# NOVDEC 1NC – Intel/Defense

WE NEGATE

Resolved: The benefits of the United States federal government’s use of offensive cyber operations outweigh the harms.

## Contention One is Losing Key Intelligence.

**Uren** of the Australian Strategic Policy Institute finds in **2019** that offensive cyber operations are operations that manipulate, disrupt, and destroy targeted computers or networks. He continues that by definition, offensive cyber operations are distinct from cyber espionage which is designed to gather information without having an effect. **Groll** of Foreign Policy furthers in **2019** that breaking into digital systems can provide key intelligence, but when one moves from surveilling a system to destroying it through offensive cyber operations, that access is lost. For every offensive cyber operation that the United States launches, we have less access to intelligence networks and fewer targets to hit in cyberspace.

Empirically this is true as **Slayton** from the Harvard Kennedy School explains in **2017** that the US Stuxnet cyberattacks on Iran’s nuclear enrichment facilities were entirely ineffective and, in the process, we lost a critical source of intelligence on their nuclear program.

Poor intelligence can be devastating as it can push us into war. Empirically, **Taylor** explains in **2013** that the cause of the **IRAQ WAR** was intelligence failure and speculation.

Problematically, **Dilanian** of NBC writes in **2019** that the US military has drastically increased offensive cyber operations on **IRAN** under the Trump administration. The resultant intelligence loss has the potential to be devastating as **Weichart** of The American Spectator writes in **2019** that poor intelligence has increased the risk of grave miscalculation with Iran. For this reason, **Tay** explains in **2019** that US-Iran tensions are escalating fast causing many experts to fear that a conflict could break out. If the US and Iran were to end up in a conflict it will be because of miscalculation due to lack of information.

## Contention Two is Protecting Our Grids.

**Johnson** of Entrepreneur explains in **2018** that artificial intelligence or AI will enable cyberattacks to reach an unprecedented new scale that could wreak untold damage on companies and critical systems. **Browne** of CNBC furthers in **2019** that AI will bring with it a dawn of new forms of cyber breaches that bypass traditional means of countering attacks.

Crucially, a US focus on offensive cyber operations drains resources for cybersecurity. **Healey** of US News highlights in **2013** that the US obsession with offensive cyber capabilities has reduced resources that should be dedicated for defense. **Wolff** continues in **2019** that the Trump administration’s switch to an offensive approach is detracting resources from defense while encouraging the government to act recklessly. **Donnelly** of Roll Call furthers in **2019** that without effective cyber defenses, more aggressive overseas operations could come back to bite the US. Defense is a necessary foundation for offense.

Importantly, a strategy that focuses on cyber defense can help solve critical vulnerabilities. **McGraw** furthers in **2013** that cyberwar and cybercrime share the same root cause: insecure computer systems. Building systems properly from a security perspective will effectively address and deter threats in cyberspace.

The impact is preventing attacks on critical infrastructure.

Not proliferating in terms of cyber defense will be catastrophic as it risks critical US energy infrastructure. **Ankura** continues in **2019** that more than 75% of energy companies had suffered at least one cyberattack in the last year alone. This is problematic, because with AI these cyberattacks will reach a new scale

The **SANS Institute** presents one possible scenario. A utility company which specializes in electrical distribution that serves critical businesses could be disrupted by cyber terrorists. The cyber terrorists could interrupt the distribution of electricity causing widespread blackouts. Unfortunately, blackouts do more than just turn off the lights.

First, they do economic damage.

Economist **Scott Borg** noted that if an attacker managed to knockout power to a third of the United States for a period of three months, the economic cost would be upwards of 700 billion dollars which is the economic equivalent of 40 to 50 large hurricanes hitting at the same time. This type of attack would be economically devastating and would have significant long-term consequences throwing millions into poverty for years to come.

Second, they cause radiation leakage.

**Heyes** reveals in **2017** how unstable the country’s nuclear power plants could become were something to happen to the power grid that provides them with the electricity they need to safely operate. This is why **Straub** of North Dakota States finds that a cyberattack could lead to a death toll that rivals that of a nuclear weapon.

And, to prevent a return to the dark ages, we negate.

# CARDS

## C1 Lost Intel

#### Uren ’18

Tom Uren, Bart Hogeveen, & Fergus Hanson, Australian Strategic Policy Institute, 4 July 2018, <https://www.aspi.org.au/report/defining-offensive-cyber-capabilities>

There is considerable concern about state-sponsored offensive cyber operations, which this paper defines as operations to manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks.

There are relatively few publicly available offensive cyber doctrine documents, but observed behaviour indicates that states such as Iran, North Korea and Russia are using operations that cause denial and manipulation effects to support broader strategic or military objectives. By definition, offensive cyber operations are distinct from cyber-enabled espionage, in which the goal is to gather information without having an effect. When information gathering is a primary objective, stealth is needed to avoid detection in order to maintain persistent access that allows longer term intelligence gathering.

#### Groll ’19

Groll, Elias. September 27 2019. “The U.S.-Iran Standoff Is Militarizing Cyber Spce.” Foreign Policy. https://foreignpolicy.com/2019/09/27/the-u-s-iran-standoff-is-militarizing-cyberspace/

But for every cyberattack that the United States launches, it must also make hard choices about the intelligence value of such a move. Attacking digital systems typically requires breaking into them ahead of time, which can provide key intelligence. When one moves from surveilling a system to destroying it, that access is lost. “You can’t attack something and stay in that network,” Williams said. And for every cyberattack that the United States launches, it will have less access to networks and fewer targets to hit in cyberspace. “It’s not like you’ve got a thousand cyber-cruise missiles.”

#### Doffman ’19

Zak Doffman, Forbes, 29 August 2019, <https://www.forbes.com/sites/zakdoffman/2019/08/29/secret-cyber-mission-devastated-irans-attack-capabilities-us-officials-say/#49b8234f5cb3>

According to U.S. officials, Iran is still trying to recover from the attack, with data lost and capability taken offline. In fact, an irony reported in the U.S. media and attributed to U.S. officials, is that the cost of the attack to the U.S. was lost access to the networks which were attacked, resulting in lost intelligence. As I've reported before, cyber warfare has reached a new phase this year—at least in terms of public awareness of the threat. The increased levels of integration between physical and cyber—an attack in one domain and retaliation in another.

#### Slayton ’17

Rebecca Slayton, Harvard Kennedy School – Belfer Center for Science and International Affairs, February 2017, <https://www.belfercenter.org/publication/why-cyber-operations-do-not-always-favor-offense>

Assessing kinetic effects. It is often more expensive for the offense to achieve kinetic effects—for instance, sabotaging machinery—than for the defense to prevent them. An empirical analysis of the Stuxnet cyberattacks on Iran’s nuclear enrichment facilities shows that Stuxnet likely cost the offense more than the defense and was relatively ineffective.

A cost-benefit analysis of Stuxnet for both the offense and the defense demonstrates why damaging physical infrastructure is more costly than simply infiltrating information networks. The costs of Stuxnet were likely far greater for the offense (the United States and Israel) than for the defense (Iran), and Stuxnet was relatively ineffective, setting back Iran’s nuclear program by fewer than three months. The great expense of Stuxnet was intelligence; though digital espionage can be used to obtain some kinds of information, the knowledge needed to disrupt a physical control system, such as the detailed methods and settings used to control pressure in Iran’s nuclear centrifuges, is not generally held in computers. The costs for both sides are dominated not by technology but by skilled labor—for example, hackers who identify and exploit zero-day vulnerabilities, systems administrators who manage and defend computer systems, and the nuclear engineers who understand enrichment processes and the means of disrupting them.

#### Dilanian ’19

Ken Dilanian, NBC News, 23 June 2019, <https://www.nbcnews.com/politics/national-security/under-trump-u-s-military-ramps-cyber-offensive-against-other-n1019281>

With little public scrutiny, the U.S. military has drastically stepped up its secret hacking of foreign computer networks in a new effort to keep China, Russia, [Iran](https://www.nbcnews.com/politics/national-security/iranian-backed-hackers-stole-data-major-u-s-government-contractor-n980986) and other adversaries on their heels, current and former U.S. officials tell NBC News. Empowered with new legal authority from both Congress and President Donald Trump, the military's elite cyber force has conducted more operations in the first two years of the Trump administration than it did in eight years under Obama, officials say — [including against Russia](https://www.nbcnews.com/news/world/russian-hackers-8-times-faster-chinese-iranians-north-koreans-says-n972926), despite Trump's well-documented affinity for Vladimir Putin. The general in charge of the push, Paul Nakasone, has spoken about the new policy in cryptic terms such as "persistent engagement," and "defending forward," without explaining what that means. Multiple current and former American officials briefed on the matter say military hackers are breaking into foreign networks, striking at enemy hackers and planting cyber bombs that would disable infrastructure in the event of a conflict.

#### Dugdale-Pointon ’07

Dugdale-Pointon, T. (22 August 2007), The Role of Intelligence in War, http://www.historyofwar.org/articles/concepts\_intelligence\_in\_war.html

Since war began the role of intelligence has been vital. Knowing where your enemy is, what he is doing, with what and what he is capable of, has always been a huge advantage. Intelligence can be classified into three main categories; Information relating to that particular local area or engagement, for example who exactly is guarding a particular bridge or strongpoint, is there a tank or other armored assets in the area, or the strength of a particular unit in the area. Strategic intelligence is of a yet bigger scale. This relates to a whole theatre of war or a country, its intentions and capabilities. In the modern era this may not just be related to military power but also economic power or intelligence relating to specific resources such as oil, minerals and even in the 21st century access to bio fuels. During the Cold War this was focused on the ability to make and the number of Nuclear weapons. One thing is certain - the role of intelligence gathering continues to be of utmost importance not only in wartime but in modern counterterrorism operations. The old problems of the validity of the information received remains, now coupled with the huge volume of data that can be received.

#### FAS ’96

February 23 1996. “The Need to Maintain an Intelligence Capability.” https://fas.org/irp/offdocs/int005.html

What the United States should maintain an intelligence capability after the Cold War is not a matter in serious dispute. The world of the 21st century is likely to be as fraught with peril and uncertainty as the world left behind. The United States finds itself in a predominant leadership role, whether sought or not, and the exercise of that leadership has become more complicated. New forces are at work and new dynamics at play. The Government must understand them in order to respond to them. Often the options available to it will depend upon how early problems are identified. Choosing the right option, in turn, will depend upon knowing what the consequences are apt to be. Once a course is chosen, it becomes important to know what the effects of the decision have been so that adjustments can be made if necessary. In every instance, making the right choice will hinge upon the quality of the information available. The volume of information openly available to the Government in the media and over computer networks has exploded in recent years, a trend which will continue. Yet intelligence capabilities will continue to be needed to collect information that is not available through conventional means. Once such information is obtained, analytical capabilities will be needed to combine it with the rapidly proliferating information available from other sources and seek to produce an objective assessment free of policy predilections. Where the process works, intelligence provides information and insights that are unique, reducing the uncertainty of decision making at all levels-from the President to the infantry platoon leader wondering what lies over the next hill. With it, there is a better chance of avoiding crisis or war, of success on the battlefield, of reaching and enforcing international agreements, of investing in the right military capabilities, and of protecting U.S. interests at home and abroad. As noted in the Introduction, there have been problems, especially at the CIA, some of which have been substantial. While these episodes are deplorable, using them to justify cutting back or eliminating intelligence capabilities is a leap the Commission is unwilling to make. Problems are, to some degree, unavoidable where intelligence activities are concerned, despite the best of intentions or management structures. Operations will, on occasion, be compromised despite reasonable precautions being taken. Mistakes will occur either as a result of poor judgment or individual incompetence. This is not to excuse or minimize such failures, or to suggest that every reasonable effort should not be made to prevent them, but only to recognize that problems to some extent are inevitable and, in the United States more so than in other countries, will continue to be highly publicized. The issue is whether the benefits justify the costs, including the problems which inevitably will occur. It is impossible to quantify the accomplishments of U.S. intelligence of which these are examples. Clearly, however, over the last five years conflicts have been avoided, wars shortened, agreements reached, costs reduced, and lives saved as a result of the information produced by U.S. intelligence. The United States had such information only because it chose to maintain a dedicated and capable intelligence apparatus. While that apparatus is expensive and will from time to time be a source of embarrassment, even consternation, the Commission has no difficulty reaching the conclusion that it is justified. Intelligence is an important element of national strength. The country should not lose sight of this amid the spy scandals and management failures of recent years. The performance of intelligence can be improved. It can be made more efficient. But it must be preserved.

#### Weichert ‘19

Brandon J Weichert, 23 May 2019, The American Spectator, <https://spectator.org/iran-more-failures-from-u-s-intelligence/>

In this land, the man who gives victory in battle is prized beyond every other man,” or so says Prince Feisal as portrayed by Sir Alec Guinness in the epic 1962 biopic, Lawrence of Arabia. Okay, so Feisal’s quote is apocryphal, and he was referring to the Arab-speaking peoples of the region. But the dog-eat-dog mindset that Feisal was referring to is as relevant to Persian thinking as it is to the Arabs. Lee Smith [referred](https://www.amazon.com/Strong-Horse-Power-Politics-Civilizations/dp/0767921801) to it as the “Strong Horse” principle. There was a time, not long ago, in fact, when the mere mention of the U.S. military caused Islamists of both the Sunni and Shiite worlds to tremble in fear. After 20 years of inconclusive combat, though, the idea of American military invincibility has been replaced by utter contempt in both the Arab and Persian minds. In other words, we’re a joke in that part of the world. What’s more, after multiple failed wars, we should quit while we’re behind (at least until we can figure out how best to win in the Sandbox without bleeding ourselves dry). Conflict Begets Fear, Begetting More Conflict Recently, it was [reported](https://www.haaretz.com/middle-east-news/iraq/as-u-s-iran-tension-simmers-rocket-fired-near-iraq-s-u-s-embassy-1.7256709) that a Katyusha rocket landed about a mile away from the U.S. embassy in Baghdad, Iraq. Iranian militants operating in a predominantly Shiite neighborhood in Baghdad are suspected… well, maybe. We don’t know. It’s likely we never will. But, the smartest people in Washington (don’t laugh) assume that it’s true. Meanwhile, single-source, unverified intelligence reports [indicate](https://www.reuters.com/article/us-usa-iran-flashpoints/irans-reach-puts-us-forces-allies-in-striking-range-idUSKCN1SR18G) that Iran was plotting to attack U.S. military outposts throughout the region and possibly [kidnap](https://www.usatoday.com/story/news/world/2019/05/17/gop-lawmaker-says-iran-threats-were-kill-and-kidnap-us-soldiers-michael-mccaul/3708808002/) American servicemen there. Iran also [attempted](https://www.youtube.com/watch?v=4Au_A_Y9RiE) an attack on two Saudi oil tankers operating in the Strait of Hormuz… or, that was the assumption, until it wasn’t. Not to worry, though, that bastion of truth, CNN, [reports](https://edition.cnn.com/2019/05/07/politics/us-iran-transporting-missiles/index.html) that U.S. intelligence detected Iranian ships being loaded with short-range ballistic missiles! Now, whether those ships were preparing to launch them at nearby U.S. forces or if they were merely transporting those missiles remains ambiguous. One would think our military-industrial-intelligence complex would want to know what the Iranian intentions were before spouting off and risking a wider war, but, that’s just not how Washington rolls. Bear in mind that launching short-range ballistic missiles from ships is a very tricky [undertaking](https://www.realcleardefense.com/articles/2019/05/13/missiles_on_ships_making_sense_of_irans_moves_in_the_gulf_114416.html) — one that the Iranians have never appeared capable of actually doing (and the undertaking is very inefficient). So, it is probable — though unconfirmed like everything else about the recent “news” about Iran — that Iran was merely transporting those missiles to another location in the region. Fears abounded among America’s policy community that Iran was preparing to move those missiles in range near U.S. forces operating in Saudi Arabia, Yemen, Iraq, or Syria. Maybe. Then again, we don’t know! Can We Cut Through the Fog of War First? The bottom line here is that the fog of war is setting in. Despite the fact that the United States has been at war basically since 1945, first against the Communists, and then against the Islamists — and that the U.S. government is [spending](https://www.dni.gov/index.php/what-we-do/ic-budget) more than $80 billion on its 17 intelligence services for FY2019 — we are somehow less informed about what’s happening in a purported major threat, like Iran, than, say, weather patterns on Mars! The entire reason for having such a bloated military-industrial-intelligence complex is, in part, to reduce the fog of war. It’s also to prevent wasteful military excursions and international misunderstandings. More dangerously, as the summer months approach Washington, D.C., its denizens can expect war fever as well as humidity to envelop the Swamp. And, just as we act more aggressive than we really want to be at times in order to scare our rivals, the Iranians do the exact same thing to us. It’s possible all of these moves were intended to put us back on our heels. It’s also more than likely that the Iranian leaders are just as stupid as ours are, and seriously miscalculated the American response to their provocations. Fact is, no one knows anything about what’s occurring in Iran. It’s an intelligence blackhole and has been since the revolution swept the Ayatollah and his fanatical theocracy into power in 1979. Iraq was also an intelligence dead zone in the run-up to the disastrous 2003 invasion. Of course, that lack of intelligence didn’t stop the democratic globalists who run Washington from pushing us into a wasteful conflict. Unsurprisingly, many of the same policymakers who were intimately involved with the Iraq War are similarly engaged with the Trump Administration’s more aggressive Iran policy. Yet, as I [noted](https://spectator.org/so-you-want-to-invade-iran/) previously, these policymakers have failed to learn the critical lessons about the mistakes of the Iraq War. Is It Containment or Invasion? The objective, as I understood it, of the Trump Administration’s Mideast policy was to reduce the threat of Islamic extremism to the United States, balance against unwanted Russian influence in the region, and roll back the Iranians’ malign presence beyond their own borders. In the process of achieving these aims, the Trump Administration sought to rehabilitate America’s ailing relations with the Sunni Arab states — notably the Kingdom of Saudi Arabia — and Israel. In so doing, a new balance of power in the region between Israel and the Sunni Arab states, backstopped by the United States, would assiduously work to roll back unwanted Iranian influence and contain Iranian ambitions with minimal force — much as how the United States fought and won the Cold War. Now, however, it appears that we’re blundering our way into another Mideast war that will be just as unwinnable as the last ones we’ve fought. President Trump insists that he doesn’t want war with Iran, as though he’s some hostage in the Oval Office. He’s the president. If he doesn’t want war with Iran now, then we don’t have a war with them. It’s possible that he’s playing good cop to his national security adviser John Bolton’s bad cop, in the hopes of getting a great deal with Iran. We can only be so lucky. Given the presence of many former George W. Bush neocons in top tier positions in the Trump Administration, though, this prospect seems unlikely. And, given how poorly our intelligence services have performed in penetrating opaque regimes, grave strategic miscalculations will be made as the democratic globalists who populate the administration rush to war. Perhaps our strike on Iran will be limited to airstrikes or debilitating the oil-rich Kharg Island in order to further decimate Iran’s energy sector, as some have suggested. This is certainly a better option than a full-fledged invasion of Iran. However, this more limited military option fails to answer the critical question: How will Iran retaliate? When pressed by his overzealous military advisers to invade Cuba during the Cuban Missile Crisis in 1962, then-President John F. Kennedy demanded to know how the Soviets would respond. His military men could only answer that the Soviets would not retaliate, because retaliating would lead to the unthinkable: general nuclear war between the two Superpowers. Of course, Kennedy knew full well that Moscow would have to respond, which is why he resisted the military advice and focused on the less popular, though, ultimately, safer approach of negotiations. While Iran is not the Soviet Union, it still has the [capability](https://www.nytimes.com/2008/01/12/washington/12navy.html) to do considerable harm to American forces in the region and to complicate U.S. foreign policy in general. Intelligence Informs Policy, Not the Other Way Around Make no mistake: Iran is a threat. Yet, that threat is not so grave that we must invade another Mideast state. Containment, covert action, and relying on regional partners, such as Israel and the Sunni Arab states, to drive the policies against Iran is key. If the Israelis and Sunni Arabs are unwilling to make the ultimate sacrifice in war against Iran, why should we? It’s likely that Iran has a rudimentary nuclear weapons capability. Why have they not used it? What’s their plan? I suspect that they would use such weapons if their arsenal were more developed, but as it stands Iran’s leadership knows they cannot win in a war against the United States. Perhaps Washington should focus on massive increases in its intelligence collection operations in Iran to answer some of these questions rather than mindlessly burbling about military escalation against Iran — especially since the mere threat of American military action is no longer sufficient to cow Mideast enemies into submission.

#### Tay ‘19

Shirley Tay, CNBC News, 16 May 2019, <https://www.cnbc.com/2019/05/16/there-is-a-real-risk-of-miscalculation-in-us-iran-tensions-expert.html>

As [U.S.](https://www.cnbc.com/united-states/)-[Iran](https://www.cnbc.com/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](https://www.cnbc.com/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](https://www.cnbc.com/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](https://www.cnbc.com/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](https://www.cnbc.com/mike-pompeo/) told CNBC on Saturday that [the U.S. is “not going to miscalculate](https://www.cnbc.com/2019/05/12/iran-is-active-threat-but-we-are-willing-to-talk-says-pompeo.html).” “Our aim is not war, our aim is a change in the behavior of the Iranian leadership,” he said. 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](https://www.reuters.com/article/usa-iran-military-assessment/no-increased-threat-from-iran-backed-militia-in-iraq-syria-british-general-idUSL2N22Q0QG) 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.”

#### Taylor ’13

Peter Taylor, 18 March 2013, <https://www.telegraph.co.uk/news/worldnews/middleeast/iraq/9937516/Iraq-war-the-greatest-intelligence-failure-in-living-memory.html>

Ten years on from the invasion, Iraq remains the most divisive war in recent history and the greatest intelligence failure in living memory. Much of the key intelligence that was used to justify the war was based on fabrication, wishful thinking and lies - and as subsequent investigations showed, it was dramatically wrong. Saddam Hussein had no weapons of mass destruction (WMD).

## C2 Cyber Defense

#### Donnelly ’19

John M Donnelly, Roll Call, 11 July 2019, <https://www.rollcall.com/news/u-s-is-woefully-unprepared-for-cyber-warfare>

Information operations and cyberattacks in the gray zone have grown in recent years — in number, sophistication and damage. China’s 2018 attack on a Navy contractor gave that country access not just to details of a key new anti-ship missile but also to much of what the Navy knows about China’s maritime capabilities. China has also reportedly stolen data on F-35 fighters, littoral combat ships, anti-missile systems and drones operated by the U.S. military. The broader U.S. economy has lost more than $1 trillion in intellectual property pilfered in cyberspace, experts say. Russia has specialized in a massive information warfare campaign to influence U.S. elections by sowing dissent and planting lies in U.S. social media circles. North Korea, Iran and even terrorist groups have shown they, too, can do damage with a few keystrokes. On June 11, national security adviser John Bolton publicly stated that the U.S. has stepped up its offensive cyber-assaults since last year. The message to America’s adversaries, Bolton said, is “You will pay a price.” Four days later, The New York Times reported that the United States, in a classified operation, had penetrated Russia’s energy grid with malware that, if triggered, could disrupt Russia’s electrical systems. The Pentagon has said the Times reporting was inaccurate but has not provided any clarification. Later that month, Yahoo News disclosed that U.S. Cyber Command had hit Iranian military computers after Iran shot down a U.S. drone in the Persian Gulf. Despite this ramped-up offense, America’s defenses lag behind, according to retired Army Gen. Keith Alexander, who headed the National Security Agency and the U.S. Cyber Command. “I think we are making gradual moves toward that, but I think there needs to be more,” said Alexander, now CEO of cybersecurity firm IronNet. “I believe it’s the government’s responsibility under the Constitution for common defense. Period.” Without effective cyber-defenses, more aggressive overseas operations could come back to bite the United States, experts warn. “Defense is a necessary foundation for offense,” the Defense Science Board, a Pentagon advisory panel, said in a 2018 report. “Effective offensive cyber capability depends on defensive assurance and resilience of key military and homeland systems.” Defenseless defense The Navy cybersecurity review, made public in March, said those defenses are severely lacking. As the Navy prepares to win “some future kinetic battle,” the report said, it is “losing” the current one. Defense contractors “hemorrhage critical data.” The current situation is the result of a “national miscalculation” about the extent to which the cyber war is upon us, and the vaunted U.S. military’s systems have been “compromised to such [an] extent that their reliability is questionable.” The U.S. economy, too, will soon lose its status as the world’s strongest if trends do not change, the authors wrote. The Defense Science Board, meanwhile, has delivered a similar message, recommending in 2017 that a second U.S. military that is truly cyber-secure be created as soon as possible, because the one America has will not necessarily work. A cyberattack on the military, the science board said, “might result in U.S. guns, missiles, and bombs failing to fire or detonate or being directed against our own troops; or food, water, ammo, and fuel not arriving when or where needed; or the loss of position/navigation ability or other critical warfighter enablers.” The report chillingly warned that doubts about U.S. defense capabilities due to cyber vulnerabilities could cause a president to more quickly turn to nuclear weapons in a conflict. Kenneth Rapuano, the Pentagon assistant secretary for homeland defense and global security, said the department is trying to implement “as a matter of top priority” the Defense Science Board recommendation to ensure that at least part of the military is at the highest level of cyber preparedness, starting with nuclear weapons.

#### Browne ’19

Ryan Browne, CNBC, 24 July 2018, <https://www.cnbc.com/2018/07/20/ai-cyberattacks-artificial-intelligence-threatens-cybersecurity.html>

The fear for many is that AI will bring with it a dawn of new forms of cyber breaches that bypass traditional means of countering attacks. “We’re still in the early days of the attackers using artificial intelligence themselves, but that day is going to come,” warns Nicole Eagan, CEO of cybersecurity firm Darktrace. “And I think once that switch is flipped on, there’s going to be no turning back, so we are very concerned about the use of AI by the attackers in many ways because they could try to use AI to blend into the background of these networks.”

#### Amaro & Gamble ’19

Silvia Amaro, Hadley Gamble, CNBC, 17 February 2018, <https://www.cnbc.com/2018/02/17/us-government-is-exceptionally-vulnerable-to-cyberattacks-security-expert-says.html>

The United States is “vulnerable” to cybersecurity attacks and need to step up their defense mechanisms, the co-founder of the computer security firm CrowdStrike told CNBC Saturday. Recent cyberattacks, including NotPetya last June, have been devastating to American companies, causing them hundreds of millions of dollars in losses. Other attacks, such as the cybersecurity breach at the Office of Personnel Management (OPM) in 2015, have reportedly given key information to governments like China’s that can be used to blackmail American citizens working with sensitive intelligence. As a result, it is urgent that U.S. authorities become better at protecting their networks, Dmitri Alperovitch, co-founder and chief technology officer at CrowdStrike told CNBC at the Munich Security Conference. “The U.S. government is actually exceptionally vulnerable,” he said. Despite the “very good” intelligence operations in the U.S., “their procurement process is so archaic that they are not actually able to buy the technologies they need to protect themselves fast enough,” Alperovitch said.

#### Zinutallin ’18

Leron Zinutallin, 10 December 2018, Tripwire, <https://www.tripwire.com/state-of-security/featured/artificial-intelligence-cybersecurity-attacking-defending/>

On the opposite side, there are many incentives to use AI when attempting to attack vulnerable systems belonging to others. These incentives include the speed of attack, low costs and difficulties attracting skilled staff in an already constrained environment. Current research in the public domain is limited to white hat hackers employing machine learning to identify vulnerabilities and suggest fixes. At the speed AI is developing, however, it won’t be long before we see attackers using these capabilities on a mass scale, if they don’t already. How do we know for sure? The fact is that it is quite hard to attribute a botnet or a [phishing campaign](https://www.tripwire.com/state-of-security/latest-security-news/phishing-campaign-stealing-money-data-industrial-companies/) to AI rather than a human. Industry practitioners, however, believe that we will see an AI-powered cyber-attack within a year; 62% percent of [surveyed Black Hat conference participants](https://maliciousaireport.com/) seem to be convinced in such a possibility. Many believe that AI is already being deployed for malicious purposes by highly motivated and sophisticated attackers. It’s not at all surprising given the fact that AI systems make an adversary’s job much easier. Why? Resource efficiency point aside, they introduce [psychological distance](https://ieeexplore.ieee.org/document/1337888) between an attacker and their victim. Indeed, many offensive techniques traditionally involved engaging with others and being present, which, in turn, limited attacker’s anonymity. AI increases the anonymity and distance. Autonomous weapons are the case in point; attackers are no longer required to pull the trigger and observe the impact of their actions.

#### Slayton ’17

Slayton, Rebecca. February 2017. Why Cyber Operations Do Not Always Favor the Offense. Belfer Center. Harvard Kennedy School. https://www.belfercenter.org/publication/why-cyber-operations-do-not-always-favor-offense

The assumption that cyberspace favors the offense is widespread among policymakers and analysts, many of whom use this assumption as an argument for prioritizing offensive cyber operations. Faith in offense dominance is understandable: breaches of information systems are common, ranging from everyday identity theft to well-publicized hacks on the Democratic National Committee. A focus on offense, however, increases international tensions and states’ readiness to launch a counter-offensive after a cyberattack, and it often heightens cyber vulnerabilities. Meanwhile, belief in cyber offense dominance is not based on a clear conception or empirical measurement of the offense-defense balance. Creating unnecessary vulnerabilities. Making offensive cyber operations a national priority can increase instabilities in international relations and worsen national vulnerabilities to attack. But because the skills needed for offense and defense are similar, military offensive readiness can be maintained by focusing on defensive operations that make the world safer, rather than on offensive operations. The skills and organizational capabilities for offense and defense are very similar. Defense requires understanding how to compromise computer systems; one of the best ways to protect computer systems is to engage in penetration testing (i.e., controlled offensive operations on one’s own systems). The similarity between offensive and defensive skills makes it unnecessary to conduct offensive operations against adversaries to maintain offensive capability. Thus, rather than stockpiling technologies in the hope of gaining offensive advantage, states should develop the skills and organizational capabilities required to innovate and maintain information and communications technologies.

#### Healey ’13

Jason Healey is director of the Cyber Statecraft Initiative at the Atlantic Council finds. <http://www.usnews.com/opinion/blogs/world-report/2013/03/08/clandestine-american-strategy-on-cyberwarfare-will-backfire>

America's generals and spymasters have decided they can secure a better future in cyberspace through, what else, covert warfare, preemptive attacks, and clandestine intelligence. Our rivals are indeed seeking to harm U.S. interests and it is perfectly within the president's purview to use these tools in response. Yet this is an unwise policy that will ultimately backfire. The undoubted, immediate national security advantages will be at the expense of America's longer-term goals in cyberspace. ¶ The latest headlines on covert and preemptive cyberplans highlight just the latest phase of a cyber "cult of offense" dating back to the 1990s. Unclassified details are scarce, but the Atlantic Council's study of cyber history reveals covert plans, apparently never acted upon, to drain the bank accounts of Slobodan Milosevic and Saddam Hussein. More recent press accounts detail cyber assaults on terrorist networks (including one that backfired onto U.S. servers) and Stuxnet, which destroyed Iranian centrifuges. American spy chiefs say U.S. cyber capabilities are so prolific that this is the "golden age" of espionage, apparently including the Flame and Duqu malware against Iran and Gauss, which sought financial information (perhaps also about Iran) in Lebanese computers.¶ Offensive cyber capabilities do belong in the U.S. military arsenal. But the continuing obsession with covert, preemptive, and clandestine offensive cyber capabilities not only reduces resources dedicated for defense but overtakes other priorities as well.

#### McGraw ‘13

[Gary McGraw](http://www.tandfonline.com/action/doSearch?action=runSearch&type=advanced&searchType=journal&result=true&prevSearch=%2Bauthorsfield%3A(McGraw%2C+G)), PhD is Chief Technology Ofﬁcer of Cigital, and author of¶ Software Security (AWL 2006) along with ten other software security¶ books. He also produces the monthly Silver Bullet Security Podcast for¶ IEEE Security & Privacy Magazine (syndicated by SearchSecurity), Cyber War is Inevitable (Unless We Build Security In), Journal of Strategic Studies - Volume 36, Issue 1, 2013, pages 109-119

**The conceptual conﬂation of cyber war, cyber espionage, and cyber**¶ **crime into a three-headed cyber Cerberus perpetuates fear, uncertainty**¶ **and doubt. This has made the already gaping policy vacuum on cyber**¶ **security more obvious than ever before.**¶ Of the three major cyber security concerns in the public eye, cyber¶ crime is far more pervasive than cyber war or espionage. And yet it is¶ the least commonly discussed among policymakers. Cyber crime is¶ already commonplace and is growing: 285 million digital records were¶ breached in 2008 and 2011 boasted the second-highest data loss total¶ since 2004.2¶ Though economic calculations vary widely and are difﬁcult to make,¶ cyber crime and data loss have been estimated to cost the global¶ economy at least $1.0 trillion dollars annually.3¶ Even if this estimate is¶ an order of magnitude too high, cyber crime is still an important problem that needs addressing. Just as consumers ﬂock to the Internet,¶ so do criminals. Why did Willie Sutton, the notorious Depression-era¶ gangster, rob banks? As he famously (and perhaps apocryphally) put it:¶ ‘That’s where the money is.’ Criminals ﬂock to the Internet for the same¶ reason.¶ Cyber espionage is another prominent problem that captivates the¶ imagination, and is much more common than cyber war. The highly¶ distributed, massively interconnected nature of modern information¶ systems makes keeping secrets difﬁcult. It is easier than ever before to¶ transfer, store and hide information, while more information than ever¶ before is stored and manipulated on networked machines. A pen drive¶ the size of a little ﬁnger can store more information than the super¶ computers of a decade ago. Cyber war, cyber espionage, and cyber crime all share the same root cause: our dependence on insecure networked computer systems. The¶ bad news about this dependency is that cyber war appears to be¶ dominating the conversation among policy-makers even though cyber¶ crime is the largest and most pervasive problem. **When pundits and**¶ **policymakers focus only on cyber war, threats emanating from**¶ **cyber crime and espionage are relegated to the background.** **Interestingly, building systems properly from a security perspective will address**¶ **the cyber crime and espionage problems just as effectively as it will**¶ **address cyber war.** **By building security into our systems in the ﬁrst**¶ **place we can lessen the possibility of cyber war, take a bite out of cyber**¶ **crime, and deter cyber espionage all at the same time.**

#### Wolff ’18

https://www.nytimes.com/2018/10/02/opinion/trumps-reckless-cybersecurity-strategy.html.

The idea of using offensive cyberattacks for defensive purposes is not a new one — discussions about the potential risks and rewards of “hacking back,” especially in the private sector, go back more than five years. But for the American government to embrace this strategy is a sharp change from the cautious, defense-oriented approach of the past decade. President Barack Obama was notably restrained in his authorization of offensive cyber missions. When deciding whether to use the Stuxnet worm to compromise uranium enrichment facilities in Iran in 2010 (his administration’s most famous use of offensive cyber capabilities), he reportedly expressed repeated concerns about the precedent it would set for other countries. The Obama administration’s forbearance and careful decision-making around cyberattack authorization aligns with the 2015 Department of Defense cyber strategy, which identified controlling the escalation of cyber conflicts as a key strategic goal. That goal is conspicuously absent from the Department of Defense’s new strategy.The Trump administration’s shift to an offensive approach is designed to escalate cyber conflicts, and that escalation could be dangerous. Not only will it detract resources and attention from the more pressing issues of defense and risk management, but it will also encourage the government to act recklessly in directing cyberattacks at targets before they can be certain of who those targets are and what they are doing.

#### Firdosi ’19

Ahad Firdosi, Medium, 3 January 2019, <https://medium.com/datadriveninvestor/cybersecurity-2019-artificial-intelligence-and-iot-devices-in-sight-6108b6ba5c27>

According to the report, cyber terrorists will exploit Artificial Intelligence (AI) systems and use their techniques to improve attacks. Automated systems powered by AI could probe networks and systems to search for undiscovered vulnerabilities that could be exploited. In turn, the AI ​​could be used to make more sophisticated some phishing attacks and social engineering, from the creation of much more realistic videos and audios or well-designed emails to deceive specific people. This highly credible resource will also easily allow the spread of fake news.

#### Johnson ’18

Larry Johnson, 21 Dec 2018, <https://www.entrepreneur.com/article/325142>

In the next few years, artificial intelligence, machine learning and advanced software processes will enable cyber attacks to reach an unprecedented new scale, wreaking untold damage on companies, critical systems and individuals. As dramatic as Atlanta’s March 2018 [cyber “hijacking” by ransomware](https://www.cnn.com/2018/03/27/us/atlanta-ransomware-computers/index.html) was, this was nothing compared to what is coming down the pike once ransomware and other malware can essentially "think" on their own. This is not a theoretical risk, either. It is already happening. Recent incidents involving Dunkin Donuts' DD Perks program, CheapAir and even the [security firm CyberReason's honeypot](https://www.securityweek.com/honeypot-shows-power-automation-hands-hackers) test showed just a few of the ways automated attacks are emerging “in the wild” and affecting businesses. (A honeypot experiment, according to [Wikipedia](https://en.wikipedia.org/wiki/Honeypot_%28computing%29), is a security mechanism designedto detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.) In November, three top antivirus companies also sounded similar alarms. [Malwarebytes](https://blog.malwarebytes.com/cybercrime/2018/11/malwarebytes-2019-security-predictions/), [Symantec](https://www.symantec.com/blogs/feature-stories/cyber-security-predictions-2019-and-beyond) and [McAfee](https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-labs-2019-threats-predictions/#extortion) all predicted that AI-based cyber attacks would emerge in 2019, and become more and more of a significant threat in the next few years. What this means is that we are on the verge of a new age in cybersecurity, where hackers will be able unleash formidable new attacks using self-directed software tools and processes. These automated attacks on their own will be able to find and breach even well-protected companies, and in vastly shorter time frames than can human hackers. Automated attacks will also reproduce, multiply and spread in order to massively elevate the damage potential of any single breach.

**Dixon ’19**, Dixon, William. June 19 2019. “3 ways AI will change the nature of cyber attakcs.” World Economic Forum. https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/

Not only will AI-driven attacks be much more tailored and consequently more effective, their ability to understand context means they will be even harder to detect. Traditional security controls will be impotent against this new threat, as they can only spot predictable, pre-modelled activity. AI is constantly evolving and will become ever-more resistant to the categorization of threats that remains fundamental to the modus operandi of legacy security approaches. The cybersecurity community is already heavily investing in this new future and is using AI solutions to rapidly detect and contain any emerging cyberthreats that have the potential to disrupt or compromise key data. Defensive AI is not merely a technological advantage in fighting cyberattacks, but a vital ally on this new battlefield. Rather than rely on security personnel to respond to incidents manually, organizations will instead use AI to fight back against a developing problem in the short term, while human teams will oversee the AI’s decision-making and perform remedial work that improves overall resilience in the long term. AI-powered attacks will outpace human response teams and outwit current legacy-based defenses; therefore, the mutually dependent partnership of human and AI will be the bedrock of defense strategies in the future. The battleground of the future is digital, and AI is the undisputed weapon of choice. There is no silver bullet to the generational challenge of cybersecurity, but one thing is clear: only AI can play AI at its own game. The technology is available, and the time to prepare is now.

**Wilson Center ’19**, April 4 2019. “AI raises the risk of cyberattacks – and the best defense is more AI.” World Economic Forum. https://www.weforum.org/agenda/2019/04/how-ai-raises-the-threat-of-cyberattack-and-why-the-best-defence-is-more-ai-5eb78ba081/

Artificial intelligence promises to accelerate the speed and success rate of cyber attacks by sophisticated actors and eventually by those less-skilled (if off-the-shelf tools are developed and made available). It will also further blur traditionally understood lines between cyber offence and defence. Whichever side better deploys these automated technologies fastest will hold an advantage. AI will bring about attacks for which a majority of the public and many private sector companies will not be prepared. The good news is that the cybersecurity industry is using the same methods for defence. But these services require sustained investment and incentives for evolving cybersecurity defences that do not yet exist at scale. In protecting networks against adversaries, humans will continue to be important players in defending their own networks. But, it is imperative that autonomous systems play a central role in any such strategy. Effectively using artificial intelligence for defensive purposes will require a hybridization of various tactics and tools of both a proactive and responsive nature. Policymakers must encourage analysis of best practices for employing such tools and consider setting standards for their use.

**Palmer ’16**, Palmer, Danny. December 14 2016. “ How AI-powered cyberattacks will make fighting hackers even harder.” https://www.zdnet.com/article/how-ai-powered-cyberattacks-will-make-fighting-hackers-even-harder/

Take phishing. It's the simplest method of cyberattack available -- and [there are schemes on the dark web which put all the tools required to go phishing into anyone's hands](https://www.zdnet.com/article/phishing-as-a-service-is-making-it-easier-than-ever-for-hackers-to-steal-data/). It's simply a case of taking an email address, scraping some publicly available personal data to make the phishing email seem convincing, then sending it to the victim and waiting for them to bite. That could become even more effective if AI is added. "Spear phishing is going to become really, really good when machine learning is incorporated into it on the attacking side," says Dave Palmer, director of technology at Darktrace, a cybersecurity firm which deploys machine learning in its technology. The machine learning algorithms don't even need to be very advanced; relatively simple sequence-to-sequence machine learning could be installed on an infected device in order to monitor emails and conversations of a compromised victim. After a period of monitoring, the AI could tailor phishing messages to mimic the message style of the victim to particular contacts in their address book, in order to convince them to click on a malicious link. "If I were emailing someone outside the company, I'd probably be polite and formal, but if I was emailing a close colleague, I'd be more jokey as I email them all the time. Maybe I'd sign off my emails to them in a certain way. That would all be easily replicated by machine learning and it's not hard to envision an email mimicking my style with a malicious attachment," Palmer explains.

#### SANS ‘03

https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154

The operations of a utility company which specializes in electrical distribution that serves critical businesses is disrupted by cyber terrorists. The cyber terrorists manage to interrupt the distribution of electricity to the customers. This will of course cause a huge problem to the affected entities or areas to carry on normal operations and the normal way of life.**, would be likely.**

#### Applegate 18 (Oct)

**https://ccdcoe.org/uploads/2018/10/10\_d2r1s4\_applegate.pdf**

Economist Scott Borg noted that if an attacker managed to knockout power to a third of the United States for a period of three months, the economy cost would be upwards of 700 billion dollars which is the economic equivalent of 40 to 50 large hurricanes hitting at the same time [5]. This type of attack would be economically devastating and would have significant long-term consequences. While it is unlikely that a state would engage in this type of large-scale attack outside the bounds of an openly declared war, it would also be short-sighted to assume that only states will have access to these types of attacks.

#### Heyes 17 (Apr)

**https://newstarget.com/2017-04-17-nuclear-power-plant-map-reveals-how-grid-down-scenario-would-obliterate-the-entire-east-coast-of-the-usa-except-maine.html**

A scientific group is sounding the alarm in a new interactive chart that **reveals how unstable the country’s nuclear power plants could become were something to happen to the power grid that provides them with the electricity they need to safely operate.** The Union of Concerned Scientists, [in its interactive database](https://www.ucsusa.org/nuclear-power/us-nuclear-power-plants-database#.WO_wAFLMwck), notes that the nation’s highest concentration of nuclear plants is along the U.S. east coast, which is also home to the highest concentration of Americans in the country. Areas around New York City, Philadelphia, Washington, D.C. and most of the southeast are at the greatest risk. **Should a grid-down scenario develop, and last for more than a few days, a hundred million Americans will be at risk of dying a horrible, radiation-filled death.** (RELATED: [28 Nuclear Reactors In The United States Could Suddenly Fail Due To Earthquakes… Most Are Located Along The East Coast](https://fukushimawatch.com/2017-04-11-28-nuclear-reactors-in-the-united-states-could-fail-due-to-earthquakes-most-are-located-along-the-east-coast.html)) Even before the Japan accident in March 2011, the U.S. Nuclear Regulatory Commission was concerned **that a protracted power outage could lead to radiation leaks as the loss of power to plants’ cooling tanks would lead to overheating and spillage of dangerous atomic elements.**

Pry ‘15, PhD, Executive Director of the Task Force on National and Homeland Security and Director of the U.S. Nuclear Strategy Forum (Peter, “TERRORISM–AN EXISTENTIAL THREAT”, [http://www.emptaskforcenhs.com/uncategorized/terrorism-an-existential-threat/)](http://www.emptaskforcenhs.com/uncategorized/terrorism-an-existential-threat/%29)

Terrorists do not need a nuclear missile to pose an existential threat to the United States, however. Technology has so evolved since World War II and the Cold War that the U.S. and the West have become an electronic civilization. Our prosperity and very lives depend upon a complex web of high-tech information, communications, financial, transportation, and industrial critical infrastructures, all supported by the keystone critical infrastructure–the electric power grid. Admiral Michael Rogers, Director of the National Security Agency and U.S. CYBERCOMMAND, in November 2014, warned that China and other actors could make a cyber attack that would blackout the U.S. national electric grid for 18 months, with catastrophic consequences for society. The Congressional EMP Commission warned that a nationwide blackout lasting one year could kill up to 9 of 10 Americans from starvation and societal collapse. Terrorists and hostile nations are probing U.S. cyber defenses every day and are working hard to develop the cyber equivalent of a nuclear warhead. Terrorists can also pose an existential threat to the United States by attacking its technological Achilles’ Heel the old fashioned way, using bullets and bombs. A study by the U.S. Federal Energy Regulatory Commission, the government agency responsible for grid security, warns that a terror attack that destroys just nine (9) key transformer substations, out of 2,000, could blackout the entire nation for over a year. Terrorists have learned that the electric grid is a major societal vulnerability. Terrorist attacks have already caused large-scale blackouts of 420,000 people in Mexico (October 2013), the entire nation of Yemen (by Al Qaeda in the Arabian Peninsula in June 2014), and 80 percent of the grid in Pakistan (January 2015)–this last a nuclear weapons state. And if terrorists steal a nuclear weapon from Pakistan, buy one from North Korea, or are given one by Iran, they could loft the warhead by balloon or missile to high-altitude over the U.S. to make the ultimate cyber attack–a nuclear electromagnetic pulse (EMP). EMP could blackout the national electric grid and other life sustaining critical infrastructures, perhaps permanently.

# F/L

### F/L Grids Are Decentralized and Resilient

1) This changes with A.I.

2) Even if the grids as a whole are resilient, a statistical analysis conducted by the Council of Foreign Relations found that an attacker would only have to take out 10 percent of generators to cause a widespread blackout that shuts down the grid.

Knake ’17, https://www.cfr.org/report/cyberattack-us-power-grid

The likelihood that an attack carried out by a determined and capable adversary would be thwarted by security measures is low. While some U.S. utilities might block attempts by an adversary to gain initial access or might be able to detect an adversary in their systems, many might not have the necessary tools in place to detect and respond. Efforts to improve data sharing that could enable detection by one company to block access across the entire industry are in their infancy. In the Lloyd’s scenario, only 10 percent of targeted generators needed to be taken down to cause a widespread blackout.

### Grids Resilient

1) Security by obscurity, meaning that trying to defend by just making it really confusing to attack our grid, no longer works. Walton explains in 2019 that the reason is because ICS technology which allows hackers to break into systems is rapidly evolving – it is both cheaper and more effective and their access into networks are becoming more common.

Walton ’19, Walton, Robert. Sep 27 2019. “Us electric grid more vulnerable to cyberattacks as DERs increase potential targets, GAO finds.” Utility Dive. https://www.utilitydive.com/news/us-electric-grid-more-vulnerable-to-cyberattacks-as-ders-increase-potential/563860/

"The challenge of cyber risk to distributed networks, be they transmission grids, smart grids, pipelines or other infrastructure is no doubt growing," Haward-Grau told Utility Dive. "No longer are we able to rely on the traditional modus operandi of isolated or air gapped networks or security by obscurity." Security by obscurity was historically an important way of protecting ICS infrastructure. The GAO report notes that early ICS "operated in isolation, running proprietary control protocols using specialized hardware and software." These systems were also often in physically secured areas, unconnected to broader networks. But ICS technology is rapidly evolving — being replaced by cheaper equipment and more standardized network protocols, thus making attacks easier. Enabling remote access to ICS is becoming more common, the report notes, but it is still a high hurdle for would-be attackers. "Cyberattacks on industrial control systems supporting grid operations may require a degree of sophistication and knowledge beyond what is needed to conduct cyberattacks on IT systems," the report says. "Industrial control systems often use operating systems and applications that may be considered unconventional to typical IT personnel." But the sheer volume of resources has grown the number of threats, and the report warns federal regulators may not be prepared. GAO makes three recommendations, two for FERC and one for the U.S. Department of Energy (DOE). According to the report, both agreed with the recommendation The U.S. Department of Homeland Security has been issuing growing numbers of ICS vulnerability advisories since 2010, according to GAO. The grid is becoming more vulnerable to cyberattacks— particularly those involving industrial control systems that support grid operations. (The figure below is a high-level depiction of ways in which an attacker could compromise industrial control systems.) The increasing adoption of high-wattage consumer Internet of Things devices—“smart” devices connected to the internet—and the use of the global positioning system to synchronize grid operations are also vulnerabilities.

## Offense Improves Defense

### More Info

**Unfortunately for them, OCOs lose actually cost us information. Remember what Groll from case tells you that for every cyber-attack that the United States launches, it will have less access to networks and fewer targets in cyberspace.**

Groll ’19

Groll, Elias. September 27 2019. “The U.S.-Iran Standoff Is Militarizing Cyber Spce.” Foreign Policy. https://foreignpolicy.com/2019/09/27/the-u-s-iran-standoff-is-militarizing-cyberspace/

But for every cyberattack that the United States launches, it must also make hard choices about the intelligence value of such a move. Attacking digital systems typically requires breaking into them ahead of time, which can provide key intelligence. When one moves from surveilling a system to destroying it, that access is lost. “You can’t attack something and stay in that network,” Williams said. And for every cyberattack that the United States launches, it will have less access to networks and fewer targets to hit in cyberspace. “It’s not like you’ve got a thousand cyber-cruise missiles.”

### Deterrence

**The problem with OCOs serving as deterrence in the specific instances we talk about is that the attackers are anonymous. As Zinutallin tells you in case, AI is allowing cyber terrorists to act anonymously alongside other infamous anonymous cyber groups. The threat does not come from Russia or China or another big entity that we can engage with and deter but rather small groups that are impossible to deter and thus the only way to shield against such attacks is good defense.**

Zinutallin ’18, Leron Zinutallin, 10 December 2018, Tripwire, <https://www.tripwire.com/state-of-security/featured/artificial-intelligence-cybersecurity-attacking-defending/>

On the opposite side, there are many incentives to use AI when attempting to attack vulnerable systems belonging to others. These incentives include the speed of attack, low costs and difficulties attracting skilled staff in an already constrained environment. Current research in the public domain is limited to white hat hackers employing machine learning to identify vulnerabilities and suggest fixes. At the speed AI is developing, however, it won’t be long before we see attackers using these capabilities on a mass scale, if they don’t already. How do we know for sure? The fact is that it is quite hard to attribute a botnet or a [phishing campaign](https://www.tripwire.com/state-of-security/latest-security-news/phishing-campaign-stealing-money-data-industrial-companies/) to AI rather than a human. Industry practitioners, however, believe that we will see an AI-powered cyber-attack within a year; 62% percent of [surveyed Black Hat conference participants](https://maliciousaireport.com/) seem to be convinced in such a possibility. Many believe that AI is already being deployed for malicious purposes by highly motivated and sophisticated attackers. It’s not at all surprising given the fact that AI systems make an adversary’s job much easier. Why? Resource efficiency point aside, they introduce [psychological distance](https://ieeexplore.ieee.org/document/1337888) between an attacker and their victim. Indeed, many offensive techniques traditionally involved engaging with others and being present, which, in turn, limited attacker’s anonymity. AI increases the anonymity and distance. Autonomous weapons are the case in point; attackers are no longer required to pull the trigger and observe the impact of their actions.

1) Deterrence still exists by conventional and economic means.

Clarke ’17, Richard A Clarke, Journal of International Affairs, Columbia, 1 June 2017, <https://jia.sipa.columbia.edu/risk-cyber-war-and-cyber-terrorism>

No, and cyber war is unique in this respect. We have to deter cyber attacks by threat of conventional or economic retaliation. It’s difficult to develop an effective cyber deterrent, because you have to have already demonstrated the capabilities of your retaliatory arsenal. Your assailants have to know what you’re capable of. This wasn’t a difficult thing to do in the Cold War, because you just had to detonate a few hydrogen bombs on some uninhabited island and everyone knew you had that weapon available to you. This is not really possible in cyber war for two reasons. First, every state’s network infrastructure is different and you can’t prove that an attack you carried out on Country A will also affect Country B. And second, there’s no cyber equivalent of that uninhabited island that you can annihilate just to prove to everyone else that you can.

# EXTRA

1) US Cybersecurity spending is sad boi hours

Tonar & Talton ’18, Remington Tonar & Ellis Talton, Forbes, 23 April 2018, <https://www.forbes.com/sites/ellistalton/2018/04/23/the-u-s-governments-lack-of-cybersecurity-expertise-threatens-our-infrastructure/#61e2685949e0>

Meanwhile, federal cybersecurity spending continues to lag, with some [estimates](https://www.fifthdomain.com/civilian/2017/09/01/how-much-does-federal-government-spend-on-cybersecurity/) suggesting it will reach a meager $22 billion by 2022. Demonstrating the low priority many federal agencies place on digital, the Department of Interior spent a paltry $209,000 on digital services in 2016, with very little of that going to cybersecurity. While many of Interior’s offices aren’t critical to most people's everyday lives, a creative hacker could definitely cause some havoc by altering, say, earthquake or volcano data housed at the U.S. Geological Survey. Fortunately, the Department of Homeland Security spent a little more — $1.7 million — on internal digital services that same year. Nevertheless, the universal under-investment in digital infrastructure security is a glaring vulnerability that must be addressed.