# NOVDEC NC

We negate

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

## Contention One is Proliferation.

The United States’ use of offensive cyber operations has aided 2 of our adversaries in acquiring nuclear weapons.

First is Iran.

**Blaustein** finds in **2013** that the United States’ cyberattack on Iranian nuclear facilities in 2010 known as Stuxnet was not only unsuccessful, but it improved Iran’s ability to make nuclear weapons by revealing vulnerabilities that they would not have discovered for years. This is why before the attack, Iran was enriching uranium to just 3.5 percent, and after the attack it began enriching uranium to 20 percent. This is problematic because **Tirone** finds in **2019** that 20% enrichment is enough to make weapons-grade material. Thus, US offensive cyber operations gave Iran the know-how it needed to bolster its nuclear force.

This is problematic as the **BBC** explains in September that now that the US has abandoned the Iran Deal and has imposed sanctions on Iran, they have begun advanced uranium enrichment to develop nuclear weapons.

Second is North Korea.

**Ranger** finds in **2018** that one issue with offensive cyber operations is that they can be analyzed and repurposed by the country or group it was used against. This is known as reverse-engineering.

**Zetter** continues in **2015** that North Korea has learned from US cyberattacks against foreign countries. **Parker** explains in **2019** that North Korea has reverse-engineered US cyber operations in order to develop their own cyber force and bolster their economy through cybertheft which is why **Nichols** finds in **2019** that through these cyberattacks, North Korea has generated $2 billion to continue its weapons of mass destruction program. This is problematic because **Vavra** of Axios found that in early 2018, North Korea had reportedly run out of funds for its nuclear program. Because of US offensive cyber operations, North Korea was able to acquire the funds necessary to continue nuclearization.

The impact is a potential nuclear war.
**Nichols** explains in **2015** that stability in nuclear deterrence depends on predictability. Because specifically countries like Iran and North Korea have unpredictable foreign policy and the US has few ways to communicate with them during a crisis or event of increased tensions, their possession of nuclear weapons becomes extremely dangerous.

## Contention Two is a Defensive Drain.

**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. 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 Proliferation

### Iran

#### Blaustein ’13

Michael Blaustein, 16 May 2013, New York Post, <https://nypost.com/2013/05/16/stuxnet-virus-might-have-improved-irans-nuclear-capabilities-report/>

When the Stuxnet computer virus attacked Iran’s nuclear enrichment facilities in 2010, it was widely acknowledged to be the most successful cyber attack of all time. Unfortunately, new research shows that the Stuxnet virus was not only unsuccessful, it might have actually improved Iran’s ability to make nuclear weapons, according to a new report The stunning claim comes from a report published in a [British academic journal](http://www.tandfonline.com/doi/pdf/10.1080/03071847.2013.787735) which claims that Stuxnet had no discernible effect on Iran’s ability to enrich uranium — which can be used as fuel in a nuclear weapon — and that it might have actually improved Iran’s nuclear capabilities by exposing vulnerabilities that the regime might not have found for years.

The increase implies that, at best, Stuxnet had no lasting effect on Iran, and at worst might have made the Iranians even savvier makers of nukes. Backing up Barzashak’s position is the fact that before the attack Iran was enriching uranium to 3.5 percent, and after the attack it began enriching uranium to 20 percent. For a bomb, Iran will need to enrich uranium to about 90 percent. “Uranium-enrichment capacity grew during the time that Stuxnet was said to have been destroying Iranian centrifuges,” Barzashak writes. “Iran produced more enriched uranium, more efficiently: the entire plant’s separative capacity per day increased. “The malware — if it did in fact infiltrate Natanz — has made the Iranians more cautious about protecting their nuclear facilities,” Barzashka writes. Furthermore, “Iran’s uranium-enrichment capacity increased and, consequently, so did its nuclear-weapons potential.” “Stuxnet was of net benefit to Iran if, indeed, its government wants to build a bomb or increase its nuclear-weapons potential,” Barzashka warns.

#### Tirone ’19

Bloomberg, 15 November 2019, Jonathan Tirone, <https://www.bloomberg.com/quicktake/irans-uranium-enrichment>

Under the [agreement](https://2009-2017.state.gov/documents/organization/245317.pdf), which was struck by Iran, the U.S., China, France, Russia, Germany, the U.K. and the European Union, Iran maintained the ability to enrich uranium for peaceful purposes. It was allowed to keep 5,000 [centrifuges](http://www.fas.org/programs/ssp/nukes/fuelcycle/centrifuges/centrifuge.html) to separate the [uranium-235](http://world-nuclear.org/information-library/nuclear-fuel-cycle/uranium-resources/the-cosmic-origins-of-uranium.aspx#.UlJlS1Cnr2Y) isotope needed to induce a fission chain reaction. Iran had agreed under the accord that for 15 years it would not refine the metal to more than 3.7% enrichment — the level needed to fuel nuclear power plants — and would limit its enriched-uranium stockpile to 300 kilograms, or 3% of the [amount it held in May 2015](https://www.iaea.org/sites/default/files/gov-2015-34.pdf). The [International Atomic Energy Agency](http://www.iaea.org/) verified that Iran eliminated its inventory of 20%-enriched uranium, which can be used to make medical isotopes and to power research reactors but could also be purified to weapons-grade material at [short notice](https://www.armscontrol.org/files/Iran_Brief_Breaking_Down_Irans_Breakout_Capacity.pdf). Inspectors also confirmed that Iran destroyed a reactor capable of producing plutonium.

#### BBC ’19

7 Sept 2019, <https://www.bbc.com/news/world-middle-east-49619246>

Iran says it has begun using new advanced centrifuges to enrich uranium - the latest step in reducing its commitment to a 2015 nuclear deal with world powers. Forty such centrifuges were now operational, said nuclear agency spokesman Behruz Kamalvandi. Enriched uranium can be used to make reactor fuel but also nuclear weapons. Iran stopped abiding by two commitments in July in response to sanctions the US reinstated when it abandoned the deal. President Donald Trump wants to force Iran to negotiate a new agreement that would place indefinite curbs on its nuclear programme and also halt its development of ballistic missiles. But Iran has so far refused.

### North Korea

#### Vavra ’18

Shannon Vavra, Axios, 26 January 2018, <https://www.axios.com/north-korea-running-out-of-money-report-1517000914-6548c7b1-777f-40fa-b9dc-da371a9e7b30.html>

Two Chinese officials with ties to top North Korean government officials told Radio Free Asia that Kim Jong-un’s regime is running low on funds for its nuclear program, [Fox News reports](http://www.foxnews.com/world/2018/01/26/kim-jong-uns-slush-fund-running-out-fuel-after-numerous-missile-nuclear-tests-report-says.html). Why it matters: The North is getting more and more isolated, according to this report. Some experts say when Kim Jong-un is isolated, he comes to the negotiating table to try to get sanctions eased — so this could explain the North’s recent talks with South Korea. But it’s also anyone’s best guess as to what Kim Jong-un wants exactly at any given time.

#### Zetter ’15

Kim Zetter, 10 February 2015, https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/

Regardless of whether Iran is behind the Shamoon attack, there's no question that it [Iran] and other nations learn from cyberattacks launched by the US and its allies. Common cybercriminals also study Stuxnet and the like to learn new techniques for evading detection and stealing data. The NSA document published by The Intercept noted that while there were no indications in 2013 that Iran planned to conduct a destructive attack against a US or UK target similar to Wiper, "we cannot rule out the possibility of such an attack, especially in the face of increased international pressure on the regime." Of course, a similar attack did strike the US. But instead of hitting the US oil industry or a similarly critical sector, it struck a Hollywood film studio. And instead of coming from Iran, it came this time (according to the White House and FBI) from North Korea. All of which suggests that when the US and Israeli strike their enemies, it isn't just that single adversary who learns from the attack.

#### Parker ’18

Mitchell Parker, CSO Online, 24 October 2018, <https://www.csoonline.com/article/3315745/defense-security-and-the-real-enemies.html>

When I was a kid, I used to read National Geographic magazines. They were 25 cents each at the local library. The August 1974 issue had an article in it titled “Rare Look at North Korea,” by H. Edward Kim, who visited North Korea (DPRK) and provided a detailed report. In that article, he spoke of how North Koreans figured out how to build their own tractors by reverse engineering one. They spoke about the tractor running backwards at first, but they eventually were able to build running tractors better than the presumably Soviet ones they took apart to learn how to build them. They have since applied their ingenuity to technology. They are guided by the Juche ideology authored by their first leader, Kim Il Sung, which is based on the tenets of independence, self-reliance, and self-defense. Under their second leader, Kim Jong Il, the Songun, or “military first” policy was added. Kim Jong Un, the third and current leader, has extended these with a focus on nuclear weapons development, empowering companies, and providing incentives for economic development called the “Socialist Corporate Responsible Management System.” Their system is focused on enriching their military, the DPRK and then their people, in that order. They have become an extremely adept force in technology, as Sony Pictures unfortunately learned, and have utilized their skills learned from reverse engineering our technology to bolster their economy. The recent thefts of $571 million in cryptocurrencies, [according to CCN](https://www.ccn.com/571-million-notorious-north-korean-hacker-group-has-stolen-a-fortune-in-cryptocurrency/), done on behalf of a country with a $28.5 billion GDP in 2016, shows that a significant portion of their income now comes from their technology skills.

#### Nichols ’19

Reuters, Michelle Nichols, 5 August 2019, <https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX>

North Korea has generated an estimated $2 billion for its weapons of mass destruction programs using “widespread and increasingly sophisticated” cyberattacks to steal from banks and cryptocurrency exchanges, according to a confidential U.N. report seen by Reuters on Monday. Pyongyang also “continued to enhance its nuclear and missile programmes although it did not conduct a nuclear test or ICBM (Intercontinental Ballistic Missile) launch,” said the report to the U.N. Security Council North Korea sanctions committee by independent experts monitoring compliance over the past six months. The North Korean mission to the United Nations did not respond to a request for comment on the report, which was submitted to the Security Council committee last week. The experts said North Korea “used cyberspace to launch increasingly sophisticated attacks to steal funds from financial institutions and cryptocurrency exchanges to generate income.” They also used cyberspace to launder the stolen money, the report said. “Democratic People’s Republic of Korea cyber actors, many operating under the direction of the Reconnaissance General Bureau, raise money for its WMD (weapons of mass destruction) programmes, with total proceeds to date estimated at up to two billion US dollars,” the report said. North Korea is formally known as the Democratic People’s Republic of Korea (DPRK). The Reconnaissance General Bureau is a top North Korean military intelligence agency.

### Impact

#### Nichols ’15

Tom Nichols, 16 May 2015, National Interest, <https://nationalinterest.org/feature/heres-what-makes-rogue-nuclear-states-really-dangerous-12899>

The stability of nuclear deterrence rests on a certain amount of predictability. Contrary to what most people believe or [have seen in movies](http://csis.org/blog/nuclear-weapons-mission-impossible-ghost-protocol), the President of the United States cannot simply go berserk and personally order a nuclear strike. Nor can Vladimir Putin, for all his talk, merely open a briefcase and rain down nuclear hell. Orders must be transmitted through civilian and military channels designed specifically to prevent such a moment. And here we return to North Korea and Iran. We have no idea who really has the authority or the ability to launch nuclear weapons. We can’t even be certain who has custody of the actual bombs. We might have assumed, for example, that the order to use nuclear arms would have to pass from North Korea’s boy-king, Kim Jong-un, to his minister of defense. Since the minister of defense is now scattered in pieces all over a stadium in North Korea, we have to rethink that notion. And who really runs Iran? In theory, the Islamic Republic has a “president,” but real power resides in a cabal of old mullahs. If Iran were to acquire nuclear weapons, who could say yes—or more important, no—to a nuclear strike? This will matter a great deal during a crisis. Whom do we watch for signs of impending attack? With whom do we communicate? The Kim family [has a capricious tendency to vanish during times of tension](http://www.brookings.edu/blogs/up-front/posts/2014/10/15-kim-jong-un-disappearing-reappearing-act-pollack); this is the exact opposite of how Americans approach foreign policy, where [the president’s visibility and engagement is a sign of reassurance both to allies and enemies](https://books.google.com/books?id=JYBQAQAAQBAJ&pg=PA123&lpg=PA123&dq=Able+Archer+President+did+not+participate+MacFarlane&source=bl&ots=YyOkbig0pm&sig=qGiWXf9g2GYowzzjOvuG0-cz17Y&hl=en&sa=X&ei=l3hTVfudOYmlNuOxgOgC&ved=0CDwQ6AEwBA#v=onepage&q=Able%20Archer%20President%20did%20not%20participate%20MacFarlane&f=false). Likewise, if we hear bellicose rhetoric from the Iranian mullahs but reassuring words from an Iranian president, whom do we believe? This is why it is so difficult to negotiate with rogue regimes, or to trust in their competence, if they are established nuclear powers. It’s bad enough that by their nature they seek to upend the international status quo; far worse is their own inability to define who makes vital decisions of war and peace. While we should resist preventive thinking, the opacity of these regimes during a crisis might make such a temptation overwhelming. If “who’s in charge?” becomes a pressing question, the preventive answer might be: “who cares?”

## C2 A.I. Revolution

#### Straub ’19

Jeremy Straub, LiveScience, North Dakota State University, 27 August 2019, <https://www.livescience.com/cyberattacks-could-kill-more-than-nuclear-attacks.html>

As someone who studies [cybersecurity](https://dl.acm.org/citation.cfm?id=2810109) and [information warfare](https://theconversation.com/artificial-intelligence-cyber-attacks-are-coming-but-what-does-that-mean-82035), I'm concerned that a cyberattack with widespread impact, an intrusion in one area [that spreads to others](https://i-hls.com/wp-content/uploads/2013/03/Critical-Infrastructure-Protection-against-Cyber-Threats-Lior.pdf) or a [combination](http://tedkoppellightsout.com/) of lots of smaller attacks, could cause significant damage, including mass injury and death rivaling the death toll of a nuclear weapon. Unlike a nuclear weapon, [which would vaporize people within 100 feet and kill almost everyone within a half-mile](https://nymag.com/intelligencer/2018/06/what-a-nuclear-attack-in-new-york-would-look-like.html), the death toll from most cyberattacks would be slower. People might die from a [lack of food, power or gas for heat](https://theconversation.com/space-weather-threatens-high-tech-life-92711) or from car crashes resulting from a [corrupted traffic light system](https://theconversation.com/connected-cars-can-lie-posing-a-new-threat-to-smart-cities-95339). This could happen over a wide area, resulting in mass injury and even deaths. This might sound alarmist, but look at what has been happening in recent years, in the U.S. and around the world. In early 2016, hackers [took control of a U.S. treatment plant](https://www.theregister.co.uk/2016/03/24/water_utility_hacked/) for drinking water, and [changed the chemical mixture](https://www.securityweek.com/attackers-alter-water-treatment-systems-utility-hack-report) used to purify the water. If changes had been made — and gone unnoticed — this could have led to poisonings, an unusable water supply and a lack of water. In 2016 and 2017, hackers shut down [major sections](https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/) of the [power grid in Ukraine](https://www.wired.com/story/crash-override-malware/). This attack was milder than it could have been, as no [equipment was destroyed during it](https://en.wikipedia.org/wiki/Aurora_Generator_Test), despite the ability to do so. Officials think it was [designed to send a message](https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/). In 2018, unknown cybercriminals gained access [throughout the United Kingdom's electricity system](https://unearthed.greenpeace.org/2018/06/11/dragonfly-uk-energy-hacker-cybersecurity/); in 2019 a similar incursion may have [penetrated the U.S. grid](https://www.eenews.net/stories/1060281821). In August 2017, a Saudi Arabian petrochemical plant was hit by [hackers who tried to blow up equipment](https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html) by taking control of the same types of electronics used in industrial facilities of all kinds throughout the world. Just a few months later, hackers shut down [monitoring systems for oil and gas pipelines](https://threatpost.com/insecure-scada-systems-blamed-in-rash-of-pipeline-data-network-attacks/130952/) across the U.S. This primarily caused logistical problems — but it showed how an insecure contractor's systems could potentially cause problems for primary ones. The FBI has even warned that [hackers are targeting nuclear facilities](https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html). A compromised nuclear facility could result in the [discharge of radioactive material](https://www.nytimes.com/2019/05/08/us/three-mile-island-shut-down.html), chemicals or even possibly a reactor meltdown. A cyberattack could cause an event similar to the [incident in Chernobyl](https://www.theatlantic.com/photo/2016/04/still-cleaning-up-30-years-after-the-chernobyl-disaster/476748/). That explosion, caused by inadvertent error, [resulted in](https://www.theatlantic.com/photo/2016/04/still-cleaning-up-30-years-after-the-chernobyl-disaster/476748/) 50 deaths and evacuation of 120,000 and has left parts of the region uninhabitable for thousands of years into the future.

#### Ankura ’19

8 April 2019, <https://ankura.com/insights/cyber-attacks-and-the-energy-sector/>

In a March 2017 article in the Houston Chronicle, the Department of Homeland Security reported that there were 59 cyber incidents at energy facilities last year. This is a nearly one-third increase from the previous year. In more than a quarter of the intrusions, the attack occurred due to spear-phishing emails, (which appear to be from an individual or business that the recipients know, but are not), that tricked employees into downloading infected attachments or clicking on malicious web links. More than 10 percent of attacks came from network probing and scanning. The article stated that the “increased number of intrusions into energy computer controls last year brings the number of such incidents in the industry to more than 400 since 2011.” That number is likely low because energy sector companies are not required to report incidents to the government. Cybersecurity researchers believe at least 3,000 attacks against computer controls at industrial facilities, including in the oil industry, occur each year.

A 2016 survey administered by the IT security firm Tripwire, of 150 IT professionals employed by companies in the energy sector, found that more than 75 percent of energy companies had suffered at least one attack in the previous 12 months. In each case, the cyberattackers breached a minimum of one firewall, antivirus software, or another safeguard.

#### 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.

#### 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.

#### 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.**

# FRONTLINES

### AT Deterrence Solves AI

1) Deterrence fails – AI allows actors to attack anonymously.

#### 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.

# EXTRA

**Firdosi** of Medium writes in **2019** that hackers will use AI systems in the future to improve attacks. **Zinutallin** furthers in **2018** that AI is highly attractive to malicious actors because it can ensure that the attackers are anonymous.