to its target, instead the Fortune ev in 19' finds that it would have had the same effect w or w out eternal blue
6. *SWE 19': Baltimore attack wasn't eternalblue, it was a general cyber attack. This takes out their impact because they don't prove intent increase w OCO's, if intent is NU, then generic weapons available everywhere will continue to attack us*

A2: OCO's disrupt norm breaking

[they just don't want to join norms]
[We're stopping full conflict - intervention tradeoff]
[Can't lead without a credible threat - NPT created by states with Nukes not those that don't]

These countries aren't innocent - they're attacking other countries too; CSIS writes that africa is attacking developing nations by influencing their elections, they have their own incentive to keep having OCOs

Any agreement won't form / won't work, cfr finds 3 reasons

1. Cyber weapons develop so quickly that the agreement becomes outdated and then everyone develops out of fear that they are being outmatched
2. To enforce an agreement countries would have to allow access to their networks which no one is willing to do - its handing over the keys to the arsenal
3. Don't know who launched the attack so it's impossible to know who to retaliate against, countries would just bypass any agreement bc they know they can't be caught

Best way to create norms is to set them, hatway 12; its so vague in cyber space that norms and retarded, but the US using OCO's is the best way to clarify how norms should be

We can develop norms outside of the US and while doing OCOs

(MARIST CITES THIS EV IN CASE LMAOO) Cyber Summit 18': Estonia got assistance from NATO to develop stronger protection standards, so obviously countries don't care we do OCOs and we can help developing nations at the same time too

MARIST HELLA MISCONTRUING ATLANTIC COUNCIL: ev is talking about security protocols companies need to adopt, not global norms, they can do this in SQUO

On the other hand, despite all circumstantial evidence Estonia did not officially accuse Russia (rather it shared its suspicion with the U.S.) [21] and chose to seek assistance from NATO in developing stronger cybersecurity protection measures

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.

Arms control regimes may also form if governments are able to make reasonable calculations regarding the likely military effect of technological changes. However, the rapid and unpredictable pace of technological innovation in the cyber domain complicates these assessments. At the tactical level, attack vectors and offensive capabilities are continuously evolving, in contrast to the nuclear arena where innovations had long development timelines and could often be observed. The lag time in nuclear innovation gave states breathing room to adjust arms control agreements or develop other means, such as tailored intelligence or their own complimentary programs, to mitigate the fears posed by technological advances. In cyberspace, the open-ended promise of innovation coupled with quickly changing tradecraft that can emerge with little to no warning challenges the creation of any agreement. A cyber arms control agreement runs the risk of being outdated or restrictive in some unanticipated way before the ink has even had time to dry.

Even if states are able to calculate relative capabilities and assess the military implications of a technological innovations, cyber arms control agreements are unlikely to form if governments cannot detect cheating. The verification problem contains two prongs: being able to ascertain the size of a state's arsenal and monitoring it to ensure future compliance. Ascertaining compliance in the cyber domain would require participants to agree to intrusive access to government networks. Malicious software can be developed just about anywhere, meaning that any verification mechanism would require a government to open up all of its networks to inspection. It would be unfathomable for one state to allow another, or any outside actor, to have unfettered access to its networks. Such access would provide an external party

with critical information about vulnerabilities and potential exploits, and potentially violate the agreement it is attempting to enforce.

Finally, even if the preceding obstacles could be overcome, enforcement of any arms control agreement would be difficult to implement due to two factors: problems associated with attribution and divining a proportionate punishment. First, in the event of a violation, states would have to attribute it with a level of confidence that would justify a reciprocal response. While attribution capabilities have unquestionably improved over time, not all states have the same attribution capabilities or enough confidence in them to justify action. This is particularly relevant given that a state that detects a violation would need to convince other parties to the same treaty that a violation occurred.

A2: Provoking NK cyber weapons

1. The NI ev indicates that it's a move towards regime survival which is whyt they're developing their weapons, that's the cause, not OCOs, they need this money for their nukes
2. OCO's give us better intel which allows us to do a preemptive strike on NK, to destroy their nuke program
3. They'd never nuke SK for fear of their regiem being over

A2: Trump hella more aggressive

https://www.fifthdomain.com/dod/cybercom/2018/11/26/why-cyberspace-demands-an-always-on-approach/

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."

A2: PMC

1. Our impact is the long term use of OCO, where we signal as much as we want to escalate. Their examples from the real world of conventional war isn't the same; we don't outsource our FONOPs or drone strikes.
2. The fifth domain '19 writes that because of recent policy changes Cyber Command, the part of the US military that handles our cyber operations, have been given a higher amount of autonomy in terms of strikes. They find that rather than just provoke adversaries around the world randomly, the organization still has many regulations that cause it to many only calculated attacks.
    a. If the generals within cybercommand are the ones controlling the operations they a)can't get influenced by political power of the PMCs b)their underlying incentive is to do things effectively so pmcs would just be fired if they tried to prolong conflict.
3. The influence of PMCs might exist in some way with conventional conflicts because everyone can see the conflict occurring and the PMCs can provide justification to the politicians they lobby by using fear mongering. However, since cyber conflict is just by definition done in secret almost always there is no way for the public to know about cyber conflict and thus politicians can't justify getting more aggressive even if they get more lobbied.
4. 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

5. The resolution asks for the USFG's use of them; we'd argue outsourcing isn't topical especially as the USFG can carry out ops on their own.
6. Competition exists that doesn't exist for conventional
7. Also we'd argue that there isn't just random companies carrying out attacks; command center controls where attacks are and severity; no examples.

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."

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.

A2: Russia Leaves Internet

1. Russia would have done this anyways, localizing data to surveille, no connection
2. Russia thinks data is key so they don't want others to do it
3. Corruption will decrease cuz ppl can't be keeping money offshores and stuff
4. Ppl prob switching to domestic servers bc cheaper prices/other incentives

A2: Dumb Iran arg

Iran OCOs SA oil → oil shocks

Stuxnet forced iran to inc. bomb production → wouldn't have done so w out stuxnet → Israel goes to war if Iran gets nuke → war goes nuclear

Other factors caused review of production protocols
Would have developed the nuke either way - need to stay alive from israel
Stuxnet worked to an extent
Can keep OCOing Iran so they can't use the nuke
Comparative is better - Israel would have invaded physically guaranteeing regional conflict
Nuke for Iran creates MAD
Why hasn't Israel invaded - greater incentive to invade now b4 the nuke is complete

1. Our first contention short circuits this entire argument. Fisher in '15 writes that one of Iran's biggest incentives to develop the Nuke is because they're scared of American Intervention, which is probably why they continued to develop the nuclear bomb even during Obama's period of cyber inactivity. If we switch to OCOs and show that we aren't planning on invading any time soon, then their wanting for the nuke will go down.

2. Their Mahony analysis is flawed. Their Mahony evidence is specific to safety standards and vulnerabilities not efficiency standards. It makes no sense why it took an attack to cause efficiency issues to be found. That's why their ev just says production went up in the same time period, and not that it was caused by Stuxnet. The reason for why production went up comes from Max in '15 who writes that there was a presidential campaign in 2010 in iran and the incumbent promised to expand the nuclear program hella, and thus why the nuclear program expanded.
3. But even on the broader trend, Iran was going to develop the bomb either way. Vox in '15 writes that Iran faces existential threats from neighboring Saudi Arabia and of course Israel which is why we would argue without Stuxnet Iran would have developed them either way.
    a. This is offense for us because the Rogin evidence from cause indicates that doing nothing, or not cyber attack at all, would have emboldened Iran to start being even more aggressive in the region, because they perceive they have a blank check. The warrant checks out too - it's better to respond to Iran and let them know they're doing the wrong thing rather than staying silent. At Least the Cyber attack probably delayed Stuxnet for a few months, giving diplomacy a chance.
4. On the impact level, it isn't true that Israel would invade Iran or try to start conflict, in two examples.
    a. First, if their argument was true, that Stuxnet did fail, then after Iran started recovering to pre-Stuxnet levels Israel should have already invaded because the threat is even higher.
    b. Second, Israel should be invading right now because it makes sense for Israel to invade BEFORE Iran finishes the Nuclear bomb so that they don't get retaliated again.
        i. This is offense for us. Accelerating Iran's nuclear program is a good thing because as it gets stronger Israel can't risk war, the warrant is because the process to take out nuclear capabilities is not a month long process, its multi-year, which is why Iran getting to their nuke quicker is good bc Israel not can't intervene bc Iran could get to their nuke during the war.
        ii. The warrant for both of these arguments is that Israel does not want regional instability as it pulls in other actors leading to Israel being screwed, which is why top level Israel military officials think that them striking Iran is, quote, "the stupidest idea they've ever heard."
5. Their internal link violates the Bengin Doctrine, bc in a world where we patch holes so we don't know Iran's nuclear capabilities, Israel won't get the intel needed as the NI writes that you need strong intel to launch doctrine.
6. Finally, if Iran gets the nuclear bomb, this is a GOOD thing. In fact Ridler of the CSMoniter in '16 writes that if they get the bomb it'll create a form of Mutually Assured Destruction that creates another form of peace-stabilizing in the region.

a/t iran would just get more agressive w nuke
https://www.belfercenter.org/publication/okay-so-what-if-iran-does-get-nuclear-weapons

A2: Lewis arg

1. Their Lewis ev contradicts their trump shift arg; it was during obama when he didn't do anything, that means their arg is NU, they can't solve, countries will always find something to blame for the agreements falling out.
2. Their obama implication of valerino on the first link is wrong; shcneider inaction 2011 exponential inc. in attacks
3. Their lewis ev is heavily powertagged; it doesn't say OCOs have caused massive distrust to increase, it just says that distrust in general means that non-binding norms work better.
    a. Manes ev o/w on probability, their china agreement was bc of us enforcing them, they say its not working but the overall trend is still good
4. Valeriano just says that we could cause escalation, but insofar as lawfare indicates that inaction causes escalation as well, adaptive learning

A2: Left of Launch

1. Russia and China have an incentive to develop left-of-launch anyway, so we're *re-establishing* MAD, not removing it. If the US didn't develop left-of-launch, then their impacts will just trigger with China as the actor instead of the United States.
2. This argument also applies to North Korea because China can act as North Korea's proxy and threaten to retaliate and disable US's systems.
3. We would only be interested in disabling North Korea's nuclear weapons if we had some intention of going to war with them and removing their nukes, but that would require removing the leadership and locating and seizing all of their nuclear weapons, NOT just 'disabling' them.

All of those steps are near-impossible to execute, which is why, even if we have these left-of-launch capabilities, we would never actually use them and go to war with North Korea.
4. This argument is also not what the resolution is asking us to debate. The resolution asks us to evaluate our existing **use** of offensive cyber operations. Even if we didn't USE offensive operations, we would still **develop** something as critical as left-of-launch capabilities. This is empirically true as well because we started exploring left-of-launch in 2013, far before we started *using* offensive operations.
(https://www.nytimes.com/2017/03/04/world/asia/left-of-launch-missile-defense.html)
5. We also outweigh on timeframe. The only way that we escalate wars to the point of even considering disabling someone's nuclear weapons is if we started a war that could escalate to begin with. We prevent conventional engagement. The comparative is this: there are MORE conventional wars on their side, and EVEN IF all of their arguments are true that our side uniquely creates left-of-launch capabilities, a) there are no conventional wars on our side when we prevent kinetic strikes by using OCOs and b) their conventional wars still carry tremendous escalation risk and have massive consequences.

A2: SMH intel link

1. Should have already done it, can't just move shit offline
    a. Good thing then, less efficient / worse at doing stuff
2. Use satellite data??