# 1NC – Flow Judge

## C1: Iranian Disaster

**It’s going to be one off**

**Start with one massive DISAD**

**Our Sole Contention is Iranian Escalation**

**U.S Offensive Cyber Operations will cause a global disaster stemming from Iran in 2 ways**

### Link – Conventional Escalation

**The first cause of conflict from OCO’s is escalation**

#### The new U.S cyber strategy lays the groundwork for tit-for-tat high-stake escalation

**Farrell 19**

Michael Farrell & Tim Starks & Gavin Bade, 7-13-2019, "Trump is rattling sabers in cyberspace — but is the U.S. ready? ," POLITICO, https://www.politico.com/story/2019/07/13/trump-cybersecurity-defense-1415650

The Trump administration is sending aggressive messages about the United States' willingness to hack its adversaries — alarming lawmakers and experts who fear the president is provoking a global cyberconflict that the U.S. may not be prepared to face. **A U.S. cyberattack on Iranian military** and intelligence **targets last month** was one of the most prominent signs of the new approach, which comes after a reported effort to implant hostile computer code in Russia's electrical grid and a temporary takedown of a notorious Kremlin-backed troll operation last fall. To supporters, the tactics are a **sign the U.S. may** finally **be getting out of its defensive crouch in cyberspace** — as advocated by hawks such as national security adviser John Bolton. But **the moves** also **lay** the potential **groundwork for** a **tit for tat of cyberattacks that** could **inflict significant damage on bystanders. Targets such as banks, hospitals, oil companies and electric utilities** in the U.S. and elsewhere **have already proved vulnerable**, as seen in recent criminal hacks that paralyzed entities such as Baltimore's city government. Now, both Republican and Democratic members of Congress are pressing the White House for details about its offensive cyber strategies, worried that unchecked operations could be dangerously destabilizing for the U.S. “It’s essential that Congress have its ability to conduct proper oversight. It’s our constitutional responsibility,” Rep. Jim Langevin (D-R.I.) told POLITICO. “I support the administration’s plan to be more forward-leaning in cyberspace, on balance. But with that comes the responsibility to make sure we’re not undermining stability in cyberspace.” Langevin added an amendment to the National Defense Authorization Act, which the House passed Friday, to compel the White House to provide details of its new cyber strategy to the House Armed Services Committee. Despite repeated requests from the committee, the administration has not shared a secret presidential directive, National Security Presidential Memorandum 13, that President Donald Trump signed last year to give U.S. Cyber Command more authority to carry out digital attacks. Langevin, along with Republican and Democratic members of the committee, complained to the White House in a February letter that the committee has been in the dark about the Pentagon’s growing use of digital weapons. “This is my first time in 19 years of Congress that a document this major has not been provided to Congress. I can’t understand what the holdup is,” Langevin said. “I just want to make sure the authorities being delegated are appropriate and our cyber missions are staying within those parameters.”

#### Furthermore, Iranian cyber-attacks are rapidly evolving to attack U.S critical infrastructure with serious domestic implications

**Fixler 19**

Annie Fixler, 3-11-2019, "Are we underestimating Iran's cyber capabilities?," TheHill, https://thehill.com/opinion/cybersecurity/433431-are-we-underestimating-irans-cyber-capabilities

After all, Tehran did reportedly conduct a similar operation in 2017 against the British parliament. In that attack, hackers compromised dozens of email accounts belonging to lawmakers by identifying accounts with weak passwords and without two-factor authentication. While Downing Street has not publicly identified the hacker, British news outlets reported that British intelligence has attributed the attack to Iran. In its annual Worldwide Threat Assessment, the U.S. Intelligence Community concluded that Iranian hackers are only capable of “causing localized, temporary disruptive effects.” Yet, the assessment also cautioned that “**Iran uses increasingly sophisticated cyber techniques**,” **and is attempting** to deploy capabilities **to attack U.S.** and allied **critical infrastructure**. In fact, as the cybersecurity firm FireEye warned in January, Iranian operations pose a threat to “a wide variety of sectors and individuals on a global scale.” A European Union report released the same month concluded that **Iran will likely** “**intensify state-sponsored cyber threat activities**.” Recent statements from the U.S. and Israeli governments offered further details about the threat. Last month, the Justice Department unsealed an indictment against a U.S. citizen and four Iranian operatives who were targeting U.S. government and intelligence agents. The operatives created fake Facebook profiles to trick victims into accepting friend requests and, in at least one case, adding the fake persona to a private Facebook group “composed primarily of USG Agents.” Although not alleged in the indictment, access to this group likely provided the hackers with additional information and targets to expand their operation. The indictment indicates, though, that Iran’s use of phishing emails failed to convince the targets to click malicious links and download malware. The emails are poorly written, with grammatical and spelling errors. **And** yet, the Justice Department noted, **had** these **[previous] efforts succeeded** or had a victim inadvertently clicked the link, **the operation would “have brought serious damage to the United States.”** In fact, a week earlier, DHS had issued an emergency directive to all federal agencies to take steps to protect their infrastructure from an operation posing “significant and imminent risks to agency information and information systems.” While DHS did not attribute the operation to Iran, the emergency directive coincided with the release of a FireEye report on a global campaign targeting the same infrastructure. The company confirmed that its initial research pointed to Iran. The Israeli military’s outgoing cyber chief, meanwhile, has been raising alarms about Iran’s cyber capabilities. Brigadier-General Noam Sha’ar told Israel Hayom that one of his division’s first operational events was the detection and prevention of an attempt to infiltrate Israel’s home front missile alert system. By corrupting the missile warning system, hackers could have activated false alerts. Even worse, when the system detected incoming rockets, hackers could have prevented sirens from activating so that civilians would not know to take cover.

#### Empirics confirm new-found escalation as cyber-attacks between Iran and the U.S are becoming rapidly more frequent and severe

**Abdollah 19**

Tami Abdollah, 6-24-2019, "Iran Increases Cyber Attacks on U.S. Gov't, Infrastructure: Cyber Security Firms," Insurance Journal, <https://www.insurancejournal.com/news/national/2019/06/24/530257.htm>

**Iran has increased** its offensive **cyberattacks against the U.S.** government and **critical infrastructure as tensions have grown** between the two nations, cybersecurity firms say. In recent weeks, hackers believed to be working for the Iranian government have targeted U.S. government agencies, as well as sectors of the economy, including oil and gas, sending waves of spear-phishing emails, according to representatives of cybersecurity companies CrowdStrike and FireEye, which regularly track such activity. It was not known if any of the hackers managed to gain access to the targeted networks with the emails, which typically mimic legitimate emails but contain malicious software. **The cyber offensive is the latest** chapter **in** the U.S. and Iran’s **ongoing cyber operations targeting the other, with** this **[a] recent sharp increase in attacks** occurring after the Trump administration imposed sanctions on the Iranian petrochemical sector this month. **Tensions have escalated** **since** **the U.S.** withdrew from the 2015 nuclear deal with Iran last year and began a **policy of “maximum pressure.”** Iran has since been hit by multiple rounds of sanctions. Tensions spiked this past week after Iran shot down an unmanned U.S. drone — an incident that nearly led to a U.S. military strike against Iran on Thursday evening. “Both sides are desperate to know what the other side is thinking,” said John Hultquist, director of intelligence analysis at FireEye. “You can absolutely expect the regime to be leveraging every tool they have available to reduce the uncertainty about what’s going to happen next, about what the U.S.’s next move will be.” CrowdStrike shared images of the spear-phishing emails with The AP. One such email that was confirmed by FireEye appeared to come from the Executive Office of the President and seemed to be trying to recruit people for an economic adviser position. Another email was more generic and appeared to include details on updating Microsoft Outlook’s global address book. The Iranian actor involved in the cyberattack, dubbed “Refined Kitten” by CrowdStrike, has for years targeted the U.S. energy and defense sectors, as well as allies such as Saudi Arabia and the United Arab Emirates, said Adam Meyers, vice president of intelligence at CrowdStrike. The National Security Agency would not address discuss Iranian cyber actions specifically but said in a statement to The Associated Press on Friday that “there have been serious issues with malicious Iranian cyber actions in the past.” “In these times of heightened tensions, it is appropriate for everyone to be alert to signs of Iranian aggression in cyberspace and ensure appropriate defenses are in place,” the NSA said. Iran has long targeted the U.S. oil and gas sectors and other critical infrastructure, but those efforts dropped significantly after the nuclear agreement was signed. After President Donald Trump withdrew the U.S. from the deal in May 2018, cyber experts said they have seen an increase in Iranian hacking efforts. “This is not a remote war (anymore),” said Sergio Caltagirone, vice president of threat intelligence at Dragos, Inc. “This is one where Iranians could quote unquote bring the war home to the United States.”

#### U.S officials have confirmed the use nuclear and conventional weapons to retaliate against major cyber-attacks. This means the line between cyber and war is very thin, and escalation is probable.

**Sanger 18**

David Sanger and William Broad, 1-16-2018, "Pentagon Suggests Countering Devastating Cyberattacks With Nuclear Arms," No Publication, https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html

WASHINGTON — **A newly drafted United States nuclear strategy** that has been sent to President Trump for approval would permit the use of nuclear weapons to respond to a wide range of devastating but non-nuclear attacks on American infrastructure, including what current and former government officials described as the most crippling kind of cyberattacks. For decades, American presidents have threatened “first use” of nuclear weapons against enemies in only very narrow and limited circumstances, such as in response to the use of biological weapons against the United States. But the new document **is the first to expand** that **to include attempts to** **destroy wide-reaching infrastructure**, like a country’s power grid or communications, that would be most **vulnerable to cyberweapons**. The draft document, called the Nuclear Posture Review, was written at the Pentagon and is being reviewed by the White House. Its final release is expected in the coming weeks and represents a new look at the United States’ nuclear strategy. The draft was first published last week by HuffPost. It called the strategic picture facing the United States quite bleak, citing not only Russian and Chinese nuclear advances but advances made by North Korea and, potentially, Iran. A spotlight on the people reshaping our politics. A conversation with voters across the country. And a guiding hand through the endless news cycle, telling you what you really need to know. “We must look reality in the eye and see the world as it is, not as we wish it to be,” the draft document said. The Trump administration’s new initiative, it continued, “realigns our nuclear policy with a realistic assessment of the threats we face today and the uncertainties regarding the future security environment.” The Pentagon declined to comment on the draft assessment because Mr. Trump has not yet approved it. The White House also declined to comment. You have 1 free article remaining. Subscribe to the Times But **three** current and former **senior government officials said large cyberattacks against the United States** and its interests **would be included in the kinds of foreign aggression that** could **justify** a **nuclear** response — though they stressed there would be other, more **[and] conventional** options for **retaliation**. The officials spoke on the condition of anonymity because they are not authorized to discuss the proposed policy. Gary Samore, who was a top nuclear adviser to President Barack Obama, said much of the draft strategy “repeats the essential elements of Obama declaratory policy word for word” — including its declaration that the United States would “only consider the use of nuclear weapons in extreme circumstances to defend the vital interests of the United States or its allies and partners.” But the biggest difference lies in new wording about what constitutes “extreme circumstances.” In the Trump administration’s draft, those “circumstances could include significant non-nuclear strategic attacks.” It said that could include “attacks on the U.S., allied, or partner civilian population or infrastructure, and attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities.” Editors’ Picks Three Students, $3,000 and a Dream: An Affordable Brooklyn Apartment. Where Did They Wind Up? A Designer’s Suicide and the Clothes He Left Behind Stop! Don’t Charge Your Phone This Way The draft does not explicitly say that a crippling cyberattack against the United States would be among the extreme circumstances. But experts called a cyberattack one of the most efficient ways to paralyze systems like

### Link- Proliferation

**The second cause of conflict from OCO’s is Iranian proliferation**

#### Stuxnet exposed inefficiencies related to enrichment software that would have otherwise have not been noticed. Without this crucial piece of intel, Iran would have given up

Mahoney **13**

Jennifer O'Mahony, 5-23-2013, "IAEA confirms: Iran expanding uranium enrichment program," Telegraph, <https://www.telegraph.co.uk/technology/news/10076194/IAEA-confirms-Iran-expanding-uranium-enrichment-program.html>

In a report obtained by The Associated Press, the International Atomic Energy Agency (IAEA) said as many as **700 new** and more sophisticated **centrifuges had been installed since [Stuxnet]** the attack, **increasing** Iran's stock of **low-enriched uranium** **by eight per cent to nearly ten tons** **in** the last **three months alone**. The progress was not limited to centrifuges. Tehran had also "advanced" in building a plutonium-producing reactor in Arak, central Iran, capable of producing "several bombs a year," the report said. Stuxnet, a computer worm designed to cause the centrifuges that separate isotopes in a reactor to spin at dangerously high speeds, is believed to have infected the Iranian nuclear enrichment facility at Natanz in 2009 and 2010. It was discovered by the Iranians in 2010, and is alleged to have originated in the US or Israel. A study published in the Royal United Services Institute journal (RUSI) earlier this month and based on IAEA data claimed **the worm** had **exposed vulnerabilities** **in Iranian** enrichment **facilities that would otherwise have** **gone unnoticed**, **and** that **production** actually **went up after it was discovered**. Related Articles Stuxnet 'increased' nuclear potential 15 May 2013 The RUSI report also said uranium enriched to a higher concentration was also likely to be produced in greater quantities by Iran, a factor confirmed as a possibility in the IAEA's latest report with the installation of powerful new centrifuges. The 700 IR-2m centrifuges are of particular concern to those worried Iran may want to make nuclear arms, because they are believed to be able to enrich two to five times faster than Tehran's old machines. Dr Thomas Rid, Reader in War Studies at King's College, London, told the Telegraph that **Stuxnet had given Iran a "major incentive" to review its enrichment programe**. He said: "Stuxnet was a psychological operation, and the goal was to essentially make Iranian engineers think they [were] incompetent. "**[and] By finding out they were attacked they had a major incentive to go back to drawing board and look at the vulnerability of their system**. "**[critically, ]** **If you think you’re the problem you’re likely to give up, but if you think it’s the software you can fix it**". Iran's nuclear spokesman Fereidoun Abbasi had already confirmed earlier this year that more than 3,000 new high-tech centrifuges would phase out its older-generation enriching machines at Natanz.

#### Furthermore, issues revealed by Stuxnet were preventing Iran from successfully making weapon-level enrichment

**Hopkins 13**

Curt Hopkins, 5-15-2013, "Stuxnet virus may have actually helped the Iranian nuclear program," Daily Dot, <https://www.dailydot.com/news/stuxnet-virus-report-iran-nuclear-weapons/>

“While Stuxnet may have had the potential to seriously damage Iranian centrifuges,” reads the study’s abstract, “evidence of the worm’s impact is circumstantial and inconclusive. [Barzashka’s] analysis of the related data shows that the 2009 version of **Stuxnet was** neither very effective nor well-timed and, in hindsight, may have been of **net benefit to Tehran**.” It was of benefit because it pointed out **vulnerabilities in the Iranian system** that **might** well **have** remained hidden and **broken the progress of weapons development on its** **own**. The rushed conclusion that Stuxnet had succeeded also prematurely diverted attention from the Iranian nuclear program. **The number of machines operational** in Iranian nuclear plants has **climbed since Stuxnet hit** initially in 2009, **and uranium enrichment has continued** unremarked. “Inspectors’ records,” wrote Barzashka, “show that between May and August that year, while the total number of operational centrifuges decreased by more than 300, the amount of machines being installed grew by almost twice that amount. … It is clear that Iran’s ability to successfully install and operate new centrifuges was not hindered.” The conclusion? “Stuxnet was not very effective and was also ill-timed. If Iran had begun producing weapons-grade material, a cyber-attack could have bought concerned nations valuable time; it could have proved a crucial tactical advantage in dealing with the threat through other means. However, Iran was not on the brink of weaponising in 2009 and 2010, nor did Stuxnet considerably set back Iran’s nuclear programme and bomb-making potential. If anything, the malware – if it did in fact infiltrate Natanz – has made the Iranians more cautious about protecting their nuclear facilities, making the future use of cyber-weapons against Iranian nuclear targets more difficult.”

#### Now that Iran has the capacity and no reason to hold back, it has begun nuclearization

**Tirone 19**

Jonathan Tirone, 9-15-2019, "Iran’s Nuclear Program," Bloomberg, <https://www.bloomberg.com/quicktake/irans-uranium-enrichment>

Iran’s nuclear capabilities have been the subject of global hand-wringing for more than two decades. While Iran’s leaders long insisted the country was not building nuclear weapons, its enrichment of uranium and history of deception created deep mistrust. In 2015, after more than two years of talks and threats to bomb the country’s facilities, Iran and world powers agreed to settle the dispute. Their deal set limits on the Islamic Republic’s nuclear work in exchange for relief from economic sanctions that had cut off oil exports and hobbled its economy. Then in May 2018, President Donald Trump announced that the U.S. would abandon the pact and reinstate sanctions. Iran responded a year later by violating the deals’s limits on uranium enrichment. The Situation **In July,** 2019, **Iran confirmed that it** had **surpassed** **agreed caps on uranium stockpiles** **and** exceeded the allowable level of purity. It also **added new enrichment capacity.** Iran expects European parties to the nuclear accord — who want to keep the deal in place — to help it get around U.S. sanctions before it agrees to limit its activities again. The country had expected the pact to stimulate an economic revival, but the U.S. move instead provoked a recession. Under the agreement, which was struck by Iran, the U.S., China, France, Russia, Germany, the U.K. and the European Union, Iran maintained the ability to enrich uranium for peaceful purposes. It was allowed to keep 5,000 centrifuges to separate the uranium-235 isotope needed to induce a fission chain reaction. Iran had agreed under the accord that for 15 years it would not refine the metal to more than 3.7% enrichment — the level needed to fuel nuclear power plants — and would limit its enriched-uranium stockpile to 300 kilograms, or 3% of the amount it held in May 2015. The International Atomic Energy Agency verified that Iran eliminated its inventory of 20%-enriched uranium, which can be used to make medical isotopes and to power research reactors but could also be purified to weapons-grade material at short notice. Inspectors also confirmed that Iran destroyed a reactor capable of producing plutonium.

#### Once Iran proliferates, Israel will launch a military preemptive strike that would spiral into regional conflict

**Horschig 19**

Doreen Horschig, 6-20-2019, "Israel could strike first as tensions with Iran flare," Conversation, https://theconversation.com/israel-could-strike-first-as-tensions-with-iran-flare-119146

“Israel will not allow Iran to obtain nuclear weapons,” said Israeli Prime Minister Benjamin Netanyahu on June 17. Netanyahu also said Iran must be punished for violating the nuclear agreement. **Israel**, which has faced threats to its national security since its founding as a Jewish homeland in the Middle East in 1948, **is known to take aggressive, preventive action to protect itself** – **including by launching preemptive strikes on neighboring nations it perceives as threatening**. If international relations with Iran grow more volatile, Israel could take dramatic, unilateral action against its neighbor and longtime adversary. How the Begin Doctrine justifies preemptive strikes I’m an international security scholar who studies Israel’s proactive use of its military to prevent nuclear buildup in the Middle East. **Israel has a counterproliferation policy, called the Begin Doctrine, which allows it to wage preventive strikes** **against** **enemies with** weapons of mass destruction **[WMD] programs.** Using the Begin Doctrine as a justification for preemptive strikes, **the Israeli government has for decades** quietly **decimated nuclear** and chemical **facilities across the Middle East**. When President Saddam Hussein’s potential nuclear military ambitions raised concerns in 1981, the Israeli government destroyed an Iraqi nuclear reactor in a surprise attack called Operation Opera. “On no account shall we permit an enemy to develop weapons of mass destruction against the people of Israel,” a government release stated at the time. “We shall defend the citizens of Israel in good time and with all the means at our disposal.” In 2007, Israel responded to Syria’s failure to report its uranium processing by striking a nuclear reactor in the Deir ez-Zor region. The United States, which was reportedly informed ahead of the attack, made no effort to stop Israel. Israel has also been accused of sponsoring the assassinations of at least four Iranian nuclear scientists since 2010. The incidents have never been fully investigated, and Israel has neither confirmed nor denied responsibility for the targeted killings. Israel has also deterred nuclear proliferation in the Mideast using less lethal, more high tech strategies. In 2008 and 2009, Israel used computer malware called Stuxnet to disrupt Iran’s nuclear infrastructure. The program infected the software that controlled centrifuge speed at the Natanz nuclear plant, alternately speeding up and slowing down the machines that produce enriched uranium to cripple production of the material. The Obama administration secretly supported the cyberattacks. Though the United States, United Nations and other world powers officially condemned some of these unprovoked Israeli military aggression, other preemptive Israeli attacks have been met with silence from the international community. The international community may even appreciate Israel’s role as a nuclear nonproliferation watchdog in the Middle East, my research suggests. Israel has never been punished for attacking its neighbors’ weapons programs. Decades after Israel’s 1981 attack on Iraq’s nuclear plant, President Bill Clinton called it “a really good thing.” “It kept Saddam Hussein from developing nuclear power,” he said at the 2005 Davos World Economic Forum. “But it’s not clear to me they have that option in Iran,” he added. Israel vs. Iran That was 14 years ago. In 2005, Iran was just beginning its nuclear buildup. Today, **Israel’s government seems strong in its belief that it has the option to strike Iran.** Iran’s Islamic fundamentalist government is openly hostile to Israel. Citing fears that Iran would use nuclear weapons against Israel, Netanyahu has warned, “Iranian acquisition of nuclear weapons would be infinitely more costly than any scenario you can imagine to stop it.” He told Iran and other adversaries not to “test” Israel. If the nuclear deal ruptures further and Iran does restarting uranium enrichment, Israel might launch targeted airstrikes against it. Iran and Israel are longtime adversaries. Here, Iranians burn the flag of Israel at a march on ‘Jerusalem Day,’ May 31, 2019. Tasnim News Agency via Reuters Risks of an Israeli strike History suggests other countries are unlikely to actively deter Israeli military aggression in the guise of nuclear nonproliferation. The Trump administration has expressed anti-Iranian sentiment and is a staunch backer of Netanyahu’s government. And while European powers will recognize preemptive Israeli strikes on nuclear facilities as a violation of international law and of the sovereignty of Israel’s neighbors, they also see Iran’s nuclear program as a grave global security concern. A nuclear Iran could escalate ongoing Middle East conflicts into nuclear exchanges, and, as some commentators say, spur other regional powers like Saudi Arabia and Egypt to develop nuclear weapons themselves. Of course, potential Israeli attacks on Iran present their own serious risks. Because most of Iran’s reactors are in full operations, air strikes may mean cutting off the power supply to Iranian citizens and could release large amounts of radioactive contaminants into the air. Iran, a militarily well-equipped country, would surely retaliate against any Israeli attacks. **That**, too, **would trigger a conflict that would spiral throughout the Middle East.** Of course, Israel faced similar dangers when it went after the weapons programs of Syria, Iraq and other neighbors. If history is any guide, Israel may strike Iran while the world quietly watches.

### Impact

**The impact is nuclear catastrophe**

#### An attack on Iran spurs a global nuclear war from regional instability that causes extinction

**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 by** accident 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.

# 1NC – Lay Judge

# Overviews

## OV: Nukeniqueness

#### **Mutually assured destruction is empirically the most effective tool in preventing nuclear conflict. However, OCO’s are expanding to undermine a nation’s capacity to retaliate upsetting the informational symmetry that ensures the failure of deterrence. This means that nuclear scenarios are unique to OCO’s**

Lindsay 17

Erik Gartzke & Jon Lindsay, 2-14-2017, "Thermonuclear cyberwar," Journal Of Cybersecurity, <https://academic.oup.com/cybersecurity/article/3/1/37/2996537>

In the other direction, the unstable cyber domain can undermine the stability of nuclear deterrence. Most analysts who argue that the cyber–nuclear combination is a recipe for danger focus on the fog of crisis decision making [85–87]. Stephen Cimbala points out that today’s relatively smaller nuclear arsenals may perversely magnify the attractiveness of NC3 exploitation in a crisis: “Ironically, the downsizing of U.S. and post-Soviet Russian strategic nuclear arsenals since the end of the Cold War, while a positive development from the perspectives of nuclear arms control and nonproliferation, makes the concurrence of cyber and nuclear attack capabilities more alarming” [88]. Cimbala focuses mainly on the risks of misperception and miscalculation that emerge when a cyber attack muddies the transparent communication required for opponents to understand one another’s interests, redlines, and willingness to use force, and to ensure reliable control over subordinate commanders. Thus a nuclear actor “faced with a sudden burst of holes in its vital warning and response systems might, for example, press the preemption button instead of waiting to ride out the attack and then retaliate” [85]. The outcome of fog of decision scenarios such as these depend on how humans react to risk and uncertainty, which in turn depends on bounded rationality and organizational frameworks that might confuse rational decision making [89, 90]. These factors exacerbate a hard problem. Yet within a rationalist framework, cyber attacks that have already created their effects need not trigger an escalatory spiral. While being handed a fait accompli may trigger an aggressive reaction, it is also plausible that the target’s awareness that its NC3 has been compromised in some way would help to convey new information that the balance of power is not as favorable as previously thought. This in turn could encourage the target to accommodate, rather than escalate. While defects in rational decision making are a serious concern in any cyber–nuclear scenario, the situation becomes even more hazardous when there are rational incentives to escalate. Although “known unknowns” can create confusion, to paraphrase Donald Rumsfeld, the “unknown unknowns” are perhaps more dangerous. A successful clandestine penetration of NC3 can defeat the informational symmetry that stabilizes nuclear relationships. Nuclear weapons are useful for deterrence because they impose a degree of consensus about the distribution of power; each side knows the other can inflict prohibitive levels of damage, even if they may disagree about the precise extent of this damage. Cyber operations are attractive precisely because they can secretly revise the distribution of power. NC3 neutralization may be an expensive and rarified capability in the reach of only a few states with mature signals intelligence agencies, but it is much cheaper than nuclear attack. Yet the very usefulness of [and] cyber operations for nuclear warfighting ensure that deterrence failure during brinksmanship crises is more likely. [and] Nuclear states may initiate crises of risk and resolve to see who will back down first, which is not always clear in advance. Chicken appears viable, ironically, because each player understands that a nuclear war would be a disaster for all, and thus all can agree that someone can be expected swerve. Nuclear deterrence should ultimately make dealing with an adversary diplomatically more attractive than fighting, provided that fighting is costly—as would seem evident for the prospect of nuclear war—and assuming that bargains are available to states willing to accept compromise rather than annihilation. If, however, one side knows, but the other does not, that the attacker has disabled the target’s ability to perceive an impending military attack, or to react to one when it is underway, then they will not have a shared understanding of the probable outcome of war, even in broad terms. Consider a brinksmanship crisis between two nuclear states where only one has realized a successful penetration of the rival’s NC3. The cyber attacker knows that it has a military advantage, but it cannot reveal the advantage to the target, lest the advantage be lost. The target does not know that it is at a disadvantage, and it cannot be told by the attacker for the same reason. The attacker perceives an imbalance of power while the target perceives a balance. A dangerous competition in risk taking ensues. The first side knows that it does not need to back down. The second side feels confident that it can stand fast and raise the stakes far beyond what it would be willing to if it understood the true balance of power. Each side is willing to escalate to create more risk for the other side, making it more likely that one or the other will conclude that deterrence has failed and move into warfighting mode to attempt to limit the damage the other can inflict.

[OPTIONAL CARD]

#### Undermining of nuclear communication systems is the bright line for the elimination of mutually assured destruction

**Wright 19**

Morgan Wright, 1-17-2019, "Cybersecurity of our nuclear systems needs to be a top priority," The Hill, https://thehill.com/opinion/cybersecurity/425757-cybersecurity-of-our-nuclear-systems-needs-to-be-a-top-priority

But it’s two other state-actors, both state sponsors of terrorism, that can and do cause as much concern as China and Russia. Those countries would be Iran and North Korea. These concerns about our aging NC3 system and inadequate cybersecurity in general threaten to dilute the most effective weapon we have—deterrence. Here’s why. The 2018 NPR addresses the modernization of the NC3 system. Two paragraphs from that report should make us shudder. “Today’s NC3 system is a legacy of the Cold War, last comprehensively updated almost three decades ago. It includes interconnected elements composed of warning satellites and radars; communications satellites, aircraft, and ground stations; fixed and mobile command posts; and the control centers for nuclear systems. “While once state-of-the-art, the NC3 system is now subject to challenges from both aging system components and new, growing 21st century threats. Of particular concern are expanding threats in space and cyber space, adversary strategies of limited nuclear escalation, and the broad diffusion within DoD of authority and responsibility for governance of the NC3 system, a function which, by its nature, must be integrated.” This means North Korea and Iran now have the ability to impact the potent, and usually unspoken, threat of nuclear attack or retaliation. If they can compromise our aging NC3 [nuclear communication] networks, and plant the seeds of doubt, then they will have successfully turned a credible threat into a bluff. This also means North Korea and Iran will be able to join Russia and China in a club once limited to nations that were great powers. The 2018 NPR addresses an “evolving and uncertain international security environment.” This environment was eloquently captured by Admiral J.M. Richardson, Chief of Naval Operations, in the report “A Design for Maintaining Maritime Superiority” released in January of 2016. “For the first time in 25 years, the United States is facing a return to great power competition. Russia and China have both advanced their military capabilities to act as a global power… Others are now pursuing advanced technology, including military technologies that were once the exclusive province of great powers – this trend will only continue.” A recent report on the Cybersecurity of Nuclear Weapons sums it up succinctly. “A compromised nuclear system that cannot be trusted and lacks credibility will undermine nuclear deterrence and its rationale. Additionally, the assurances that nuclear weapons states make to allies would likely lose their reliability if an adversary could successfully hack into the nuclear weapons systems on which several countries rely.” With great power comes great responsibility. Our government must modernize our NC3 and ensure no one thinks we’re bluffing.

# Frontlines

## FL: Proliferation

### AT: Efficiency Inevitable

#### Enrichment efficiency was worsening prior to Stuxnet only bolstering our link and proving that OCO’s have streamlined Iranian weaponization.

**Lindsay 13**

Jon Lindsay, 8-01-2013, “Stuxnet and the Limits of Cyber Warfare”, Security Studies, [https://sci-hub.tw/https://www.tandfonline.com/doi/abs/10.1080/09636412.2013.816122?scroll=top&needAccess=true&journalCode=fsst20](https://sci-hub.tw/https:/www.tandfonline.com/doi/abs/10.1080/09636412.2013.816122?scroll=top&needAccess=true&journalCode=fsst20)

One can still argue that Stuxnet degraded long-term efficiency by cutting into Iranian spares and raising error rates. As we have seen, the attack appears to have been designed to chronically degrade enrichment rather than halt it altogether. The difficulty in evaluating this type of performance is that Natanz was already a very inefficient operation, and for reasons that had nothing to do with the worm. The IR-1 centrifuge is a notoriously unreliable design. Stuxnet broke 11.5 percent of the total of about 8,700 centrifuges installed, but that is just barely above the normal 10 percent error rate reported by the IAEA. 82 Moreover, a trend of **diminishing enrichment efficiency is visible from early 2008** (measured as a declining ratio of LEU output to feed gas), **which predates Stuxnet**. **Ironically**, because **Stuxnet** seems to have only damaged the empty centrifuges of module A26, the attack **actually** seems to have **improved** **overall centrifuge efficiency**. As the Iranians replaced centrifuges after the attack, overall efficiency at Natanz again declined, no doubt exacerbated by chronic IR-1 problems that had nothing to do with Stuxnet. Stuxnet was surely intended to exploit these prior inefficiencies at Natanz. One American planner reportedly said, “The thinking was that the Iranians would blame bad parts, or bad engineering, or just incompetence. The intent was that the failures should make them feel they were stupid, which is what happened. We soon discovered they fired people.”84 IAEA inspectors reported that “the Iranians had grown so distrustful of their own instruments that they had assigned people to sit in the plant and radio back what they saw.”85 Perhaps Stuxnet inflicted some additional friction on an already troubled program. However, the imperative for it to remain undiscovered amidst the noise placed an upper bound on the damage Stuxnet could inflict: too much and Iranians would know they were under attack. Anonymity enabled the attack, but maintaining anonymity imposed a restraint upon the attacker

# Short-Circuits

## SC: Economy

**They read economic impacts, but even conventional war with Iran devastates the global economy meaning the impact is also probable in the affirmative world.**

#### Iran retaliates to conflict with oil disruption causing a global price surge

**Haltiwanger 19**

John Haltiwanger, 9-19-2019, "Trump and Iran may be on the brink of a war that would likely be devastating to both sides," Business Insider, https://www.businessinsider.com/trump-iran-near-brink-of-a-war-that-would-likely-devastate-both-sides-2019-5

In terms of other geopolitical blowback, Iran is allied with Russia and China, and it's unclear how these major powers might react if conflict breaks out. Key US allies such as Israel and Saudi Arabia, which are adversaries of Iran and just a stone's throw away from it, would also likely get sucked into a US-Iran war. **A war with Iran could** also **be extraordinarily disruptive economically**, **given** it borders **the Strait of Hormuz, a** narrow **route that** roughly **one-third of** the **world**'s **oil**-tanker traffic **travels through.** Experts have predicted that **if the route were blocked, it would quickly lead to a 30% drop in daily global oil exports, and prices would rapidly go up**, The Washington Post reported.

#### These oil shocks would cause global recession

**Elliott 12**

Larry Elliott, 1-5-2012, "Why Iran could start the next global recession," Guardian, https://www.theguardian.com/business/economics-blog/2012/jan/05/iran-global-recession-oil-price

What does all this mean? In the very short term, there is little prospect of crude prices coming down to the sort of levels that would be expected given the current state of global demand – $75 a barrel or thereabouts. On the contrary, there is a higher chance of Brent climbing above $120 a barrel than there is of it falling below $100. In the slightly longer term, much depends on who wins the game of chicken. **If the Iranians** tough it out and are prepared to risk military action with the west by **clos**ing **the strait of Hormuz, the cost of crude could** easily **rocket** above $150 a barrel. **That would, without question, lead to a deep global recession** in 2012. Policymakers in the west are banking on weaker inflationary pressure this year boosting real incomes, and have certainly not factored a serious oil shock into the equation. And, as every finance minister and central banker knows, each and every recession since 1973 has been associated with a sharp increase in the cost of crude.

## SC: Terrorism