# 1NC Preset (Policy Speed)

**We negate**

**Resolved:** The United States’ use of offensive cyber operations benefits outweigh the harms

## Framing

**The framework is prioritizing existential threats**

#### Existential threats cannot be reactive off experience and require absolute preventative action

**Bostrom 02**

Nick Bostrom, 9-1-2002, “Existential Risk: Analyzing Human Extinction Scenarios and Related Hazards”, Journal of Evolution and Technology

Our **approach to existential risks cannot be** one of **trial-and-error. There is no opportunity to learn from errors.** The reactive approach – see what happens, limit damages, and learn from experience – is unworkable. Rather, **we must take a proactive approach.** This requires foresight to anticipate new types of **threats and a willingness to take decisive preventive action and to bear the costs** (moral and economic) **of such actions.** We cannot necessarily rely on the institutions, moral norms, social attitudes or national security policies that developed from our experience with managing other sorts of risks. Existential risks are a different kind of beast. We might find it hard to take them as seriously as we should simply because we have never yet witnessed such disasters.[[5]](https://nickbostrom.com/existential/risks.html" \l "_ftn5" \o ") Our collective fear-response is likely ill calibrated to the magnitude of threat. Reductions in existential risks are global public goods [13] and may therefore be undersupplied by the market [14]. Existential risks are a menace for everybody and may require acting on the international plane. Respect for national sovereignty is not a legitimate excuse for failing to take countermeasures against a major existential risk. If we take into account the welfare of future generations, the harm done by existential risks is multiplied by another factor, the size of which depends on whether and how much we discount future benefits [15,16].

#### The infinite nature of existential threats mean they always outweigh conventional impacts

**Schell 82**

Jonathan Schell, xx-xx-1982, “The Fate of the Earth”, Published Book, PAGE 93-96

To say that human extinction is a certainty would, of course, be a misrepresentation – just as it would be a misrepresentation to say that extinction can be ruled out. To begin with, we know that a holocaust may not occur at all. If one In the shadow of this power, the earth became small and the life of the human species doubtful. In that sense, the question of human extinction has been on the political agenda of the world ever since the first nuclear weapon was detonated, and there was no need for the world to build up its present tremendous arsenals before starting to worry about it. At just what point the species crossed, or will have crossed, the boundary between merely having the technical knowledge to destroy itself and actually having the arsenals at hand, ready to be used at any second, is not precisely knowable. But it is clear that at present, with some twenty thousand megatons of nuclear explosive power in existence, and with more being added every day, we have entered into the zone of uncertainty, which is to say **the** zone of **risk of extinction**. But the mere risk of extinction has a significance that **is** categorically different from, and immeasurably **greater than that of any other risk** and as we make our decisions we have to take that significance into account. Up to now, every risk has been contained within the framework of life; extinction would shatter the frame. It represents not the defeat of some purpose but an abyss in which all human purpose would be drowned for all time. **We have no right to place** the possibility of this limitless, **eternal defeat on the same footing as** risk that we run in the **ordinary** conduct of our **affairs** in our particular transient moment of human history. To employ a mathematician's analogy, we can say that although **[even if] the risk of extinction may be fractional**, the stake is, humanly speaking, infinite,and **a fraction of infinity is still infinity**. In other words, once we learn that a holocaust might lead to extinction we have no right to gamble, because if we lose, the game will be over, and neither we nor anyone else will ever get another chance. Therefore, although, scientifically speaking, there is all the difference in the world between the mere possibility that a holocaust will bring about extinction and the certainty of it, morally they are the same, and we have no choice but to address the issue of nuclear weapons as though we knew for a certainty that their use would put an end to our species. In weighing the fate of the earth and, with it, our own fate, we stand before a mystery, and in tampering with the earth we tamper with a mystery. We are in deep ignorance. Our ignorance should dispose us to wonder, our wonder should make us humble, our humility should inspire us to reverence and caution, and our reverence and caution should lead us to act without delay to withdraw the threat we now post to the world and to ourselves.

## C1: Iran

**Our Sole Contention is preventing Iranian Crisis**

**Two Links**

## Links

### Link - General Escalation

**The first is general escalation**

#### Trump’s new cyber strategy is the groundwork of 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.”

#### Empirically, Minor cyber operations elevate through the escalation ladder into attacking critical military and health-based infrastructure

**Powell 18**

Nadiya Kostyuk & Scott Powell & Matt Skach, 4-xx-2018, "Determinants of the Cyber Escalation Ladder," The Cyber Defense Review, <https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Determinants%20of%20the%20Cyber_Kostyuk_Powell_Skach.pdf?ver=2018-07-31-093725-923>

The Spectrum of Conflict’s lowest rung is a stable peace. **In** this **preparatory phase, cyber activity is directed towards developing the capability to offensive and defensive cyber actions**. This means that **effective cyber forces**, even with no immediate threat on the horizon, must **continuously build and maintain** its **cyber capabilities** by recruiting, training and organizing cyber forces as well as **providing them with the financial, technological, organizational, and infrastructure resources needed** for their mission. In addition, these forces should develop contingency plans and be ready to defend against threats in cyberspace that appear with little or no advanced warning. These conditions are needed in preparation for an adversary taking hostile actions towards unstable peace or any other form of escalation. In a conflict **that escalates into minor harassment, cyber activities expand to exploit weaknesses in an adversary’s system without disrupting operations or damage infrastructure**. The mission of the US cyber forces at this Spectrum level incorporates all of the prior actions and expands to include espionage and cyber counterintelligence, gathering credentials, and propaganda. Credential collection is an important activity to launch larger scale cyberattacks or facilitate the access of information on protected systems.[10]As intelligence gathering is an accepted norm, it should not be considered escalatory. Propaganda, although not explicitly a cyberattack, can incorporate cyber elements to enhance the spread or impact of a message. In response to the early conflict in Ukraine, social media emerged as a major channel of communication for protesters and international observers, and Russia utilized the “comments” section of news sites to promote pro-Russian dialogue on domestic and foreign websites. [11] In a more direct approach that may cross the border into unstable peace occurred during the 2016 US Presidential Election. Russia combined an extensive propaganda campaign with cyberattacks on the Democratic National Committee and subsequent release of damaging emails through WikiLeaks in an attempt to influence the outcome. [12] Moving upwards from stable peace to an unstable peace, cyber activities at the major harassment level aggressively exploit weaknesses and disrupt daily operations, but do not cause permanent damage to infrastructure or compromise systems. **On the conventional (non-cyber) side, sanctions are a common tool used by the US and exemplified by their reaction to Russian interference** in the 2016 Presidential election. [13] At this stage, **equivalent cyber operations include overt demonstrations of cyber capability** to deter the opponent **and minor** denial of service (**DOS**) **attacks** **that** exert influence but **do little permanent damage**. Overt displays of cyber capability such as the defacement of public websites were a common tool of the hacktivist group Anonymous during Operation China in response to China’s crackdown on protests. [13] Similarly, DOS attacks that deny cyber or non-cyber infrastructure can pose varying levels of inconvenience against an adversary. Lizard Squad, a hacktivist group, launched distributed denial of service (DDOS) attacks against Sony’s PlayStation Network and Microsoft’s Xbox Live services. [15] Website defacement Matt Skach is a PhD candidate in the Department of Computer Science and Engineering at the University of Michigan, and a combat engineer in the 1433rd Engineering Company of the Michigan Army National Guard. His research interests include novel design and technologies for large-scale computer systems and data centers. Skach has an MS in electrical engineering from the University of Michigan and a BS in electrical engineering from Oregon State University. DDOS by an adversary can present a significant inconvenience but poses little risk of permanent damage. **Although initiated in cyberspace, the impact of DOS and DDOS attacks are not limited to the cyber domain.** ‘SWATing’ [16] and other **attacks** that **focus on emergency services**, if applied on a large scale, could be **used to tie up law enforcement** **resources** and other emergency first responders (EFR). SWATing style attacks pose an increased risk of injury or loss of life over DOS cyberattacks, but neither of these incursions alone is likely to be escalatory. Moving up the escalation ladder from harassment to minor damaging attacks, cyberspace enables a range of low-financial-cost attacks that compromise non-critical data or inflict minor, repairable damage. Potential targets include the destruction of non-critical data on networked systems and the targeted harassment of military infrastructure. Sony Pictures suffered a massive data loss in 2014 at the hands of North Korean state hackers, [17] and Saudi Aramco lost data on 35,000 hard drives in a 2012 cyberattack. [18] The attacks did not pose a significant disruption of services outside of the affected company, and neither event prompted retaliation, but both companies faced severe financial costs to restore services. On the other hand, WannaCrypt, [19] one of the most significant Ransomware attacks to date, demonstrated the compelling capability to tie up businesses and critical services such as hospitals by encrypting data and holding it ransom until demands are met. There exists the potential for extensive collateral damage from this type of cyberattack. This is fundamentally different from traditional DOS attacks that temporarily make a site or service inaccessible, as opposed to Ransomware that may permanently destroy data if demands are not met. Although WannaCrypt primarily struck unpatched civilian targets, there is the potential for targeted harassment of military infrastructure. Interference actions that target noncritical military services stand to interrupt day-to-day operations by delaying email communication or hindering logistics, but do not pose a significant threat to critical military infrastructures such as strategic missile or air defense systems. Similarly, interference or delay of supplies can pose a problem, but outside of a war zone, it is unlikely to pose a critical threat to combat readiness. Highly targeted attacks with limited destructive capability such as Stuxnet [20] may also be deployed at this level. These attacks are not inherently escalatory, but depending on the target and duration of the attack **the risk posed by the vulnerability may be considered escalatory** (e.g., hindering communications may be seen as the prelude to a larger attack). **Smaller cyberattacks may also become escalatory** **when paired with other kinetic attacks**. A DOS attack on EFR services combined with a limited kinetic action **such as a drone strike could increase the** net effect **from a minor damaging attack** **to** **a major one** **when [emerging first responder]** EFR **resources are not immediately available to treat casualties**

#### U.S led escalation is already on track and Iran is the first victim.

**Kennedy 19**

David Kennedy, 10-5-2019, "How Iran Would Wage Cyber War Against the United States," National Interest, https://nationalinterest.org/blog/buzz/how-iran-would-wage-cyber-war-against-united-states-85841

While such a conflict is certainly possible, and the situation remains highly fluid, the reality is that neither Iran nor the United States actually wants a war. Iran knows it can’t withstand one against the United States, and President Donald Trump has stated repeatedly that he is disinclined to involve America in another “endless” Middle East war. This means both sides are likely to engage in a more covert battle of wills—and cyber will be a primary focus. **Cyberwarfare is an ideal tool** in this type of situation, **since** the risk of escalation from physical attacks remains high. Over the last fifteen years, **Iran has shown an increasing reliance on asymmetric warfare to confront,** challenge and undermine **U.S. interests in the region**, and since 2011 it has increasingly turned to cyber when doing so. On numerous occasions in the last nine years, **Iran’s cyber operations have demonstrated** to the world **that they are** **willing to act aggressively** **and**—some might say—**recklessly in cyberspace**, and to achieve only limited goals and objectives. With this in mind, here is a closer look at how Iran is likely to engage the United States in cyberspace. Iran’s Cyber Strategy 10 SECONDS Do You Know What Happened On This Day? **Iran** uses cyber mostly as an extension of its military forces, and it **seems less cognizant of red lines than other U.S. adversaries**. Just consider some of the brazen attacks it has carried out in recent years. **In 2012, it risked triggering a disruption** **in** **the international oil supply** when it launched a massive destructive malware attack on Saudi Aramco. **From 2011 to 2013, it targeted the U.S. financial sector in a widespread DDoS campaign** that disrupted services. **In 2013, it attempted to gain remote access to the sluice gate controls of a New York dam**, which could have produced the first cyber kinetic event on the U.S. homeland. As we’ve seen in Iran’s traditional military operations, from its September strike on Saudi oil facilities to the June shoot down of a U.S. drone in international waters and the 2016 interdiction of U.S. sailors in the Persian Gulf, Iran is both aggressive and unpredictable—to the point of being reckless. This is important in understanding how the Islamic Revolutionary Guard Corps (IRGC) is likely to approach future cyber operations against the United States. It has fewer restraints than other American adversaries (even Russia, North Korea and China), and is willing to act boldly and dangerously just to send a message. Iran’s Cyber Capabilities Since 2010, **when Iran’s nuclear industry was attacked by** a physically destructive malware called “**Stuxnet**,” **the country has been steadily ramping up its development of cyber warfare capabilities**. Although **Iran** is generally considered at least a step below the major cyber powers—the United States, Russia, China, Israel and our European allies—it **is clearly evolving rapidly**, **and** Iran’s leadership appears to appreciate the value of cyber as an effective retaliatory measure to U.S. attacks and provocations. Iran’s cyber operations are more decentralized than other leading cyber powers. It relies heavily on proxy cyber forces, and the extent to which the IRGC can directly control these groups is questionable, with some analysts suggesting it has less control than would be desirable. While Iran is likely to be developing its own custom cyber “weapons,” to date it has primarily relied on criminal malware and other tools it can modify for its own purposes. Iran is proficient in a variety of standard network attacks, such as phishing, DDoS, DNS hijacking and remote access, but it has also shown a developing ability to carry out more complicated attacks—particularly the infiltration of industrial control systems (ICS). What Role Will Proxy Forces Play? There is no scenario in which Iran’s proxy forces would not be utilized—and heavily—in a cyber conflict with the United States. They are vital to Iran’s overall strength in cyber, and its “show of force” tactics. However, between Iran’s questionable control of these groups and their reduced capabilities when compared with the IRGC, they would most likely be used in regional attacks on Gulf states—and, if extended to the United States, to soft targets only. How Would Iran Attack America? The Center for Strategic & International Studies (CSIS) offers this assessment of Iran: “Iranian [cyber] attacks are likely to be retaliatory, intending to make the point that the United States is not invulnerable but without going too far.” It goes on to say that, “Attacking major targets in the American homeland would be escalatory, something Iran wishes to avoid.” This is a fair assessment of Iran, but there is a lot of wiggle room in terms of what is considered “retaliatory”—as well as what Iran deems to be instigative and the timeframe for a response—and what constitutes “major targets” in the United States. Remember, Iran has already shown itself to be brazen in its attacks on U.S. homeland targets—and some describe the early 2010s cyber skirmishes with Iran as America’s first known cyberwar. Iran is likely to carry out the bulk of any attacks on Gulf state rivals, with a particular focus on the royals, government assets and oil and gas industry infrastructure. But **we should not underestimate its ability or willingness to attack important targets within the United States**. Whether it limits these attacks to soft targets, like media companies, think tanks, outspoken critics of Iran, etc., or instead goes after hard targets like the U.S. financial system, energy industry and government assets depends entirely on how escalatory the regime considers U.S. actions to be. What Trump calls “maximum pressure,” the Iranians view as “economic terrorism.” **To Iran’s leaders, any cyber offensive action taken at any time during the current standoff** and destabilizing economic sanctions **may be deemed justified as a retaliatory measure.** Could a Cyber War Escalate? Yes. The question isn’t so much “if” as “by how much?” Already, the United States, Iran and Saudi Arabia are in the early phases of conflict. It’s not unlikely that the United States will turn to Israel for additional support. A recent report by DarkMatter showed that cyber attacks (linked to Iran) have been increasing generally in the Middle East, particularly against the United Arab Emirates. We can expect that trend to continue and worsen as tensions mount. Iran is more likely to be the aggressor in these regional attacks, with countries like Saudi Arabia and the UAE largely playing defense. **Iran and its proxies will target the energy infrastructure, critical infrastructure and government networks of its regional rivals**, as it attempts to weaken those governments, signal the growing danger it can pose to the global energy market and in general create complications for the United States. A key question is what role China will play in the event of a serious escalation in cyber incidents. China is Saudi Arabia’s largest oil customer, and its economy can’t afford price hikes or supply disruptions. Conclusion Iran is a potent force in the cyber domain and the threats it poses should be taken seriously. **The chances are high that we will see an extended cyber conflict between the United States and Iran, which will likely spill over into other regional players**.

#### A cyberwar would quickly escalate to full-blown conflict

**Lindsey 19**

Nicole Lindsey, 10-14-2019, "Cyber War Between Iran and United States Could Have Far-Reaching Implications," CPO Magazine, https://www.cpomagazine.com/cyber-security/cyber-war-between-iran-and-united-states-could-have-far-reaching-implications/

Will cyber war lead to kinetic conflict? The biggest concern, of course, is that **cyber war will** eventually **lead to a shooting war**. We may already be seeing signs of this in the Middle East. Military attacks against drones, shipping vessels and oil facilities are tantamount to a declaration of war, so it’s not out of the question that the U.S. will respond in kind.Add in the fact that **the U.S. Cyber Command has transitioned from cyber defense to a more aggressive cyber posture, thanks to a new strategic philosophy known as “persistent engagement,”** and you can begin to grasp the enormity of the situation. Growing possibility that the tensions between Iran and the U.S. will lead to the militarization of cyberspace. It might be possible in today’s modern warfare arena to carry out missile strikes with lethal precision, but that still is not possible **with** today’s cyber weapons. If the world doesn’t want to wait around for a catastrophic event (such as a cyber Hiroshima) to take place involving **the digital equivalent of nuclear weapons**, then it’s now time to implement international norms and rules of engagement for reducing the risk of a cyber war becoming a full-fledged kinetic conflict with unimaginable loss of life.

### Link - NC3

**The second link undermining nuclear deterrence**

**First with a definition: NC3 sta**

#### Nuclear launch systems are dangerously vulnerable to cyberattacks that undermine 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

Cybersecurity of our nuclear systems needs to be a top priority. Many jokes have been made about who actually invented the internet, most notably after former Vice President Al Gore publicly declared he took the initiative to create it during his time in Congress. But credit — for the impetus, at least — for creation of the internet goes to the former Soviet Union (USSR). On October 4, 1957 the USSR launched Sputnik, the first artificial satellite. Then-Senate Majority Leader Lyndon B. Johnson remarked “Now, somehow, in some way, the sky seemed almost alien.” He remembered “the profound shock of realizing that it might be possible for another nation to achieve technological superiority over this great country of ours.” In February of 1958, the Advanced Research Projects Agency (ARPA) was born. According to the history of ARPA, the first three primary research priorities focused on space technology (to counter Sputnik), ballistic missile defense (to counter the USSR) and solid propellants (to eventually power the Minuteman ICBM). As ARPA grew, so did the threats they were being asked to counter. In the 1960s, telephone systems were copper wire and circuit-based. This made our primary means of communication vulnerable to a single missile strike by the USSR. What was needed was a “galactic network” of computers that would continue to function even if the Soviets devastated our telephone system. Twelve years after the launch of Sputnik, ARPAnet went live. On October 29, 1969 researchers at four universities delivered the first node-to-node communication. UCLA, Stanford, UC Santa Barbara and the University of Utah became the vanguard for what would become the modern internet. That invention is now coming back to threaten the very thing it was designed to counter; the threat of nuclear weapons. The Nuclear Posture Review (NPR) is a “legislatively-mandated review that establishes U.S. nuclear policy, strategy, capabilities and force posture for the next five to ten years.” The first NPR took place in 1994. In 2010, the NPR referred to ‘cyber’ once as the report only discussed the need to “protect its assets in cyberspace and outer space and enhanced by U.S. capabilities to deny adversaries’ objectives through resilient infrastructure (including command and control systems), global basing and posture, and ballistic missile defense and counter-WMD capabilities.” Fast forward to the 2018 Nuclear Posture Review and ‘cyber’ is mentioned sixteen times. This reflects the changing nature of our most critical systems, and the still-lacking protections our aging systems are dealing with. The most critical system is our Nuclear Command, Control and Communications (NC3). According the 2018 NPR, “The United States must have an NC3 system that provides control of U.S. nuclear forces at all times, even under the enormous stress of a nuclear attack. NC3 capabilities must assure the integrity of transmitted information and possess the resiliency and survivability necessary to reliably overcome the effects of nuclear attack.” What is most telling is what the report lists as the first initiative to ensure “our NC3 system remains survivable and effective. That initiative is “strengthening protection against cyber threats.” Since the 2010 NPR, the threats globally have worsened and include “an unprecedented range and mix of threats, including major conventional, chemical, biological, nuclear, space, and cyber threats, and violent non-state actors.” There is no doubt that Russia and China continue to be our biggest nuclear threats from a state-actor perspective. 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 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.

#### **The resulting muddled deterrence drastically increases probability of miscalc**

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 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.

## Impact

**The impact is nuclear catastrophe**

#### War with Iran spurs a global nuclear war 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 nuclear weapons would be used, either intentionally, or by accident or miscalculation.** Recent research has shown that **besides making large areas of the world uninhabitable** through 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 Preset (PF Judge Speed)

## C1: Iran

**Our Sole Contention is preventing Iranian Crisis**

**Two Links**

## Links

### Link - General Escalation

**The first is general escalation**

#### Trump’s new cyber strategy is the groundwork of 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.”

#### U.S led escalation is already on track and Iran is the first victim.

**Kennedy 19**

David Kennedy, 10-5-2019, "How Iran Would Wage Cyber War Against the United States," National Interest, https://nationalinterest.org/blog/buzz/how-iran-would-wage-cyber-war-against-united-states-85841

While such a conflict is certainly possible, and the situation remains highly fluid, the reality is that neither Iran nor the United States actually wants a war. Iran knows it can’t withstand one against the United States, and President Donald Trump has stated repeatedly that he is disinclined to involve America in another “endless” Middle East war. This means both sides are likely to engage in a more covert battle of wills—and cyber will be a primary focus. **Cyberwarfare is an ideal tool** in this type of situation, **since** the risk of escalation from physical attacks remains high. Over the last fifteen years, **Iran has shown an increasing reliance on asymmetric warfare to confront,** challenge and undermine **U.S. interests in the region**, and since 2011 it has increasingly turned to cyber when doing so. On numerous occasions in the last nine years, **Iran’s cyber operations have demonstrated** to the world **that they are** **willing to act aggressively** **and**—some might say—**recklessly in cyberspace**, and to achieve only limited goals and objectives. With this in mind, here is a closer look at how Iran is likely to engage the United States in cyberspace. Iran’s Cyber Strategy 10 SECONDS Do You Know What Happened On This Day? **Iran** uses cyber mostly as an extension of its military forces, and it **seems less cognizant of red lines than other U.S. adversaries**. Just consider some of the brazen attacks it has carried out in recent years. **In 2012, it risked triggering a disruption** **in** **the international oil supply** when it launched a massive destructive malware attack on Saudi Aramco. **From 2011 to 2013, it targeted the U.S. financial sector in a widespread DDoS campaign** that disrupted services. **In 2013, it attempted to gain remote access to the sluice gate controls of a New York dam**, which could have produced the first cyber kinetic event on the U.S. homeland. As we’ve seen in Iran’s traditional military operations, from its September strike on Saudi oil facilities to the June shoot down of a U.S. drone in international waters and the 2016 interdiction of U.S. sailors in the Persian Gulf, Iran is both aggressive and unpredictable—to the point of being reckless. This is important in understanding how the Islamic Revolutionary Guard Corps (IRGC) is likely to approach future cyber operations against the United States. It has fewer restraints than other American adversaries (even Russia, North Korea and China), and is willing to act boldly and dangerously just to send a message. Iran’s Cyber Capabilities Since 2010, **when Iran’s nuclear industry was attacked by** a physically destructive malware called “**Stuxnet**,” **the country has been steadily ramping up its development of cyber warfare capabilities**. Although **Iran** is generally considered at least a step below the major cyber powers—the United States, Russia, China, Israel and our European allies—it **is clearly evolving rapidly**, **and** Iran’s leadership appears to appreciate the value of cyber as an effective retaliatory measure to U.S. attacks and provocations. Iran’s cyber operations are more decentralized than other leading cyber powers. It relies heavily on proxy cyber forces, and the extent to which the IRGC can directly control these groups is questionable, with some analysts suggesting it has less control than would be desirable. While Iran is likely to be developing its own custom cyber “weapons,” to date it has primarily relied on criminal malware and other tools it can modify for its own purposes. Iran is proficient in a variety of standard network attacks, such as phishing, DDoS, DNS hijacking and remote access, but it has also shown a developing ability to carry out more complicated attacks—particularly the infiltration of industrial control systems (ICS). What Role Will Proxy Forces Play? There is no scenario in which Iran’s proxy forces would not be utilized—and heavily—in a cyber conflict with the United States. They are vital to Iran’s overall strength in cyber, and its “show of force” tactics. However, between Iran’s questionable control of these groups and their reduced capabilities when compared with the IRGC, they would most likely be used in regional attacks on Gulf states—and, if extended to the United States, to soft targets only. How Would Iran Attack America? The Center for Strategic & International Studies (CSIS) offers this assessment of Iran: “Iranian [cyber] attacks are likely to be retaliatory, intending to make the point that the United States is not invulnerable but without going too far.” It goes on to say that, “Attacking major targets in the American homeland would be escalatory, something Iran wishes to avoid.” This is a fair assessment of Iran, but there is a lot of wiggle room in terms of what is considered “retaliatory”—as well as what Iran deems to be instigative and the timeframe for a response—and what constitutes “major targets” in the United States. Remember, Iran has already shown itself to be brazen in its attacks on U.S. homeland targets—and some describe the early 2010s cyber skirmishes with Iran as America’s first known cyberwar. Iran is likely to carry out the bulk of any attacks on Gulf state rivals, with a particular focus on the royals, government assets and oil and gas industry infrastructure. But **we should not underestimate its ability or willingness to attack important targets within the United States**. Whether it limits these attacks to soft targets, like media companies, think tanks, outspoken critics of Iran, etc., or instead goes after hard targets like the U.S. financial system, energy industry and government assets depends entirely on how escalatory the regime considers U.S. actions to be. What Trump calls “maximum pressure,” the Iranians view as “economic terrorism.” **To Iran’s leaders, any cyber offensive action taken at any time during the current standoff** and destabilizing economic sanctions **may be deemed justified as a retaliatory measure.** Could a Cyber War Escalate? Yes. The question isn’t so much “if” as “by how much?” Already, the United States, Iran and Saudi Arabia are in the early phases of conflict. It’s not unlikely that the United States will turn to Israel for additional support. A recent report by DarkMatter showed that cyber attacks (linked to Iran) have been increasing generally in the Middle East, particularly against the United Arab Emirates. We can expect that trend to continue and worsen as tensions mount. Iran is more likely to be the aggressor in these regional attacks, with countries like Saudi Arabia and the UAE largely playing defense. **Iran and its proxies will target the energy infrastructure, critical infrastructure and government networks of its regional rivals**, as it attempts to weaken those governments, signal the growing danger it can pose to the global energy market and in general create complications for the United States. A key question is what role China will play in the event of a serious escalation in cyber incidents. China is Saudi Arabia’s largest oil customer, and its economy can’t afford price hikes or supply disruptions. Conclusion Iran is a potent force in the cyber domain and the threats it poses should be taken seriously. **The chances are high that we will see an extended cyber conflict between the United States and Iran, which will likely spill over into other regional players**.

#### A cyberwar would escalate to full-blown conflict

**Lindsey 19**

Nicole Lindsey, 10-14-2019, "Cyber War Between Iran and United States Could Have Far-Reaching Implications," CPO Magazine, https://www.cpomagazine.com/cyber-security/cyber-war-between-iran-and-united-states-could-have-far-reaching-implications/

Will cyber war lead to kinetic conflict? The biggest concern, of course, is that **cyber war will** eventually **lead to a shooting war**. We may already be seeing signs of this in the Middle East. Military attacks against drones, shipping vessels and oil facilities are tantamount to a declaration of war, so it’s not out of the question that the U.S. will respond in kind.Add in the fact that **the U.S. Cyber Command has transitioned from cyber defense to a more aggressive cyber posture, thanks to a new strategic philosophy known as “persistent engagement,”** and you can begin to grasp the enormity of the situation. Growing possibility that the tensions between Iran and the U.S. will lead to the militarization of cyberspace. It might be possible in today’s modern warfare arena to carry out missile strikes with lethal precision, but that still is not possible **with** today’s cyber weapons. If the world doesn’t want to wait around for a catastrophic event (such as a cyber Hiroshima) to take place involving **the digital equivalent of nuclear weapons**, then it’s now time to implement international norms and rules of engagement for reducing the risk of a cyber war becoming a full-fledged kinetic conflict with unimaginable loss of life.

### Link - NC3

**The second is attacks on Nuclear Infrastructure**

**First with a definition: NC3 systems are Nuclear Command, Control, and Communication processes.**

#### NC3 systems are dangerously vulnerable to cyberattacks that undermine 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

Cybersecurity of our nuclear systems needs to be a top priority. Many jokes have been made about who actually invented the internet, most notably after former Vice President Al Gore publicly declared he took the initiative to create it during his time in Congress. But credit — for the impetus, at least — for creation of the internet goes to the former Soviet Union (USSR). On October 4, 1957 the USSR launched Sputnik, the first artificial satellite. Then-Senate Majority Leader Lyndon B. Johnson remarked “Now, somehow, in some way, the sky seemed almost alien.” He remembered “the profound shock of realizing that it might be possible for another nation to achieve technological superiority over this great country of ours.” In February of 1958, the Advanced Research Projects Agency (ARPA) was born. According to the history of ARPA, the first three primary research priorities focused on space technology (to counter Sputnik), ballistic missile defense (to counter the USSR) and solid propellants (to eventually power the Minuteman ICBM). As ARPA grew, so did the threats they were being asked to counter. In the 1960s, telephone systems were copper wire and circuit-based. This made our primary means of communication vulnerable to a single missile strike by the USSR. What was needed was a “galactic network” of computers that would continue to function even if the Soviets devastated our telephone system. Twelve years after the launch of Sputnik, ARPAnet went live. On October 29, 1969 researchers at four universities delivered the first node-to-node communication. UCLA, Stanford, UC Santa Barbara and the University of Utah became the vanguard for what would become the modern internet. That invention is now coming back to threaten the very thing it was designed to counter; the threat of nuclear weapons. The Nuclear Posture Review (NPR) is a “legislatively-mandated review that establishes U.S. nuclear policy, strategy, capabilities and force posture for the next five to ten years.” The first NPR took place in 1994. In 2010, the NPR referred to ‘cyber’ once as the report only discussed the need to “protect its assets in cyberspace and outer space and enhanced by U.S. capabilities to deny adversaries’ objectives through resilient infrastructure (including command and control systems), global basing and posture, and ballistic missile defense and counter-WMD capabilities.” Fast forward to the 2018 Nuclear Posture Review and ‘cyber’ is mentioned sixteen times. This reflects the changing nature of our most critical systems, and the still-lacking protections our aging systems are dealing with. The most critical system is our Nuclear Command, Control and Communications (NC3). According the 2018 NPR, “The United States must have an NC3 system that provides control of U.S. nuclear forces at all times, even under the enormous stress of a nuclear attack. NC3 capabilities must assure the integrity of transmitted information and possess the resiliency and survivability necessary to reliably overcome the effects of nuclear attack.” What is most telling is what the report lists as the first initiative to ensure “our NC3 system remains survivable and effective. That initiative is “strengthening protection against cyber threats.” Since the 2010 NPR, the threats globally have worsened and include “an unprecedented range and mix of threats, including major conventional, chemical, biological, nuclear, space, and cyber threats, and violent non-state actors.” There is no doubt that Russia and China continue to be our biggest nuclear threats from a state-actor perspective. 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 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.

#### **The resulting muddled deterrence drastically increases probability of miscalc**

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 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.

## Impact

#### War with Iran spurs a global nuclear war 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 nuclear weapons would be used, either intentionally, or by accident or miscalculation.** Recent research has shown that **besides making large areas of the world uninhabitable** through 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 Preset (Lay Judge Speed)

# Frontlines

## FL: Framing

### AT: Policy Paralysis

### AT: Probability Important

#### Probability first framing falls prey to psychological biases that neglect disaster which lead to mass death.

Clarke 8 [Lee, member of a National Academy of Science committee that considered decision-making models, Anschutz Distinguished Scholar at Princeton University, Fellow of AAAS, Professor Sociology (Rutgers), Ph.D. (SUNY), “Possibilistic Thinking: A New Conceptual Tool for Thinking about Extreme Events,” Fall, Social Research 75.3, JSTOR]

In scholarly work, the subfield of disasters is often seen as narrow. One reason for this is that a lot of scholarship on disasters is practically oriented, for obvious reasons, and the social sciences have a deep-seated suspicion of practical work. This is especially true in sociology. Tierney (2007b) has treated this topic at length, so there is no reason to repeat the point here. There is another, somewhat unappreciated reason that work on disaster is seen as narrow, a reason that holds some irony for the main thrust of my argument here: **disasters are unusual and the social sciences are** generally biased **toward** **phenomena** **that are frequent**. Methods textbooks caution against using case stud- ies as representative of anything, and articles in mainstreams journals that are not based on probability samples must issue similar obligatory caveats. The premise, itself narrow, is that the only way to be certain that we know something about the social world, and the only way to control for subjective influences in data acquisition, is to follow the tenets of probabilistic sampling. This view is a correlate of the central way of defining rational action and rational policy in academic work of all varieties and also in much practical work, which is to say in terms of probabilities. **The irony is** that **probabilistic thinking** has its own biases, **which**, if unacknowledged and uncorrected for, lead to a conceptual neglect **of extreme events**. This leaves us, as scholars, paying attention to disasters only when they happen and doing that makes the accumulation of good ideas about disaster vulnerable to issue-attention cycles (Birkland, 2007). These conceptual blinders lead to a neglect of disasters as "strategic research sites" (Merton, 1987), which results in learning less about disaster than we could and in missing opportunities to use disaster to learn about society (cf. Sorokin, 1942**).** We need new conceptual tools **because of an upward trend in frequency and severity of disaster** since 1970 (Perrow, 2007), and because of a growing intellectual attention to the idea of worst cases (Clarke, 2006b; Clarke, in press). For instance, the chief scientist in charge of studying earthquakes for the US Geological Service, Lucile Jones, has worked on the combination of events that could happen in California that would constitute a "give up scenario": a very long-shaking earthquake in southern California just when the Santa Anna winds are making everything dry and likely to burn. In such conditions, meaningful response to the fires would be impossible and recovery would take an extraordinarily long time. There are other similar pockets of scholarly interest in extreme events, some spurred by September 11 and many catalyzed by Katrina. The **consequences** of disasters **are** also **becoming** **more severe**, both in terms of lives lost **and** property damaged. **People** and their places **are** **becoming more vulnerable**. The most important reason that vulnerabilities are increasing is population concentration (Clarke, 2006b). This is a general phenomenon and includes, for example, flying in jumbo jets, working in tall buildings, and attending events in large capacity sports arenas. Considering disasters whose origin is a natural hazard, the specific cause of increased vulnerability is that people are moving to where hazards originate, and most especially to where the water is. In some places, this makes them vulnerable to hurricanes that can create devastating storm surges; in others it makes them vulnerable to earthquakes that can create tsunamis. In any case, the general problem is that people concentrate themselves in dangerous places, so when the hazard comes disasters are intensified. More than one-half of Florida's population lives within 20 miles of the sea. Additionally, Florida's population grows every year, along with increasing development along the coasts. The risk of exposure to a devastating hurricane is obviously high in Florida. No one should be surprised if during the next hurricane season Florida becomes the scene of great tragedy. The demographic pressures and attendant development are wide- spread. People are concentrating along the coasts of the United States, and, like Florida, this puts people at risk of water-related hazards. Or consider the Pacific Rim, the coastline down the west coasts of North and South America, south to Oceania, and then up the eastern coast- line of Asia. There the hazards are particularly threatening. Maps of population concentration around the Pacific Rim should be seen as target maps, because along those shorelines are some of the most active tectonic plates in the world. The 2004 Indonesian earthquake and tsunami, which killed at least 250,000 people, demonstrated the kind of damage that issues from the movement of tectonic plates. (Few in the United States recognize that there is a subduction zone just off the coast of Oregon and Washington that is quite similar to the one in Indonesia.) Additionally, volcanoes reside atop the meeting of tectonic plates; the typhoons that originate in the Pacific Ocean generate furiously fatal winds. Perrow (2007) has generalized the point about concentration, arguing not only that we increase vulnerabilities by increasing the breadth and depth of exposure to hazards but also by concentrating industrial facilities with catastrophic potential. Some of Perrow's most important examples concern chemical production facilities. These are facilities that bring together in a single place multiple stages of production used in the production of toxic substances. Key to Perrow's argument is that there is no technically necessary reason for such concentration, although there may be good economic reasons for it. The general point is that we can expect more disasters, whether their origins are "natural" or "technological." We can also expect more death and destruction from them. I predict we will continue to be poorly prepared to deal with disaster. People around the world were appalled with the incompetence of America's leaders and orga- nizations in the wake of Hurricanes Katrina and Rita.

## FL: Escalation

### AT: Cyber-Military tradeoff

**(SPECIFIC TO IRAN)**

#### Trump has always been hesitant to deploying military operations in the middle east. Anecdotes do not prove general trends

**Lippman 19**

Daniel Lippman & Nahal Toosi, 9-17-2019, "Trump leans against striking Iran," POLITICO, <https://www.politico.com/story/2019/09/17/trump-iran-strike-1500742>

**Trump is reluctant to take military action in the Middle East because he wants to live up to his campaign vows to reduce foreign entanglements**, according to multiple people who speak with him regularly. He’s also worried about the economic and political ramifications of embroiling the United States in a war with Iran, which stands accused of the recent attack on oil facilities in Saudi Arabia. The president has hinted publicly at those concerns in recent days, saying on Monday afternoon, “Do I want war? I don’t want war with anybody. I’m somebody that would like not to have war,” while also warning, “We’re prepared more than anybody.”

**(GENERAL)**

**Cyber eventually escalates into general conflict so they actually link**

## FL: NC3

## FL: Nuclear War

### AT: Alt Causes

**Deterrence exists in the squo to prevent nuclear war. After all, mutually assured destruction is proven 100% effective in containing any nuclear conflict. HOWEVER, deterrence is undermined when second strike capability can be digitally disabled. THIS asymmetry in nuclear capacity creates massive risk for nuclear conflict.**

### AT: Miscalc Never Happened

#### Miscalc does cause conflict despite nations wanting peace. Look to historical precedent

**Tay 19**

Shirley Tay, 5-16-2019, “There is a ‘real’ risk of miscalculation in US-Iran tensions, expert says,” CNBC, <https://www.cnbc.com/2019/05/16/there-is-a-real-risk-of-miscalculation-in-us-iran-tensions-expert.html>

**As U.S.-Iran tensions continue to escalate**, there is rising fear among experts and government officials that a **conflict** between the two countries **may break out**. According to Henry Rome, a global macro and Iran analyst at political risk consultancy Eurasia Group, the risk of miscalculation by Washington and Tehran is “real.” “**If the U.S. and Iran were to end up in conflict in the near future, it will be because of a miscalculation or a misperception**,” he told CNBC. While President Donald Trump and Iran’s Supreme Leader Ali Khamenei have both said they are not interested in war, Rome said Thursday that “**history has shown us that** many, **many times** **that even two states — uninterested in armed confrontation — can be drawn into it based on accidents, misperceptions or other provocations**.” The Trump administration has deployed a carrier strike group and bombers to the Middle East region in response to what it calls “troubling and escalatory indications and warnings” from Iran. Despite rising fears of how misunderstandings between the two countries could escalate into a full-blown conflict, U.S. Secretary of State Mike Pompeo told CNBC on Saturday that the U.S. is “not going to miscalculate.” “Our aim is not war, our aim is a change in the behavior of the Iranian leadership,” he said. GP: Iran's President Hassan Rouhani 190516 Hassan Rouhani, Iran’s president, looks on during a news conference in Tehran, Iran, on February 6, 2018. On Wednesday, the U.S. State Department announced that all non-emergency American staff on diplomatic missions will be pulled out of Iraq, citing concerns of threats from Iranian-backed forces. Washington’s decision, however, runs counter to remarks from a senior British military official on Tuesday— who said there has been “no increased threat from Iranian-backed forces in Iraq or Syria.” “The U.S. is having a credibility problem here in trying to convince its allies of the threats faced by Iran, largely because of its track record and the individuals leading it, namely (U.S. National Security Advisor) John Bolton,” Rome said. Still, Rome said the “vague” U.S. intelligence and lack of public confirmation of Iranian threats in Iraq doesn’t mean that “we should reflexively reject these threats.”