# Iran 1AC

## C1: Iran De-Escalation

#### The U.S has a direct need to show Iran that recent attacks will not go ignored and offensive cyber operations, or OCOs, are able to accomplish that goal without igniting any further military conflict

**Handler 19 (got tier)**

Simon Handler, 10-28-2019, "The zero-day war? How cyber is reshaping the future of the most combustible conflicts," Atlantic Council, <https://www.atlanticcouncil.org/blogs/new-atlanticist/the-zero-day-war-how-cyber-is-reshaping-the-future-of-the-most-combustible-conflicts/>

As tensions rage beneath [in] the Middle East cauldron, the expanded employment of cyber operations is preventing the region from boiling over. An October 17 Reuters report detailing the United States’ covert cyber operation against Iran, in response to the September 14 attacks on oil facilities in Saudi Arabia, underscores the inclination of states to utilize cyber operations and points to broader strategic implications in the region. Israeli-Saudi security cooperation quietly incubated over mutual intolerance toward an expansionist Iran is blossoming into a gradually open relationship, with cyber at its heart. Bonds such as these, forged behind closed doors, provide options for de-escalatory approaches to regional conflict. Conventional wisdom would suggest that scaled-up capabilities, growing competition, and the proliferation of malware across cyberspace presents a legitimate risk of escalation in state conflict, transcending the cyber domain toward the kinetic. However, **recent history has shown that states** havemore **often availed** themselves of **their offensive cyber** **arsenals** **to achieve** surprisingly **de-escalatory effects**. Offensive cyber operations **[as OCO’s] sit low on the escalation ladder**— the figurative scale ranging from diplomatic engagement to all-out nuclear war—**and provide states with means of signaling adversaries without using force**, **and** potentially even **deescalating** tense or **provocative situations**. Through this lens, there is a case to be made for the responsible diffusion of malware as a tool of diplomacy and statecraft to de-escalate regional conflict. **Cyber operations have served this exact** de-escalatory **purpose** **throughout** **recent tensions in the Persian Gulf**. **When** the Lincoln Carrier Strike Group was deployed to the Persian Gulf in May 2019, after intelligence detected an Iranian threat to US assets in the area, **Washington signaled** **that it was prepared to meet** potential **Iranian aggression with airstrikes**. US President Donald J. **Trump** **went** **as far as to tweet** **that** **the United States was “cocked & loaded,”** alluding to a kinetic response option**, but instead, the US deployed malware to neutralize the Iranian threat,** **while demonstrating that** Tehran’s **provocations** **would not go unchecked**. The United States does not have an appetite for a large-scale deployment of ground forces, which could foreseeably succeed a major escalation, so its decision **to prioritize cyber response options** **underscores** Washington’s **desire to cool things down** **and reassert** its **control by utilizing short-of-war tactics**. A similar strategy is playing out some 1,400 miles away, on the eastern shores of the Mediterranean Sea. While remaining largely out of the fray, Israel is closely monitoring tensions in the Persian Gulf. Israel, like the United States, remains chiefly concerned with breaking Tehran’s spreading influence and power in the region, but does not want to bear the risk of doing so alone. Iran has supplied and employed several proxy militias to exert pressure on Israel and draw Jerusalem’s focus to several fronts at once. This strategy has forced Israel into a heightened operational tempo in which it is now conducting interdiction operations against illicit Iranian-backed materiel transports in Syria, Iraq, Lebanon, Gaza, and the West Bank. This dilemma has led Israel to utilize unconventional tactics and seek assistance from unlikely sources.

#### OCO’s provide crucial intel and response options to provocations that ultimately achieve de-escalation

**Valeriano 19**

Brandon Valeriano & Benjamin Jensen, 6-25-2019, "How Cyber Operations Can Help Manage Crisis: Escalation with Iran," Washington Post, <https://www.washingtonpost.com/politics/2019/06/25/how-cyber-operations-can-help-manage-crisis-escalation-with-iran/>

Instead, the United States chose to disrupt Iranian military targets with two distinct covert cyber operations. The United States appears to have sought to disable Iranian missile sites and eliminate the Iranian military’s command and control capabilities. The case illustrates the new character of strategy in a connected era. In times of crisis, countries increasingly opt for non-military coercive instruments of power, including cyberattacks and economic sanctions, to control escalation risk. As we note in a recent Cato Institute foreign policy analysis article, “**rather than escalate with** conventional **military options, cyber operations offer rivals a way to respond to provocations without** significantly **increasing tension** **in** a **crisis**.” Cyber operations are more political warfare than decisive battle instruments. **They provide** decision-makers **valuable** **intell**igence **and** potentially **coercive options** **that** **help avoid direct military** **confrontation** **and** can **reduce the severity** **of** the **response**. The current crisis began with Iran seeking covert responses to the challenge of economic sanctions. U.S.-based cyber security firms noted an increase in Iranian hacking and spear-phishing attempts — when emails seek access to computer systems by pretending to originate from a trusted source. And there were also several conventional attacks attributed to Iran on shipping in the region. In response, the United States deployed additional military assets to the Persian Gulf. After accusing Iran of shooting down the Global Hawk surveillance drone on Thursday, the United States faced the choice of limited military strikes to signal resolve — or choosing options representing less of an escalation. Events in the gulf reflect a larger pattern of cyber exchanges between rival nations, and echo the results of a series of survey experiments by our team and others**. Data on cyber conflict** between rival states **between 2000 and 2016** **suggests** that Iran and the United States have engaged in 20 cyber conflicts during this time period. Iran has launched 13 operations, while the United States launched seven operations. A decade ago, the Stuxnet operation successfully penetrated Iran’s nuclear production facilities and digitally destroyed some equipment used in the enrichment of uranium. Since then, the United States tends to use cyber options to respond to Iranian aggression. And Iran often relies on cyber espionage directed against nongovernmental targets — or hits American allies in the region, in attacks such as the computer virus attributed to Iranian hackers that targeted Saudi Arabia’s oil production facilities. Trump’s decision to respond to Iranian aggression with cyber operations aligns with recent findings from our ongoing war games and survey experiments. Based on 277 war game experiments involving a mix of national security practitioners, the business sector and college students at international relations-related programs, we find **that parties are reluctant to escalate with cyber options in a crisis, preferring to use them** — as we saw happen with Iran — **in a more proportionate or equivalent response**. Teams use cyber operations to **in a way that** signals risk and **preserves** future **options [to] manage a crisis.** The general public also tends to favor proportional responses involving cyber retaliation. **Cyber** responses **offer[s]** great powers **response options that stop short of military force**, preserve flexibility **and limit risk**. In our ongoing research, we see a similar logic at play in survey experiments funded by the Carnegie Corporation of New York. We surveyed a representative sample of Americans, Russians and Israelis to run an experiment on the use of cyber operations in a scenario similar to the current standoff between Washington and Tehran. We randomly assigned 1,500 of the respondents the option of responding to an unfolding crisis with cyber options and offered the other 1,500 more traditional diplomatic, economic and military response options. **The findings were clear**: **Cyber options can help de-escalate deadly militarized disputes**. The majority of the survey responses (764 total) in the cyber options group favored a de-escalatory approach, compared to proportional (620) and escalatory (156) alternatives. These levels were similar to the non-cyber treatment. What’s interesting in relation to the Iranian crisis is that when participants chose to escalate, 69 percent preferred cyber options, while 26 percent opted for a proportional cyber response. Survey respondents across these three countries used cyber options in a manner that preserved their flexibility and set conditions for follow-on operations. For leaders, managing an escalating international crisis with a rival nation is one of the most challenging situations. Contrary to conventional wisdom, cyber options preserve flexibility and give leaders an off-ramp to war. National security decision-makers are increasingly turning to cyber responses to manage great power competition. When there is a crisis, some analysts argue that cyber options function best not as deterrence, but to manage an out-of-control situation — and avoid outright war. The question remains how the opposition is likely to perceive these moves. Will they recognize them as methods to tamp down the drums of war or see them as aggressive moves that require escalatory responses?

**Everything about cyber-attacks makes them de-escalatory**

#### U.S cyber operations are made to not prompt retaliation and remain in the gray-zone between war and peace

**Barnes 19**

Julian Barnes, 8-28-2019, "U.S. Cyberattack Hurt Iran’s Ability to Target Oil Tankers, Officials Say," New York Times, https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html

Senior officials discussed the results of the strike in part to quell doubts within the Trump administration about whether the benefits of the operation outweighed the cost — lost intelligence and lost access to a critical network used by the Islamic Revolutionary Guards Corps, Iran’s paramilitary forces. **The United States and Iran have long been involved in** an undeclared **cyberconflict**, one **carefully calibrated to remain in the gray zone between war and peace**. The June 20 strike was a critical attack in that ongoing battle, officials said, and it went forward even after President Trump called off a retaliatory airstrike that day after Iran shot down an American drone. Iran has not escalated its attacks in response, continuing its cyberoperations against the United States government and American corporations at a steady rate, according to American government officials. **American cyberoperations are designed to change Iran’s behavior without initiating a broader conflict or prompting retaliation**, said Norman Roule, a former senior intelligence official. Because they are rarely acknowledged publicly, cyberstrikes are much like covert operations, he said. You have 3 free articles remaining. Subscribe to the Times “You need to ensure your adversary understands one message: The United States has enormous capabilities which they can never hope to match, and it would be best for all concerned if they simply stopped their offending actions,” Mr. Roule said. Defying U.S. Sanctions, China and Others Take Oil From 12 Iranian Tankers The U.S. has been unable to halt Iranian oil exports. Cyberoperations do not work exactly like other conventional warfare. A cyberattack does not necessarily deter future aggression in the same way a traditional military strike would, current and former officials say. That is in part because cyberoperations are hard to attribute and not always publicly acknowledged by either side, the senior defense official said. [Sign up for the weekly At War newsletter to follow the cyber conflict between Iran and the United States.] Yet cyberoperations can demonstrate strength and show that the United States will respond to attacks or other hostile acts and impose costs, the official said.

#### Cyber-attacks will always remain heavily limited in physical impact

**Lacy 18**

Mark Lacy & Daniel Prince, 2-15-2018, “Securitization and the global politics of cybersecurity “, Global Discourse, [https://sci-hub.tw/https://www.tandfonline.com/doi/abs/10.1080/23269995.2017.1415082?scroll=top&needAccess=true&journalCode=rgld20](https://sci-hub.tw/https:/www.tandfonline.com/doi/abs/10.1080/23269995.2017.1415082?scroll=top&needAccess=true&journalCode=rgld20)

Of course, one of the arguments in this terrain is that in the coming century, non-state actors will be empowered in new ways. But, for the digital realist, it is unlikely to get to the point where they could do anything significant: critical infrastructures are too resilient (Calvety 2008, 139); states will retain the monopoly over violence and weapons of mass destruction (and the monopoly of cyber-offensive and cyber-defensive capability). Some might argue that the cyberweapons that states have deployed – such as Stuxnet – will be developed and used by non-state actors. But malware like Stuxnet are expensive to develop and require long-term planning and research, with a high level of access to information about the infrastructure that will be attacked (Singer and Friedman 2013). Malware like Stuxnet are state-of-the art projects by the most powerful actors in the international system, and even if non-state actors develop similar projects in coming decades, they will have to deal with the fact that there will be increased research and development in the protection of systems. Of course, there could be well-funded research facilities in shadow economies and failed states but there are less sophisticated ways of making money or making a political point. As Myriam Dunn Calvety suggests, ‘[t]hese doomsday scenarios are quite frightening. But it is good to know that they are about as likely to happen as a landing of alien spaceships’ (2011). The digital realist would argue that we should continue to focus on the development of offensive and defensive cybersecurity and cyberwar strategies. But **we need** to be careful **not to equate cyberweapons with** ‘game changers’ thatwill transform the future of war andcreate **the possibility for destructive scenarios common in science fiction movies.** On this view, **there will always be technical fixes to secure critical infrastructures**; non-state (and non-West) **[and] actors will lack the capability and** states – even if they could – would lack the **incentive to create a cyber-catastrophe that resulted in ‘physical’ violence.** We have to recognize that there are limits to what we can do: cyberspace is only partly controlled or controllable by governments. For the digital realist, it all comes back to the problem of resources. We do not want to over-react in our response to threats with costly measures and uncertain benefits, leaving government with less for middle to low impact but high-probability threats (Calvety 2008, 151). Like Hansen and Nissenbaum, the digital realist suggests that we need to counter hypersecuritizations, remaining alert to the possibility that the conditions of cyberwar may change – but for now are twenty-first-century nuisances with primarily social and economic consequences. The questions the digital realist leaves us with are: how can we avoid GLOBAL DISCOURSE 9 exaggerating the threat of cyberwar – and how (for the more ‘strategically’ minded) can we use these new techniques and technologies to ‘improve’ performance in our traditional militaries without creating new vulnerabilities?

#### The lack of visible and physical effects means that support for retaliation is far less likely with cyber operations

**Kreps 19**

Sarah Kreps, 9-29-2019, "Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics," OUP Academic, <https://academic.oup.com/cybersecurity/article/5/1/tyz007/5575971>

Is there a cyber firebreak, and is it related to means or effects? Our study suggests that Americans’ propensity for escalatory responses to cyberattacks cannot be explained solely by the effects created by attacks. Just as other scholars have argued that a nuclear firebreak exists, it appears that a cyber firebreak exists at the bottom of the escalation ladder. According to our experimental findings, **cyberattacks** create a threshold that **restrain**s **the escalation of conflict**. For **the American public**, cyberattacks are qualitatively different than those of similar magnitude from other domains. They are **[is] statistically less likely to support retaliation with force**—escalation into a kinetic response—**when** our scenario took place **in the cyber domain**. Those differences in support for retaliation are significant even when the perceived magnitudes of the effects of the attack are the same. Our findings suggest an answer to our initial puzzle about the importance of means versus effects in modern escalation but also introduce new puzzles about the determinants of the cyber reverse-firebreak. What might explain the reluctance of individuals and the American population to respond in cyberspace? What is the mechanism through which the resistance to retaliation for cyberattacks operates? Several factors might come into play. First, although attribution has improved, individuals may have assumed that corroborating a perpetrator would be more difficult, thereby also dampening their willingness to engage in aggressive retaliatory responses. Second, individuals may find the types of kinetic consequences described in the cyber scenario implausible. Cyber is, by definition, virtual. **Since it does not create large**-scale **first-order effects** in the same way **as an explosive, it creates a cognitive dissonance for individuals considering responses to threats** emanating **from cyberspace. Individuals cannot fear cyberattacks that lack a physical quality** that they have **evolutionarily associated with death** or existential threat. If cyber creates this cognitive distance, then the cyber firebreak may be as much a product of our constructed understandings of threat as the nuclear taboo. The findings also raise the question of whether the responses we observed are idiosyncratic to the American public or might they generalize to other countries? On the one hand, the USA is more digitally dependent than most nations, a vulnerability that might have made its public more protective in response to cyberattacks, which might mean other countries’ publics are even less prone to retaliation. On the other hand, the USA retains conventional military superiority and a geographic advantage against any military invasion, which means Americans are willing to absorb some level of cyberattacks both because it always has other capabilities to fall back on and out of a fear that retaliation could escalate into a Pandora’s box of large-scale cyberattacks on US digital capabilities. In any case, further research is warranted to understand whether the US results generalize and which cultural, structural, or institutional factors might condition the public’s propensity for retaliation.

**These more restricted attacks are especially important when considering alternatives, as the implications are detrimental**

#### Iran has clearly indicated that a military strike would prompt an all-out war

**Khalid 19**

Tuqa Khalid, 9-20-2019, "Military strike against Iran would result in 'all-out war': Zarif," Reuters, <https://www.reuters.com/article/us-saudi-aramco-zarif-war/military-strike-against-iran-would-result-in-all-out-war-zarif-idUSKBN1W41II>

DUBAI (Reuters) - Any U.S. or Saudi military strike against Iran would bring “all-out war”, Tehran said on Thursday, keeping up a drumbeat of warnings to its adversaries after they accused the Islamic Republic of a strike on Saudi oil facilities. Zarif said on Thursday any U.S. or Saudi military strike against Iran would result in "all-out war". The United States has been discussing with Saudi Arabia and other Gulf allies possible responses to Saturday’s attack, which they blame on Iran and which U.S. Secretary of State Mike Pompeo described as an act of war on the kingdom. “I am making a very serious statement that **we don’t [Iran doesn’t] want** **war**; we don’t want to engage in a military confrontation ... **But** we **[they] won’t blink to defend** our **territory**,” Iranian Foreign Minister Mohammed Javad Zarif told CNN in an interview. **Asked what** **the** **consequence of an American** or a Saudi military **strike on Iran would be, Zarif said “an all-out war”.** Zarif earlier warned on Twitter that what he described as the B team - including Israeli Prime Minister Benjamin Netanyahu and Saudi Crown Prince Mohammed Bin Salman - was deceiving U.S. President Donald Trump into a war against Iran.

### MPX: Extinction

**The impact is nuclear disaster**

#### An attack on Iran forces preemptive strikes and likely nuclear conflict

**Kahl 12**

Colin Kahl, 4-xx-2012, "Not Time to Attack Iran," Foreign Affairs, <https://www.foreignaffairs.com/articles/iran/2012-01-17/not-time-attack-iran?page=show>

RIDING THE ESCALATOR Kroenig's discussion of timing is not the only misleading part of his article; so is his contention that the United States could mitigate the "potentially devastating consequences" of a strike on Iran by carefully managing the escalation that would ensue. His picture of a clean, calibrated conflict is a mirage. Any war with Iran would be a messy and extraordinarily violent affair, with significant casualties and consequences. According to Kroenig, Iran would not respond to a strike with its "worst forms of retaliation, such as closing the Strait of Hormuz or launching missiles at southern Europe" unless its leaders felt that the regime's "very existence was threatened." To mitigate this risk, he claims, the United States could "make clear that it is interested only in destroying Iran's nuclear program, not in overthrowing the government." But [and] Iranian leaders have staked their domestic legitimacy on resisting inter-national pressure to halt the nuclear program, and so they would inevitably view an attack on that program as an attack on the regime itself. Decades of hostility and perceived U.S. efforts to undermine the regime would reinforce this perception. And when combined with the emphasis on anti-Americanism in the ideology of the supreme leader and his hard-line advisers, as well as their general ignorance about what drives U.S. decision-making, this perception means that there is little prospect that Iranian leaders would believe that a U.S. strike had limited aims. Assuming the worst about Washington's intentions, **Tehran is likely to overreact to even a surgical strike** against its nuclear facilities. Kroenig nevertheless believes that the United States could limit the prospects for escalation by warning Iran that crossing certain "redlines" would trigger a devastating U.S. counterresponse. Ironically, Kroenig believes that **a nuclear**-armed **Iran would be deeply** irrational and **prone to miscalculation** yet somehow maintains that under the same leaders, Iran would make clear-eyed decisions in the immediate aftermath of a U.S. strike. But **[as] the two countries share no direct and reliable channels for communication, and the inevitable confusion brought on by a crisis would make signaling difficult and miscalc**ulation **likely**. To make matters worse, in the heat of battle, **Iran would face powerful incentives to** escalate. In the event of a conflict, both sides would come under significant pressure to stop the fighting due to the impact on international oil markets. Since this would limit the time the Iranians would have to reestablish deterrence, they might choose to **launch a[n]** quick, **all-out response, without care for redlines**. **[as] Iranian fears that the United States could success-fully disrupt its** command-and-control **infrastructure or preemptively destroy its ballistic missile arsenal could** also **tempt Iran** **to launch as many missiles as possible** early in the war. And the decentralized nature of Iran's Islamic Revolutionary Guard Corps, especially its navy, raises the prospect of unauthorized responses that could rapidly expand the fighting in the crowded waters of the Persian Gulf. **Controlling escalation would be no easier on the U.S. side**. In the face of reprisals by Iranian proxies, "token missile strikes against U.S. bases and ships," or "the harassment of commercial and U.S. naval vessels," Kroenig says that Washington should turn the other cheek and constrain its own response to Iranian counter-attacks. But this is much easier said than done. Just as Iran's likely expectation of a short war might encourage it to respond disproportionately early in the crisis, so the United States would also have incentives to move swiftly to destroy Iran's conventional forces and the infrastructure of the Revolutionary Guard Corps. And if the United States failed to do so, **proxy attacks** against U.S. civilian personnel in Lebanon or Iraq, the transfer of lethal rocket and portable air defense systems to Taliban fighters in Afghanistan, or missile strikes against U.S. facilities in the Gulf **could cause significant U.S. casualties**, **creating irresistible** political **pressure in Washington to respond.** Add to this the normal fog of war and the lack of reliable communications between the United States and Iran, and Washington would have a hard time determining whether Tehran's initial response to a strike was a one-off event or the prelude to a wider campaign. If it were the latter, a passive U.S. approach might motivate Iran to launch even more dangerous attacks -- and this is a risk Washington may choose not to take. The sum total of these dynamics would make staying within Kroenig's proscribed limits exceedingly difficult. Even if Iran did not escalate, purely defensive moves that would threaten U.S. personnel or international shipping in the Strait of Hormuz -- the maritime chokepoint through which nearly 20 per- -cent of the world's traded oil passes -- would also create powerful incentives for Washington to preemptively target Iran's military. Of particular concern would be Iran's "anti-access/area-denial" capabilities, which are designed to prevent advanced navies from operating in the shallow waters of the Persian Gulf. These systems integrate coastal air defenses, shore-based long-range artillery and antiship cruise missiles, Kilo-class and midget submarines, remote-controlled boats and unmanned kamikaze aerial vehicles, and more than 1,000 small attack craft equipped with machine guns, multiple-launch rockets, antiship missiles, torpedoes, and rapid-mine-laying capabilities. The entire 120-mile-long strait sits along the Iranian coastline, within short reach of these systems. In the midst of a conflict, the threat to U.S. forces and the global economy posed by Iran's activating its air defenses, dispersing its missiles or naval forces, or moving its mines out of storage would be too great for the United States to ignore; the logic of preemption would compel Washington to escalate. Some analysts, including Afshin Molavi and Michael Singh, believe that the Iranians are unlikely to attempt to close the strait due to the damage it would inflict on their own economy. But Tehran's saber rattling has already intensified in response to the prospect of Western sanctions on its oil industry. In the immediate aftermath of a U.S. strike on Iran's nuclear program, Iranian leaders might perceive that holding the strait at risk would encourage international pressure on Washington to end the fighting, possibly deterring U.S. escalation. In reality, it would more likely have the opposite effect, encouraging aggressive U.S. efforts to protect commercial shipping. The U.S. Navy is capable of keeping the strait open, but the mere threat of closure could send oil prices soaring, dealing a heavy blow to the fragile global economy. The measures that Kroenig advocates to mitigate this threat, such as opening up the U.S. Strategic Petroleum Reserve and urging Saudi Arabia to boost oil production, would be unlikely to suffice, especially since most Saudi crude passes through the strait.

#### In fact, an attack on Iran spurs regional instability and drawing in nuclear actors which causes miscalculation and nuclear war. This results in global famine destroying human civilization.

**Avery 13**

John Avery, 9-06-2013, "An Attack On Iran Could Escalate Into Global Nuclear War By John Scales Avery," Counter Currents, <https://www.countercurrents.org/avery061113.htm> (QUALS: John Avery studied theoretical chemistry at the University of London, and was awarded a Ph.D. there in 1965. He is now Associate Professor, at the Department of Chemistry, University of Copenhagen. He has been the Contact Person in Denmark for Pugwash Conferences on Science and World Affairs. In 1995, this group received the Nobel Peace Prize for their efforts.)

Despite the willingness of Iran's new President, Hassan Rouhani to make all reasonable concessions to US demands, Israeli pressure groups in Washington continue to demand **an attack on Iran**. But such an attack **might escalate into a global nuclear war**, with catastrophic consequences. As we approach the 100th anniversary World War I, we should remember that this colossal disaster escalated uncontrollably from what was intended to be a minor conflict. There is a danger that an attack on Iran **[because it] would escalate into a large-scale war in the Middle East, entirely destabilizing a region** that is **already deep in problems**. The unstable government of Pakistan might be overthrown, and **the revolutionary Pakistani government might enter the war** on the side of Iran, thus **introducing nuclear weapons into the conflict**. Russia and China, firm allies of Iran, might also be drawn into a general war in the Middle East. Since much of the world's oil comes from the region, such a war would certainly cause the price of oil to reach unheard-of heights, with catastrophic effects on the global economy. In the dangerous situation that could potentially result from an attack on Iran, there is a risk that **[and] nuclear weapons would be used, either intentionally, or** byaccident or **miscalculation.** Recent research has shown that besides making large areas of the world uninhabitablethrough long-lasting radioactive contamination, **a nuclear war would damage global agriculture to** **such** a **extent that a global famine** of previously unknown proportions **would result**. Thus, **nuclear war** is the ultimate ecological catastrophe. It **could destroy** human **civilization and much of the biosphere.** To risk such a war would be an unforgivable offense against the lives and future of all the peoples of the world, US citizens included. To accept money from agents of a foreign power to perform actions that put one's own country in danger is, by definition, an act of treason. Why are members of the US Senate and House of Representatives, who demonstrably have accepted money from agents of a foreign power, the State of Israel, not accused of treason when they are bribed to take actions that put their country in danger? If members of the US government should vote for an attack on Iran, they would be traitors not only to the United States, but to all of humanity, and indeed traitors to all living things.

**Now for a brief overview**

**The pure severity and scope of our impact means**

# Frontlines

## AT: Cancellation Unrelated

**While the cyber operation was in relation to military strikes, that does not interact with our warrant. The U.S refuses to allow Iran to get away with military aggression and needs to signal concern. We indicate that the military strike was cancelled because it was more de-escalatory to only use cyber to accomplish this goal and thus: providing a crucial off-ramp from war. That’s the Handler 19 evidence from case**

## AT: Escalation

### AT: Attacks Increasing

**Increasing external tensions are causing more cyber operations, and that’s good because they are made to be de-escalatory and provide an off-ramp from war. Even increasing attacks won’t ever prompt physical violence they are easily fixed. This along with a lack of physical quality that spurs the need for physical retaliation means that escalation does not happen. That’s the Lacy 18 evidence read in case**

**EXT EMBED: This is crucial as cyber operations cover the U.S requirement to show that attacks cannot go ignored. This means that the military strikes that would’ve been a necessity now become unnecessary. That’s the Handler 19 evidence read in case**

## AT: Spark

**Cyber operations directly prevent war so the notion that it’s inevitable is unrealistic. Nations use cyber as offramp from conflicts and the disaster scenarios are all circumvented. This short-circuits the solvency and is preferable to slaughtering everyone who didn’t [Whatever method used to protect people].**