Cybersecurity
Andrew and Nicole Cornish
Texas
2019 Topic Selection Meeting

Table of Contents

Background

Cyber threats are not new to the United States, but the 2016 election escalated the exposure of cyber threats many times over.

> During the 2016 elections, Russian hackers unleashed a 'new form of political sabotage'[18]. Lines of code replaced the secret White House tapes of Watergate fame as Russian hackers passed stolen emails from the Democratic Party political operatives to WikiLeaks in an attempt to undermine the US election. At the same time, Russian information warfare operatives seeded social media networks with stories about racial unrest to propel an image of America in decline. According to the New York Times, it was 'the perfect weapon'; designed to undermine the American electoral institutions and, through them, confidence in the next elected government of the United States [18, 40].

While election meddling gets most of the headlines, it is just the tip of the iceberg when it comes to cybersecurity threats to the United States. The US has a long history of using cyber weapons, but it does not have a strong defense against cyber-attacks. Believed to have begun in 2005, the United States and Israel intelligence agencies cooperated to develop malware that targeted Iranian nuclear enrichment centrifuges, causing them to spin out of control. Accidentally made public in 2010, this program was dubbed "Stuxnet" and the operation, "Operation Olympic Games" [12].

The United States is skilled at attacking via cyberspace, but apparently does not even have the ability to prevent election meddling.

In addition, the recent scandals, including Facebook's Cambridge Analytica, and breaches like Marriott (500 million affected) and Yahoo (3 billion affected), have made cybersecurity one of the most important issues for American's. A 2018 survey by Harris Poll finds that "78 percent of U.S. consumers believe a company's ability to protect user data is 'extremely important' and only 20 percent now 'completely trust' organizations to protect their data… In one of the survey's more surprising revelations, it found 60 percent of consumers are more concerned about cybersecurity than they are of the U.S. going to war."[15].

The Cybersecurity Information and Sharing Act of 2015 is the only major legislative effort to combat cybersecurity threats in the United States, but it does not do enough to keep up with the threat level and even at the time of passage was controversial. Critics say it will allow the government to collect personal data without limits[32]. The bill is designed to foster information sharing with the government from the private sector. Since that bill passed and Donald Trump took office, there has been very little progress on cybersecurity. A bill was introduced in 2017 (The Internet of Things Cybersecurity Act of 2017) but not passed. The bill would have sought to improve the security of internet-connected devices[1].

Timeliness:

The 2016 election and subsequent Russia meddling investigation set the stage for a new focus on cybersecurity concerns. Robert Mueller issued a 38-page indictment on February 16th, 2018 against Russia's Internet Research Agency that makes it clear the Russian efforts to impact America's election were broad and sophisticated.

> The Russian efforts described in the indictment focused on establishing deep, authenticated, long-term identities for individuals and groups within specific communities. This was underlaid by the establishment of servers and VPNs based in the US to mask the location of the individuals involved. US-based email accounts linked to fake or stolen US identity documents (driver licenses, social security numbers, and more) were used to back the online identities. These identities were also used to launder payments through PayPal and cryptocurrency accounts. All of this deception was designed to make it appear that these activities were being carried out by Americans. [21]

With the 2020 election ramping up, the timeliness of research will be perfect for a 2020-2021 topic. The focus on cybersecurity will be high, but not just for election meddling. The 2016 election proved to be a catalyst for more focus on our cybersecurity as a whole [25].

Scope

The opening sentence of the Executive Summary for ISF's Threat Horizon 2021 is:

> By 2021 the world will be heavily digitized. Technology will enable innovative digital business models and society will be critically dependent on technology to function. This new hyperconnected digital era will create an impression of stability, security and reliability. However, it will prove to be an illusion that is shattered by new vulnerabilities, relentless attacks and disruptive cyber threats.[16]

It is clear that cyber threats pose dangers to society as we know it, and it is only becoming more dangerous as society increasingly digitizes. These threats range from disinformation campaigns threatening the legitimacy of our elections to full on cyber-attacks that take down our aging electrical grid. "[D]amage related to cybercrime [is] projected to hit $6 trillion annually by 2021 according to CyberSecurity Ventures" [38].

Range

One of the great aspects of cybersecurity as a debate topic is that it has a wide appeal. It can be nuanced and specific for advanced debaters but is also approachable for novices. Election meddling specifically is a great area for novice debaters to focus because it has such broad coverage in the news media. Also, most of the meddling evidence for 2016 focuses on social media, which is something high school students are experts at and understand.

Affirmative Ground

Below are three cards meant to illuminate only a few of the potential arguments on this topic.

Solvency Mechanism: Repeal CFAA and encourage security research
Wheeler 18
[Wheeler, T. (2018, September 12). In Cyberwar, There are No Rules. *Foreign Policy*. Retrieved from Foreign Policy]

Cyberattacks—some egregious, some mundane—are happening now, quietly and unnoticed by the public. Much of the confusion and fear over cybersecurity comes from the distorted publicity surrounding a few outlying events. While cybersecurity experts can't have perfect certainty over attribution or even the existence of some attacks, we can understand the larger security landscape, in which cybersecurity is merely a banal and predictable component of national infrastructure. The risk of cyberattacks is knowable, probabilistically. Technology and cyberspace are changing faster than countries can legislate internally and negotiate externally. Part of the problem with defining and evaluating acts of cyberwarfare against the United States is that U.S. law is unclear and unsettled when it comes to defining what constitutes an illegal cyber act as opposed to normal computer activity by information security researchers. The legal status of most information security research in the United States therefore remains unclear, as it is governed by the poorly drafted and arbitrarily enforced 1986 Computer Fraud and Abuse Act (CFAA)—a piece of legislation that was roundly derided by tech experts on its inception and has only grown more unpopular since. The law creates unnecessary fear that simple and useful information security research methods could be maliciously prosecuted. These methods include network scanning using tools such as Nmap (a computer network discovery and mapping tool) or Shodan (a search engine for devices on the internet of things) to find unsecured points of access to systems. Such scanning does not constitute the exploitation of computer or network vulnerabilities; a real-world equivalent would be walking down a street and noting broken windows, open doors, and missing fence planks without actually trespassing on someone else's property. One of the fastest fixes for the dismal state of federal cybersecurity expertise would be to overturn the CFAA and reward cybersecurity researchers engaged in preventive research instead of tying their hands with fears of breaking the law. Yet at present the U.S. governmentham-handedly discourages many information security researchers from entering what should be a noble service.

Potential Case Area - Critical Infrastructure
US GAO March 19
United States Government Accountability Office. (2019, March). *High-Risk Series.* Retrieved from https://www.gao.gov/assets/700/697245.pdf

Federal agencies and the nation's critical infrastructures—such as energy, transportation systems, communications, and financial services— are dependent on information technology systems to carry out operations. The security of these systems and the data they use is vital to public confidence and national security, prosperity, and well-being. The risks to systems underpinning the nation's critical infrastructure are increasing as security threats evolve and become more sophisticated.

Arms Reduction does not solve
Clark et al 2014

Committee on Developing a Cybersecurity Primer: Leveraging Two Decades of National Academies Work; Computer Science and Telecommunications Board; National Research Council; Clark D, Berson T, Lin HS, editors. At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. Washington (DC): National Academies Press (US); 2014 Jun 16.

The intent of an arms control agreement in general is usually to reduce the likelihood that conflict will occur and/or to reduce the destructiveness of any conflict that does occur. Such agreements can be bilateral or multilateral, and they can be cast formally as treaties, informally as memorandums of understanding, or even more informally as coordinated unilateral policies. In principle, arms control agreements can limit or ban the signatories from conducting some combination of research, development, testing, production, procurement, or deployment on certain kinds of weapons; limit or ban the use of certain weapons and/or the circumstances under which certain weapons may or may not be used; or oblige signatories to take or to refrain from taking certain actions under certain circumstances to reassure other signatories about their benign intent (i.e., to take confidence-building measures). For cyber weapons (where a cyber weapon is an information technology-based capability for conducting some kind of cyber intrusion), any limit on research, development, testing, production, procurement, or deployment of certain kinds of weapons is unlikely to be feasible. One reason is the verification challenge for such weapons; a second is the fact that such weapons have legitimate uses (e.g., both military and civilian entities use such weapons to test their own defenses). Distinguishing offensive capabilities developed for cyberattack from those used to shore up defenses against cyberattack would seem to be a very difficult if not impossible task. Restrictions on the use of cyber weapons might entail, as an example, agreement to refrain from launching cyberattacks against national financial systems or power grids, much as nations today have agreed to avoid targeting hospitals in a kinetic attack. Agreements to restrict use are by their nature not verifiable, but the inability to verify such agreements has not prevented the world's nations (including the United States) from agreeing to the Geneva Conventions, which contain similarly “unverifiable” restrictions. Yet recognizing violations of such agreements may be problematic. One issue is that non-state actors may have access to some of the same cyber capabilities as do national signatories, and non-state actors are unlikely to adhere to any agreement that restricts their use of such capabilities. Another issue is the difficulty of tracing cyber intrusions to their ultimate origin. If the ultimate origin of a cyberattack can be concealed successfully, holding the violator of an agreement accountable becomes problematic. Last, ambiguities between cyber exploitation and cyberattack complicate arms control agreements in cyberspace. A detected act of cyber exploitation may well be assessed by the target as a damaging or destructive act, or at least the prelude to such an act, yet forbidding cyber exploitation would go far beyond the current bounds of international law and fly in the face of what amounts to standard operating procedure today for essentially all nations.

Election Meddling

Election meddling is one of the biggest areas of the topic because it has been in the news consistently since Trump was elected. It is irrefutable that Russia did meddle in our election. The only question is how much of an effect it had [21]. This area also gets a lot of internal links to large impacts, like democracy and hegemony, and even politics impacts like GOP win good or bad.

Fidler 2018

[Fidler, D. (2019, January 2). *Year in Review: Cyber Threats and the Mid-Term U.S. Elections*. Retrieved from Council on Foreign Relations: https://www.cfr.org/blog/year-review-cyber-threats-and-mid-term-us-elections; AC]

Looking ahead, election cybersecurity requires consolidating and expanding the progress achieved in 2018, which demands White House leadership, robust commitment from DHS, the passage of new laws, and additional federal funding for hardening election systems against cyber intrusions. Although DHS will remain a key catalyst and partner, the politically divided Congress that begins in January 2019 might have difficulty adopting the laws and appropriating the funds necessary to advance election cybersecurity, especially without a crisis from the 2018 elections galvanizing action. Continued action is, however, imperative. Russia and other adversaries might have closely watched the 2018 elections to assess changes in U.S. election cybersecurity in order to develop strategies for targeting election systems in 2020.In terms of disinformation operations, less consensus exists about how to counter this threat, which might metastasize more in 2020 as artificial intelligence and "deep fakes" enhance the arsenal of information warfare. The scale of Russian information warfare during the 2016 and 2018 elections have produced calls for dramatic measures, such as regulating social media and inflicting damage on foreign states rather than just threatening it. A divided Congress will have trouble imposing regulations on social media. To have a credible deterrent effect for 2020, the U.S. government would have to retaliate more harshly against Russia for its interference in the 2018 elections—an escalation this White House appears unlikely to take.

Election meddling is going to be one of the first areas many will think of when first introduced to a cybersecurity topic because of its timeliness and media saturation. Politico has an entire tag dedicated to "election cybersecurity", and googling cybersecurity + election generates 33,200,000 hits.

Coverage of election security for the 2020 elections is already going, with a *New York Times* article on June 6, 2019 (*Election Rules Are an Obstacle to Cybersecurity of Presidential Campaigns*) detailing the roadblocks for candidates to defend against cyber-attacks and serving as a potential solvency mechanism for election security – overturning current statutes that prevent private companies from offering discounted security assistance to candidates. The article also says that the FBI Director (Christopher Wray) "warned in April that Russian election interference continued to pose a "significant counterintelligence threat" and that Russian efforts in the 2016 and 2018 elections were 'a dress rehearsal for the big show in 2020.'"

Healthcare

The healthcare industry is a very interesting area on which affirmatives could focus. Hospitals are increasingly reliant on internet and cloud based records to deliver care in a continuous and streamlined manner. As more reliance is placed on technology to deliver care, patient safety goes up but vulnerability to attack also increases.

> Cyberattacks are an increasing threat across all critical infrastructure sectors. For the health sector, cyberattacks are especially concerning because these attacks can directly threaten not just the security of our systems and information but also the health and safety of American patients. We are under constant cyberattack in the health sector, and no organization can escape that reality. While innovation in health information technology is a cause for optimism and increasing sophistication in health IT holds the promise to help address some our most intractable problems, whether in clinical care, fundamental research, population health or health system design, our technology will work for us only if it is secure. Information systems are crucial to today and tomorrow's healthcare system, so we must take every step possible to protect them. [14]

Potential affirmative cases could focus on protecting hospitals from cyber-attacks by increasing investment in cyber defense or even combatting ransomware specifically. There are many advantage areas to focus on with healthcare security, including patient health/safety, economic impact, and privacy to name a few. Privacy in particular is a very easy internal link story to prove.

> Cybersecurity threats to health care organizations and patient safety are real. Health information technology, which provides critical life-saving functions, consists of connected, networked systems and leverages wireless technologies, leaving such systems more vulnerable to cyber-attack. Recent highly publicized ransomware attacks on hospitals, for example, necessitated diverting patients to other hospitals and led to an inability to access patient records to continue care delivery. Such cyber-attacks expose sensitive patient information and lead to substantial financial costs to regain control of hospital systems and patient data. From small, independent practitioners to large, university hospital environments, cyber-attacks on health care records, IT systems, and medical devices have infected even the most hardened systems. Given the increasingly sophisticated and widespread nature of cyber-attacks, the health care industry must make cybersecurity a priority and make the investments needed to protect its patients. Like combatting a deadly virus, cybersecurity requires mobilization and coordination of resources across myriad public and private stakeholders, including hospitals, IT vendors, medical device manufacturers, and governments (state, local, tribal, territorial, and federal) to mitigate the risks and minimize the impacts of a cyber-attack. The U.S. Department of Health and Human Services (HHS) and the Health Care and Public Health (HPH, Health Sector, Health Care Industry) sector are working together to address these challenges.[14]

Ransomware

Healthcare & Public Health Sector Coordinating Councils. (2018). *Health Industry Cybersecurity Practices.* https://healthsectorcouncil.org/wp-content/uploads/2018/12/HICP-Main-508.pdf

In 2016, a bold new threat arrived on the scene: ransomware, a type of malicious software that attempts to deny access to data, usually by encrypting the data with a key known only to the hacker, until the data's owners pay a ransom. In ransomware schemes, attackers hold a hospital's or a physician's data hostage until money is paid, interrupting services and putting patients' lives at risk. Ransomware attacks that occurred at hospitals in 2016 and 2017, distributed denial of service attacks, and theft of protected health information (PHI), all demonstrate that cyber threats are capable of triggering emergencies that impact patient care and public health. Furthermore, in 2016, a private hospital suffered a ransomware attack resulting in the freeze of all computer systems. The attack forced the hospital to revert to pen and paper during the downtime to maintain patient and data records. With the systems down, schedules, documents, and patient data were unavailable, requiring the transfer of some patients to nearby health care institutions for more complete care. The attacker demanded compensation before restoring access to the hospital's systems and network. Although authorities became involved, after a week, the hospital conceded and paid the $17,000 ransom to regain full operational control.2Although the hospital regained control following the ransom payment in this instance, the FBI does not recommend paying ransoms to criminal actors. Furthermore, paying a ransom does not guarantee an organization will regain control of its data. [14]

Solvency Advocate
Weintraub and Borenstein 17

[Rebecca Weintraub and Joram Borenstien; June 1, 2017; *11 Things the Health Care Sector Must Do to Improve Cybersecurity*; Harvard Business Review; https://hbr.org/2017/06/11-things-the-health-care-sector-must-do-to-improve-cybersecurity; 7/10/19; AC]

Here are some specific recommendations, which are based on our collective expertise in care delivery, health systems, financial regulation, and risk management. Update HIPAA. Like the PCI DSS rules for debit and credit card security, the HIPAA Security Rule and the HIPAA Privacy Rule are already well-known frameworks for defining how a health care organization should secure its people, systems, data, and equipment. These established methods of approaching health care security would merely need to be updated to cover new forms of cyberattacks and new tactics employed by cybercriminals. Take stock of basic housekeeping. Care providers should apply strong encryption to all patient data and limit who has permission to access medical charts. In addition, organizations should monitor searches and downloads from their IT systems by tracking exfiltrated data such as large batch files of patient, research, financial, or other sensitive data. Purchase insurance. Many financial services organizations have cyber insurance, and health care systems should get it, too. Since this is a relatively nascent kind of insurance, most leaders of health care organizations and boards of directors may not be aware that it exists. Significant open questions about it remain, including who should pay for such policies and whether it should protect the institution, the patient, or both. At the moment, the institutions themselves are paying, and this likely will not change in the foreseeable future. Require training for personnel. Human error, including falling for phishing attacks, is the leading cause of major security breaches today. Health care systems should regularly remind people of the importance of information security best practices through required training, strategic reminders, and other means. Protect supply chains. Hospitals and health care systems have diversified supply chains and massive lists of vendors with whom they digitally interface. They are a tempting way for cybercriminals to gain access to health care organizations' IT systems. Consequently, care providers must understand the many moving parts that are involved and protect their relationships and information exchanges with and among those groups. Third-party vendors can help assess such risks and recommend ways to minimize them. Share industry best practices regarding cybersecurity. The FS-ISAC has made life easier and safer for the financial services sector by enabling peer financial institutions to share information rapidly and directly. Similar groups, such as the NH-ISAC, can serve as starting points for expanding similar types of discussions and planning. Deploy strong authentication. Health care systems should use multifactor authentication or other types of consumer security that are already ubiquitous in the U.S. financial services arena. Most U.S. consumers are already familiar with this type of technology and won't need to be significantly reeducated (a challenge the financial services sector had to deal with a decade ago). Adopt "tokenization." This approach, which involves substituting sensitive data with other unique but nonsensitive data, has been in vogue in the credit card world for the past few years. It is a suitable way to protect data in situations in which a consumer (i.e., a patient) is involved in some type of card-based transaction. This might involve using a flexible spending reimbursement card or paying a health care–related bill online. Copy the chip card approach. The U.S. consumer first encountered chip cards in a significant way in early 2015, when card issuers began to widely distribute them. Much of this was done in the run-up to a shift in who was liable for fraud. U.S. consumers are now intimately familiar with how to use such cards. (The cards have been in use for many years in France, the UK, Canada, Australia, and elsewhere.) Public and private payers are discussing the merits of issuing chip cards to beneficiaries to expedite patient identification and eligibility verification. Experiment with blockchain. The technology can record transactions between two parties efficiently and in a verifiable and permanent way. It is being used in financial services as well as other areas. For instance, after Estonia suffered a significant cyberbreach in 2007, the country became more aggressive about protecting its society and is now using blockchain to protect its citizens' medical data. A number of blockchain-based identity-credentialing systems exist, including Guardtime, TruCred, Civic, and OneName. Consider biometric-based security. Biometrics are increasingly being embraced as the ultimate "bio-identifier." Start-ups such as Simprints and RightPatient are testing its value as a verification feature for electronic medical records. Perhaps the most ambitious application of biometrics is the Indian government's Aadhaar project, which has created 12-digit unique identity numbers based on biometric and demographic information (e.g., iris scans, digital fingerprints, and a digital photo) for nearly all of the country's 1.2 billion citizens. But underlining the sad reality that no system is totally safe, this new system has already faced difficulties: Last month, the Centre for Internet and Society reported that 130 million Aadhaar numbers and around 100 million bank numbers of beneficiaries have been leaked online. The great boon of the digital era has been that patients' medical data is becoming increasingly portable. This promises to make it vastly easier to collect and share data from all the players in health care in the years ahead. But, unfortunately, it also poses major cybersecurity risks. In this new world, protecting patients' health information in accordance with HIPAA will take a highly coordinated effort among care providers, insurers, and institutions, as well as significant investments in new tools and practices. It also will require health care institutions to look at the cyber risks across their business, not simply in one niche area (e.g., access to patient records). In the risk management world, that is known as taking a holistic approach. The health care sector needs to adopt lessons from industries, such as financial services, that are much more advanced in their ability to thwart cyberattacks. Given how badly health care organizations are lagging others, they must make boosting cybersecurity a priority.

Electromagnetic Pulse

EMPs get access to a lot of "big stick" impacts, like hegemony and civilization collapse. Essentially an EMP (electromagnetic pulse) is a nuclear weapon detonated above the Earth's surface, which would destroy our electrical grid because of the waves of energy that an EMP exudes. One of the leading researchers on EMPs (Dr. Peter Vincent Pry) describes an EMP attack as "easy" compared to a nuclear attack and as a first strike opportunity, but also is something that is relatively easy to protect against. We can upgrade our electrical grid and put protections in place to prevent disruption. [28]

Any nuclear weapon, even a primitive first-generation weapon like the A-bombs that destroyed Hiroshima and Nagasaki, will produce gamma rays and fireballs that generate the high-frequency (E1 EMP), medium-frequency (E2 EMP), and low-frequency (E3 EMP) electromagnetic pulses. EMP attack delivers a three-fold punch to electronics small and large, ranging from personal computers to national electric grids and everything in-between: • Nuclear EMP attack entails detonating the weapon at such high altitude that no blast, thermal, fallout or effects other than EMP are experienced on the ground. • EMP is like "super-lightning" in that it delivers a shock much more powerful than lightning against, not a point, but against electronics over a vast area. • A single nuclear weapon can potentially make an EMP attack against a target the size of North America. • E1 EMP is much faster (lasting nanoseconds) and much more powerful than lightning, cannot be stopped by devices designed specifically for lightning protection, can damage and destroy small electronics and control systems necessary for the operation of everything from automobiles to airplanes, including electric grids, communications, and all other critical infrastructures. • E2 EMP is as fast (lasting milliseconds) and as powerful as lightning and can be stopped by lightning protection, but many commercial enterprises and homes lack lightning protection. • E3 EMP is much slower (lasting seconds) but has much more net energy than lightning, is potentially more powerful than the electromagnetic fields that could be generated by a solar super-storm, that can melt transformers designed to carry hundreds of thousands of volts. • Because EMP propagates in three "waves" their damaging effects will be dynamic and mutually reinforcing, the E1 EMP damaging and destroying systems (including possibly lightning protection) that opens the door for wider and deeper damage by E2 and E3 EMP. Any nuclear weapon detonated at an altitude of 30 kilometers or higher will generate a potentially catastrophic EMP. A nuclear detonation at 30 kilometers altitude will generate an EMP field with a radius on the ground of about 600 kilometers. Detonated at 400 kilometers altitude, the radius of the EMP field will be about 2,200 kilometers.42 [26]

EMPs are 'easy' to carry out
Pry, D. P. (2017). *Nuclear EMP Attack Scenarios and Combined-Arms Cyber Warfare.* Report to the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack.

EMP Attack is easy. Accuracy is not necessary for an EMP attack because the target altitude (30-400 kilometers) is so wide, and the radius and the coverage of the EMP field is so vast. EMP attack does not require a re-entry vehicle, heat shield, shock absorbers and other paraphernalia associated with a nuclear missile warhead designed for blasting a city. These are unnecessary for an EMP attack, which detonates the warhead above the atmosphere, in outer space. EMP attack can be executed by a wide variety of delivery vehicles, anything that can loft a nuclear weapon to 30 kilometers or higher. Possible delivery vehicles against the United States include a satellite, a long-range missile, a medium- or short-range missile launched off a freighter, some kinds of cruise missiles and anti-ship missiles (like Russia's Club-K exported to Iran), a jet fighter or some kinds of jet airliner doing a zoom climb, even a meteorological balloon.

EMP Attack kills millions
Graham and Pry 2018

Graham, W., Pry, P. (2018, October 16). *Ignoring EMP threat is a death sentence for Americans*. The Hill. https://thehill.com/opinion/cybersecurity/411451-ignoring-emp-threat-is-a-death-sentence-for-americans

In 2008, the statutory Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack delivered over 100 recommendations to Congress to protect the national electric grid and other life-sustaining critical infrastructures — including communications, transportation, energy, business and finance, food and water. We were hopeful the job would get done. Following an EMP attack, 326 million Americans could not long survive bereft of the electronic civilization that sustains their lives. EMP would be a civilization killer. The EMP commission reports are "good news," because they prove there is no excuse for the nation to be vulnerable. Electric grids and other life-sustaining critical infrastructures can be protected — affordably. For example, the 2008 report estimates that the electric grid's bulk-power system can be hardened to survive for a few billion dollars. So, in 2008, when the EMP Commission delivered what we thought then was our final report to Congress, we were hopeful America soon would be protected. However, by 2015 — 20 years after the first open congressional EMP hearing in 1995 — the U.S. Government Accountability Office testified to Congress that not a single major recommendation of the EMP Commission had yet been implemented. Not one. Consequently, Congress re-established the EMP Commission in 2015-2017 to re-examine the threat and to make further recommendations. The commission concludes in its new reports that the threat to electric grids and other life-sustaining critical infrastructures is just as great, or greater, than in 2008. U.S. military power, the national economy and civil society are increasingly dependent upon electricity and electronics that are vulnerable to EMP. And, now, North Korea has nuclear missiles and satellites that could execute an EMP attack on the United States. Moreover, on July 23, 2012, a massive and energetic solar coronal mass ejection crossed the orbit of the Earth, narrowly missing our planet by a few days. NASA now estimates the likelihood of a solar superstorm, of worldwide magnitude like the 1859 Carrington Event, is 12 percent per decade. Perhaps the most alarming conclusion of the new EMP Commission reports is that the U.S. government has been incapable of protecting our electronic civilization from EMP extinction. The EMP commissioners mostly are from a generation accustomed to thinking of the U.S. government as having the wisdom, vision and competence to successfully accomplish great enterprises in the national interest and protect our nation from existential threats. For example: During World War II, the U.S. government transformed its almost nonexistent U.S. Army into liberators of Western Europe and Asia and the "Arsenal of Democracy" that defeated Nazi Germany and Imperial Japan. The Manhattan Project (1942-1945) invented the atomic bomb and built the scientific-industrial infrastructure that sustained nuclear deterrence, preserved peace and won the Cold War. In 1954, with the launch of the USS Nautilus, the so-called U.S. Nuclear Navy soon included nuclear-powered aircraft carriers, cruisers, attack and ballistic missile submarines. The 1956 Dwight D. Eisenhower National System of Interstate and Defense Highways launched construction of the world's largest highway system, 50,000 road miles costing $120 billion, for commercial and defense purposes. In 1958, President Eisenhower's National Aeronautics and Space Act created NASA, responding to the USSR's launch of a satellite causing the "Sputnik crisis." NASA sent men to the moon in 1969 and won the space race. Whatever happened to the U.S. government capable of such feats? Bureaucratic politics, negligence and gross incompetence accounts for why the U.S. government has failed to protect Americans from the existential threat that is EMP. For example: The U.S. Federal Energy Regulatory Commission (FERC) is a rotating door for lawyers and lobbyists serving electric utilities and has been "captured" by the North American Electric Reliability Corporation (NERC), which is essentially a lobby for the electric power industry. The Department of Defense (DOD) over-classifies data on the EMP threat and hardening techniques needed by electric utilities and private sectors to protect the critical infrastructures, indifferent to the fact that DOD cannot defend the nation without electricity from the national grids. The Department of Homeland Security (DHS), bereft of data on the real EMP threat from DOD, relies for EMP expertise on novices working for the Department of Energy. The Department of Energy (DOE) relies for EMP expertise on novices, bureaucrats and erroneous "junk science" studies by recent administrations and electric power industries. Despite President Trump's direction to the U.S. government in his National Security Strategy that the nation's electric grid and other life-sustaining critical infrastructures be EMP-protected, and despite Congress in the Critical Infrastructure Protection Act ordering protection of the nation from EMP as a legal obligation, bureaucrats in DHS and DOE have, to date, deliberately ignored or dismissed the guidance of the president, the Congress and the EMP Commission. The bureaucratic Gordian knot preventing national EMP preparedness appears to be a greater challenge than winning World War II, the invention of the atomic bomb, the development of the nuclear navy, building the national highway system or sending men to the moon. What is needed, as recommended by the commission, is White House leadership, an executive agent appointed by the president — or, perhaps President Trump himself taking charge of national EMP preparedness — to plough through a resistant federal bureaucracy, the way that President Roosevelt did with the Manhattan Project or President Eisenhower with the national highway system. Protecting our electronic civilization is easy to do: A FERC regulation requiring utilities to protect the electric grid from 100 kilovolts/meter E1 EMP and 85 volts/kilometer E3 EMP would seriously address, and eventually solve, the problem.

EMP Attack kills 9/10 Americans
Bedard 19
Bedard, P. (2019, January 24). *New EMP Warning: US Will 'cease to exist,' 90 percent of population will die*. Retrieved from Washington Examiner: https://www.washingtonexaminer.com/washington-secrets/new-emp-warning-us-will-cease-to-exist-90-of-population-will-die

At a time when the military is starting to take the potential for an attack on the national electric grid more seriously, a newly declassified report is warning of an electronic world war launched by Russia, Iran, North Korea, and China that could wipe out North America, Europe, and Israel. With ease and using a primitive nuclear weapon, a "New Axis" of those aggressive nations could "black out" the Western world, dismantle all electricity and electronics, end water and food supply, and lead to millions of deaths in America. "Nine of 10 Americans are dead from starvation, disease, and societal collapse. The United States of America ceases to exist," warned the report declassified by recently decommissioned U.S. Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. The report, written by EMP expert Peter Vincent Pry, revealed EMP war plans drawn up by Iran, Russia, China, North Korea, and even ISIS. In "Nuclear EMP Attack Scenarios and Combined-Arms Cyber Warfare," Pry said that the Russians have called EMP a "revolution in military affairs." He explained it this way to the *Washington Examiner*: "This new warfare uses cyber viruses, hacking, physical attacks, non-nuclear EMP weapons, and a nuclear EMP attack against electric grids and critical infrastructures. It renders modern armies, navies, and air forces obsolete. It paves the way for asymmetric warfare by small nations and terrorists." Pry said that the U.S. is an easy target because virtually everything, military and civilian, relies on computers, and even the Pentagon uses the civilian Internet. "Ours is the most technologically advanced society, and therefore the most susceptible to attack," said Pry. The commission, the military and civilian groups have begun to take attacks on the U.S. electrical and Internet network more seriously, and they have discovered that those would be far more effective against the United States than a bomb. "Although it is very difficult to predict exactly which electronic systems would be upset, damaged, or destroyed by an EMP attack, with certainty massive disruption and damage will be inflicted on unprotected electronics within the EMP field and, because of cascading failures, far beyond. EMP is analogous to carpet bombing or an artillery barrage that causes massive random damage that is specifically difficult to predict, but reliably catastrophic in its macro-effects," he said. Pry, in calling for greater Pentagon and Homeland Security attention to the issue, compared the potential for an attack to Pearl Harbor. He also presented an "EMP World War" scenario where all the countries with EMP warfare plans join in a "New Axis" to attack the U.S., Europe, and Israel. Pry even suggested that a nuclear explosion in the atmosphere above Omaha, Neb., could black out Canada, the U.S., and Mexico. He predicted that an attack would lead to "damage too broad and too deep to repair, requiring years, if the U.S. could survive for years." Without making relatively inexpensive fixes to the electric grid and military bases to protect against an EMP attack, Pry said that the end could come fast. "There is no coming back," said his report, adding: "Everything is in blackout and nothing works. The EMP sparks widespread fires, explosions, all kinds of industrial accidents. Firestorms rage in cities and forests. Toxic clouds pollute the air and chemical spills poison already polluted lakes and rivers. In seven days, the over 100 nuclear power reactors run out of emergency power and go Fukushima, spreading radioactive plumes over the most populous half of the United States. There is not even any drinking water and the national food supply in regional warehouses begins to spoil in three days. There was only enough food to feed 320 million people for 30 days anyway."

Solvency Advocate
McNeil and Weitz 08

[Jena Baker McNeil and Richard Wetz; October 20, 2008; *Electromagnetic Pulse (EMP) Attack: A Preventable Homeland Security Catastrophe*; Heritage.org; https://www.heritage.org/homeland-security/report/electromagnetic-pulse-emp-attack-preventable-homeland-security-catastrophe; accessed 7/10/19; AC]

The Time for Action Is Now The U.S. cannot continue to ignore the EMP threat. While some progress has been made in hard-ening potential U.S. targets against attack, including critical military and government systems, the vast majority of electrical systems are unshielded and unprotected, especially in the civilian sector. If properly shielded, electrical devices and systems can generally survive even the strongest EMPs.[20] Congress and the new Administration must: Perform More Research on the Threat. Further research is needed in order to ensure that Amer-ica can respond to the EMP threat appropriately without wasting government resources on flimsy or useless security measures. Although there are numerous methods to harness EMPs capable of affecting electronic systems, there is still a theo-retical limit to what damage they can produce in terms of both geographic size and intensity. Some EMP weapons release just enough energy to disable small electrical devices while others can destroy all the electronic devices and sys-tems within a city block. Altitude plays a major role in whether an EMP attack will be successful; lower heights typically expose a smaller surface area to EMP damage. Some systems are simply more vulnerable to EMP attack than others, such as devices plugged into power grids and commercial computer equipment. The U.S. gov-ernment must gain knowledge of the attributes and capabilities of EMP and understand the amount of money, time, and effort that will be required for meaningful prevention. EMP research should also include actions by Con-gress to simulate the effects of an EMP attack on Washington and other high-value targets and re-examine the Graham Report recommendations. Build a Comprehensive Missile Defense Sys-tem. The most likely method of EMP attack would be a ballistic missile armed with a nuclear warhead. Building a comprehensive missile defense system would allow the U.S. to intercept and destroy a missile bound for the United States. The mere implementation of such a sys-tem would go a long way to prevent an attack by dissuading those who wish to carry out such actions and sending a clear message that the U.S. takes this threat seriously. Those opposed to missile defense in Congress and elsewhere have attempted to paint such an endeavor as a waste of resources that does noth-ing to further American security. 33 Minutes: Pro-tecting America in the New Missile Age, A Reader, a collection of essays by pre-eminent defense scholars, emphasized the need for such mea-sures, and recent missile testing by Iran demon-strates that other countries are actively involved in developing missile programs-which could be used against the U.S.[21] Incorporate EMP Attacks into National Plan-ning Scenarios. The National Planning Scenar-ios are 15 all-hazards planning scenarios used by federal, state, and local officials in disaster response exercises. The exercises can determine capabilities and needs and address problems before a disaster instead of after the fact. Given an EMP attack's unique nature and its ability to paralyze the U.S., individualized preparation is necessary. EMP must be added to the list. Develop a National Recovery Plan. The U.S. must identify the key power grid and telecom-munications infrastructure that is critical to pre-serving our nation's core capabilities and create a National Recovery Plan. This risk-based approach recognizes that certain infrastructure is key to recovery after an EMP attack. By taking measures to protect this infrastructure, we can lessen the recovery time from an attack.According to the National Fire Protection Associ-ation's (NFPA) "Standard on Disaster/Emergency Management and Business Continuity Programs," a private company should prepare to function without electricity for a short period in order to maintain uninterrupted operations.[22] While this time period will certainly vary by industry, encouraging the private sector to prepare in this manner and to develop company recovery plans will allow the government to focus on bringing key infrastructure back online. The private sector can move toward this goal by investing in more adequate infrastructure now. A Threat too Big to Be Ignored Although many in Congress and the White House tend to ignore the EMP threat, America's potential adversaries will not. To these adversaries, EMP technology represents the opportunity to inflict-with relative ease-catastrophic and lasting damage on the United States that could threaten our very existence. Preventing such an attack depends on the U.S. government's ability to understand the very real chance and the devastating consequences of an EMP attack-and to take the actions necessary to prevent them.

Negative Ground

Privacy

Privacy concerns are integral to questions of cybersecurity. The major federal cybersecurity bill, The Cybersecurity Information and Sharing Act of 2015, is arguably a large violation of privacy[33.] Arguments can be made both for and against increasing cybersecurity. Increasing security usually means a decrease in privacy because the company or government has more access to information, but it also means an increase in privacy because hackers cannot get access to the information.

> 2018 has been the year of privacy. News of Facebook's exposure of tens of millions of user accounts to data firm Cambridge Analytica broke in March — a scandal that was only compounded by recent news that the tech giant shared even more private data through hidden agreements with other companies. Then in May, the European Union's General Data Protection Regulation, the world's most stringent privacy law, came into effect. By the end of the year, even Apple's and Microsoft's CEOs were calling for new national privacy standards in the United States. It's not just a coincidence that privacy issues dominated 2018. These events are symptoms of larger, profound shifts in the world of data privacy and security that have major implications for how organizations think about and manage both. So what, exactly, is changing? Put simply, privacy and security are converging, thanks to the rise of big data and machine learning. What was once an abstract concept designed to protect expectations about our own data is now becoming more concrete, and more critical — on par with the threat of adversaries accessing our data without authorization. More specifically, the threat of *unauthorized access* to our data used to pose the biggest danger to our digital selves — that was a world in which we worried about intruders attempting to get at data we wanted private. And it was a world in which privacy and security were largely separate functions, where privacy took a backseat to the more tangible concerns over security. Today, however, the biggest risk to our privacy and our security has become the threat of *unintended inferences*, due to the power of increasingly widespread machine learning techniques. Once we generate data, anyone who possesses enough of it can be a threat, posing new dangers to both our privacy and our security. These inferences may, for example, threaten our anonymity — like when a group of researchers used machine learning techniques to identify authorship of written text based simply on patterns in language. (Similar techniques have been used to identify software developers based simply on the code they've written.) [6]

That same article goes on to detail the impact that privacy and security concerns have on the bottom line of companies like Facebook, Apple, etc. The line between privacy and security is becoming less and less clear as time goes on. The real issue with privacy going forward is the impossibility of understanding all the threats and risks to information breaches.

> This is precisely why the recent string of massive data breaches, from the Marriott breach that impacted 500 million guests to the Yahoo breach that affected 3 billion users, are so troubling. The problem isn't simply that unauthorized intruders accessed these records at a single point in time; the problem is all the unforeseen uses and all the intimate inferences that this volume of data can generate going forward. It is for this reason that legal scholars such as Oxford's Sandra Wachter are now proposing legal constraints around the ability to perform this type of pattern recognition at all. Once described by Supreme Court Justice Louis Brandeis as "the right to be let alone," privacy is now best described as the ability to control data we cannot stop generating, giving rise to inferences we can't predict. And because we create more and more data every day — an estimated 2.5 quintillion bytes of it — these issues will only become more pressing over time. If we thought that 2018 was dominated by privacy concerns, just wait until 2019.

States CP

Some states are already giving tax credits for cybersecurity improvements for businesses. Maryland, for instance, gives up to 50% of the cost of cybersecurity improvements as a tax credit for qualified businesses [17]. As such, arguments can be made that the states are already doing the plan and going through the state governments is better than using the federal government. There are many solvency advocates that argue federal action is key (such as Liwar 19 in this paper), so affirmatives will have case specific responses to this argument, but states will still be a popular counterplan.

Private Sector Good/CP

A good argument against most affirmative cases will be to have the private sector do the plan instead of the federal government. Typically, negative teams will read a politics or federalism disadvantage as the net benefit to the counterplan, but there is also good evidence to be had that the private sector is better in this case because of concerns over privacy. Adding the privacy impacts to a private sector counterplan will make for an interesting and fresh debate over the federal government's involvement in cyber security.

Not only does this argument pair well with privacy, it is also the direction the current administration is taking our cybersecurity policy. [5]

Brown et al 18

Brown, M. L., Gardner, M. J., Burd, J. W., Diakiwski, M. L., & Scott, K. L. (2018, September 21). *National Cyber Strategy Emphasizes Private Sector's Shared Responsibility for Cyberspace*. Retrieved from Wiley Rein LLP: https://www.wileyrein.com/newsroom-articles-National_Cyber_Strategy_Emphasizes_Private_Sectors_Shared_Responsibility_for_Cyberspace.html

On September 20, 2018, the White House released the long-awaited National Cyber Strategy (Strategy). The Strategy builds off of Executive Order 13800 "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" and the National Security Strategy, which was heavily focused on cyber issues. While a major policy shift includes enabling offensive cyber measures as a means of deterrence, the private sector should take note of the emphasis on shared responsibilities and rising expectations for government contractors, technology companies, the transportation and telecommunications sectors, and others. The Strategy notes that America's adversaries have taken advantage of American innovation, using our openness and reliance on connected networks as an asymmetric equalizer. This environment of "new threats and a new era of strategic competition," the Administration contends, demands "a new cyber strategy that responds to [these] new realities, reduces vulnerabilities, deters adversaries, and safeguards opportunities for the American people to thrive." The Strategy confirms trends that we have observed in recent years: the government is putting more responsibility on the private sector. The National Cyber Strategy outlines rising expectations for government and non-government actors, including contractors, information and communications technology developers, telecommunications providers, and satellite system operators, among others.

Incentives or No Incentives

Including incentives in the wording of the resolution will shift the debate away from the limited scope the federal government can have into the private sector without violating privacy or federalism restrictions and instead allow us to have debates over what incentives are most likely to engender change in the market.

Not including incentives makes more sense if we focus the resolution on very specific types of cybersecurity issues, like election security, that are much more government focused.

With a more general cybersecurity resolution, including incentives serves to limit the resolution, as well as improve ground for both the affirmative and negative. If we leave incentives out of the resolution, some affirmative teams will still use some sort of incentive-based approach to improve cybersecurity in order to avoid federalism and privacy arguments in addition to other mechanisms.

The ground is improved because negative teams now have access to counterplans to use different types of incentives and to attack the incentive choice of the affirmative. The affirmative now gets to avoid a lot of the links to federalism while accessing solvency of a much broader scope since it can now argue private sector involvement/initiative is topical.

We need more incentives
DHS 13
[Department of Homeland Security. (2013). Executive Order 13636: Improving Cybersecurity Infrastructure Incentives Study Analytic Report; AC]

"While some market-based incentives exist to improve the cybersecurity of critical infrastructure, independent of government intervention, the pace of the necessary improvement in cybersecurity needs to be hastened in order to more rapidly counter the increasing risk of cyber attacks and cyber espionage. As such, it is appropriate to consider where government action can provide additional impetus to the market, while acknowledging that there are places where market-based incentives may perform adequately independent of government intervention."

Cyber incentives work – Grants and rate-recovery work best, followed by subsidies and tax incentives.
DHS 13
[Department of Homeland Security. (2013). Executive Order 13636: Improving Cybersecurity Infrastructure Incentives Study Analytic Report; AC]

"2.6.1. Effectiveness: Does it work? As described above, effectiveness is defined by the extent to which an incentive affects the probability of Framework adoption. Recall that the attributes in the microeconomic model that define the marginal benefit of Framework adoption are uncertain: Increasing unknown, and to some extent unknowable, benefits could increase the probability of adoption for some Framework adopters, while reducing Framework implementation costs that will occur with certainty increases the probability of Framework adoption for all Framework adopters. Additionally, marginal revenue increases would apply only to the subset of organizations that both adopt the Framework and sell goods and services to the Federal Government through the procurement process. For these reasons, other things being equal, incentives that minimize the marginal increase in cybersecurity costs required to adopt the Framework through cost sharing are more likely to promote the adoption of the Framework than incentives that increase the perceived expected loss avoided by Framework adoption and/or that increase marginal revenue or ancillary benefits.

As a result, effectiveness judgments are principally driven by Framework cost sharing, though expected loss avoidance, marginal revenue increase, and ancillary benefits also contribute to a lesser extent. The incentives that minimize the marginal increase in cybersecurity costs required to adopt the Framework through cost sharing include: • Grants, • Rate-recovery for price-regulated industries, • Subsidies, and • Tax incentives. Of these four categories, two incentives are assessed to be in the top tier of incentive categories for cost-sharing, and thus the top tier of incentive categories for the probability of Framework adoption: grants to non price-regulated industries, and rate-recovery for price-regulated industries. Subsidies and tax incentives are assessed to be in the second tier for cost-sharing and thus the second tier for the probability of Framework adoption."

Solvency Advocate
Liwer 19

[Dror Liwer, January 16, 2019; *Voices It's time for the federal government to incentivize cybersecurity*; Accounting Today; https://www.accountingtoday.com/opinion/its-time-for-the-federal-government-to-incentivize-cybersecurity; accessed 6/20/19; AC]

It should come as no surprise to learn that cybercrime is on track to cost the global economy more than $600 billion in 2018. What is surprising, however, is that many of the organizations contributing to such economic peril are not of Fortune 1000 status, but rather they are the small and midsized businesses that drive the U.S. economic engine. Today, hackers, fraudsters and cyber criminals regularly target smaller companies as larger organizations prove more difficult to breach due to the time, money and resources they have to invest in cybersecurity. A recent survey by Hiscox found that nearly half of all small businesses have experienced at least one cyberattack in the past year at an average cost of $34,604 to remediate. Similarly, Symantec research concludes that 43 percent of all cyberattacks now target small business, while 6 in 10 of such businesses go out of business for good post breach. Cybersecurity threats to small business The vast majority of small businesses do not have the time, money and resources to invest in the depth of cybersecurity needed within today's threat landscape. That's unfortunate, as only 16 percent of small businesses report being very confident in their cybersecurity readiness, and barely half had a clearly defined cyber security strategy, according to Hiscox. Today, SMBs rely primarily on outdated firewalls and consumer-grade solutions, or the limited security inherent to the cloud apps they use most. However, such confidence in cloud app security is misguided, creating a false sense of security. For a variety of reasons and unbeknown to most users, cloud apps, such as Office 365, G-Suite, Dropbox, Slack, etc., are highly vulnerable to cyberattack. With low risk and high reward for attackers, cloud apps mask as a primary attack vector on a regular basis. Making cybersecurity accessible to small business Knowing the increase in attacks targeting small businesses will not moderate anytime soon, and that the financial burden of implementing strong cybersecurity will price out many of the 30.2 million American small businesses, it's time for the federal government to act. Offering incentives, such as tax credits or reduced costs, to small businesses to invest in cybersecurity tools could not only boost innovation and help companies acquire a much-needed safety net, but it would improve security across the entire economy. With small businesses making up almost half of U.S. private sector employment, any mass increase in downtime and forced closures due to cyberattack, such as a data breach, would likely have ripple effects throughout the public and private sector. Such a reality represents a daunting proposition for what is already a fragile U.S. economy hampered by inequality, stagnant wages, and soaring debt and deficits. Incentives would offer the same endgame as regulations without the stigma of companies being forced to do something. In fact, there are many cases where the federal government has used tax rebates, deductions and credits to encourage behavior that may have otherwise not occurred or been financially unattractive. The federal solar tax credit, for example, allows consumers and businesses to deduct 30 percent of the cost of a solar system from their federal taxes, has helped consumers bridge the cost gaps in solar panels. This has made it more affordable for consumers and has encouraged more innovators to enter the space and improve the technology. Federal incentives have also been partly responsible for the rapid advancement in wind power and electric vehicles. And they have also been used to encourage the purchase of health insurance at a time when rising health costs are contributing mightily to the national debt and deficit. Some states are already offering cybersecurity industry incentives. In Maryland, the Cybersecurity Investment Incentive Tax

Credit offers a refundable income tax credit equal to 33 percent (up to a maximum of $250,000) for companies that invest in a qualified cybersecurity company. Recently, The Mayor's Office of the Chief Technology Officer (MOCTO) of New York City, launched a 'moonshot' challenge, incentivizing the cybersecurity community to devise "new, affordable and scalable solutions to protect New York's small and mid-size business from cyber-attacks." Maryland and New York aren't alone. According to the National Council of State Legislators, "states are addressing cybersecurity through various initiatives, such as providing more funding for improved security measures, requiring government agencies or businesses to implement specific types of security practices, increasing penalties for computer crimes, addressing threats to critical infrastructure and more." Now, action is needed at the federal level. While such incentives do carry a price tag, the Atlantic Council and Zurich Insurance Group noted that a completely secure internet could result in a global net gain of $190 trillion by 2030. Incentivizing the adoption of and investment in cybersecurity could significantly reduce risk across the entire U.S. economy. Incentives for cybersecurity adoption would likely reduce risk to not just individual businesses but would have the same effect throughout the entire economy. With global trade and economic tensions heightening, we as a country cannot afford to wait for small businesses to find the means to afford the cybersecurity that they now need, and we certainly cannot expect cybersecurity companies to reduce their costs of goods and services. Instead, we must look to the federal government to join states and municipalities and formulate an incentives program that does more than simply encourage smaller businesses to adopt cybersecurity – it makes it realistic for them to do so.

Incentives needed

[Cybersecurity for the homeland; December 2004; Report of the Activities and Findings by the Chairman and Ranking Member Subcommittee on Cybersecurity, Science, and Research & Development of the U. S. House of Representatives Select Committee on Homeland Security; accessed 4/21/19; AC]

Addressing vulnerabilities requires additional attention. For example, companies that develop hardware, software, and networking platforms should continue to strive to eliminate as many flaws and vulnerabilities as possible before their products enter the market. While it is nearly impossible to create a product that is 100% error-free, several IT security businesses stated that they have efforts underway to increase the security and dependability of pre-marketed technologies. The Subcommittee views these initiatives as positive. More, however, can be done. Both Congress and the Department of Homeland Security should consider incentives and recognition programs to encourage private industry to develop more secure cyber products. Additionally, all users—from the individual consumer to the large corporation—should strive to understand vulnerabilities within their networked environment and safeguard against them. It is also necessary to prepare mitigation and contingency plans to respond if a vulnerability is exploited.

Definitions

Cybesecurity

Cybersecurity definition – "core function"

What is Cybersecurity? A Definition of Cybersecurity; CyberPedia, PaloAlto Networks; https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security; accessed 6/20/2019; AC

Cybersecurity refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access. According to Forbes, the global cybersecurity market is expected to reach 170 billion by 2020. This rapid market growth is being fueled by an array of technology trends, including the onslaught of initiatives with ever-evolving security requirements, like "bring your own device" (BYOD) and the internet of things (IoT); the rapid adoption of cloud-based applications and workloads, extending security needs beyond the traditional data center; and stringent data protection mandates, such as the European Union's General Data Protection Regulation and the National Institute of Security Technology (NIST) Cybersecurity Framework. Why Cybersecurity Is Required The core functionality of cybersecurity involves protecting information and systems from major cyberthreats. These cyberthreats take many forms (e.g., application attacks, malware, ransomware, phishing, exploit kits). Unfortunately, cyber adversaries have learned to launch automated and sophisticated attacks using these tactics – at lower and lower costs. As a result, keeping pace with cybersecurity strategy and operations can be a challenge, particularly in government and enterprise networks where, in their most disruptive form, cyberthreats often take aim at secret, political, military or infrastructural assets of a nation, or its people. Some of the common threats are outlined below in more detail. Cyberterrorismis the disruptive use of information technology by terrorist groups to further their ideological or political agenda. This takes the form of attacks on networks, computer systems and telecommunication infrastructures. Cyberwarfareinvolves nation-states using information technology to penetrate another nation's networks to cause damage or disruption. In the U.S. and many other nations, cyberwarfare has been acknowledged as the fifth domain of warfare (following land, sea, air and space). Cyberwarfare attacks are primarily executed by hackers who are well-trained in exploiting the intricacies of computer networks, and operate under the auspices and support of nation-states. Rather than "shutting down" a target's key networks, a cyberwarfare attack may intrude into networks to compromise valuable data, degrade communications, impair such infrastructural services as transportation and medical services, or interrupt commerce. Cyberespionage is the practice of using information technology to obtain secret information without permission from its owners or holders. Cyberespionage is most often used to gain strategic, economic, political or military advantage, and is conducted using cracking techniques and malware.

Cyber vs Cyberspace vs Cyber conflict vs Cyber war
Valeriano and Maness 15

[Brandon Valeriano and Ryan C. Maness, 2015; *Cyber War versus Cyber Realities;* print]

The prefix *cyber* simply means computer or digital interactions, which are directly related to *cyberspace*, a concept we define as the networked system of microprocessors, mainframes, and basic computers that interact at the digital level. Our focus in this volume is on what we call *cyber conflict*, the use of computational technologies for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions among states. *Cyber war* would be an escalation of cyber conflict to include physician destruction and death. Our focus, therefore, is on cyber conflict and the manifestation of digital animosity short of and including frames of war. These terms will be unpacked in greater detail in the chapters that follow.

Cyber ecosystem –
The cyber ecosystem includes not only the interconnected network of information technology infrastructure we call cyberspace, but also the people, environment, norms, and conditions that influence that network.
https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf
Herb Lin, January 5, 2018; Dr. Herb Lin is senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University; https://www.lawfareblog.com/election-hacking-we-understand-it-today-not-cybersecurity-issue

Start with the U.S. government's working definition of cybersecurity as "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation." (This unclassified definition comes from National Security Presidential Directive NSPD-54.)

Critical Information Infrastructure –

Emma-Iwuoha 17
[Lisa Emma-Iwuoha, January 22nd, 2017; https://www.michalsons.com/blog/what-is-a-national-critical-information-infrastructure/17701; ALC]

What falls within the definition of Critical Information Infrastructure? The Cybercrimes and Cybersecurity Bill defines Critical Information Infrastructure very broadly. It is any data, database, network, communications infrastructure, (or part thereof), or anything associated with them that has been declared a CII. Critical Information Infrastructures also include the things listed above, which are in the possession or under the control of the State (national, provincial or local), and anyone exercising a public power or performing a public function. Examples of possible CIIs are the infrastructure (or part) of: a bank Home Affairs JSE a medical scheme Basically, anything State Security thinks that if lost, could cause harm to people, the economy or the country.

Information Infrastructure distinct from other critical infrastructure
[Cybersecurity for the homeland; December 2004; Report of the Activities and Findings by the Chairman and Ranking Member Subcommittee on Cybersecurity, Science, and Research & Development of the U. S. House of Representatives Select Committee on Homeland Security; accessed 4/21/19; AC]
The information infrastructure is unique among the critical infrastructures because it is owned primarily by the private sector, it changes at the rapid pace of the information technology market, and it is the backbone for many other infrastructures. Therefore, protection of this infrastructure must be given the proper attention throughout government.

Coercion

Threats, punishment or escalation of costs
Valeriano et al 2018
Valeriano, B., Jensen, B., & Maness, R. C. (2018). *Cyber Strategy.* New York City: Oxford University Press.
Coercion is the use of threats, punishment, or escalation of costs during a crisis or conflict to alter the foreign policy behavior of the target. The application of force is more potential than actual, taking minimal actions to alter the cost-benefit calculation of an adversary short of using "brute" force that results in escalation to a major military campaign (Schelling 1966).

Coercion = positive inducements too
Valeriano et al 2018
Valeriano, B., Jensen, B., & Maness, R. C. (2018). *Cyber Strategy.* New York City: Oxford University Press.

In our conceptionalization of combined coercive actions, consistent with coercive diplomacy, we account for positive inducements in diplomatic, economic, or military categories alongside covert punishment in cyberspace. Diplomatic overtures, meetings, consultations, and summits are seen as positive steps forward where dialogue and a frank exchanges of ideas take precedence over threats. In economic maneuvers, negative sanctions are popular, but so are positive events like freeing up previously seized money, removing sanctions, or exchanging cash and goods to remove ill will.

Incentives

Incentives include punishment and reward
American Heritage, 06 (http://dictionary.reference.com/browse/incentive)
in·cen·tive
n. Something, such as the fear of punishment or the expectation of reward, that induces action or motivates effort.

Incentives are positive and negative
Ostrum et al, 01 - Workshop in Political Theory and Policy Analysis, Indiana University (Elinor, "Aid, Incentives, and
Sustainability: An Institutional Analysis of Development Cooperation",
http://www.asdi.org/shared/jsp/download.jsp?f=Stud02-01.pdf&a=2429)

The dictionary definition of an incentive is "that which incites or encourages; a motive; a stimulus" (MacMillans Modern Dictionary). Thus, the concept implies both an external stimulus and an internal motivation. In institutional analysis, one uses the term to refer to rewards and punishments that are per-ceived by individuals to be related to their actions and those of others. The payments people receive or costs they have to pay, the respect they earn from others, the acquisition of new skills or knowledge are all external stimuli that may induce more of some kinds of behavior and less of other kinds. Donors use a variety of external stimuli in their effort to change behavior of officials and beneficiaries in recipient countries. Perceived rewards and punishments can motivate individuals to take actions that are genuinely productive for all involved. The positive incentives within a well-structured, competitive market for private goods where private rights are well enforced, for example, lead most participants to invest in activities that help themselves while generating benefits for others. Incentives are consid-ered perverse when they lead individuals to avoid engaging in mutually pro-ductive outcomes or to take actions that are generally harmful for others.

Incentives – even broadly defined – must be positive – they exclude negative penalties

Knowler, 99 - UN Food and Agricultural Organization (D., "Incentive Systems for Natural Resource Management: The Role of Indirect Incentives", ftp://ftp.fao.org/docrep/fao/007/x2247e/x2247e00.pdf)

1.8 Incentives may be broadly defined, as in "everything that motivates or stimulates people to act" (Giger 1996). What is important about such a broad definition is that it allows for incentives to be of either a passive or an active nature. In the former case, we can think of incentives as signals in the producer's environment which influence decision-making about farming practices, whether intended or otherwise. Many macroeconomic policies, being remote from the producer and targeted at objectives other than promoting sustainable farming practices, would fit into this category. In contrast, the notion of 'active' refers to a government's ability to actually design or modify policies with a desire to bring about certain conservation outcomes. McNeely (1988), for example, refers to this concept of incentive when he defines incentives as "any inducement which is specifically intended to incite or motivate governments, local people, and international organizations" (p.38-39). We draw this distinction because of the need to consider both active and passive aspects when assessing the importance of incentives for NRM. While governments may be most concerned with the design of good policies aimed at improving NRM, they need to be cognizant of the sometimes counterproductive influence exerted by a poor incentive structure, in the passive sense. 1.9 McNeely (1988) also makes the useful distinction between incentives, disincentives and perverse incentives. In contrast to incentives, which we have described above, disincentives are purposely designed to discourage particular behaviours and can include taxes, fines and various other penalties or moral suasion. For purposes of this study, we will not consider disincentives as distinct from incentives per se, but it is useful to be aware of the distinction. In contrast, perverse incentives incite resource users to damage or deplete the resources in question in a socially inefficient manner and are closely related to the concept of policy failure, which is discussed in Chapter 2.

Incentives are an offer of value meant to alter a course of action

Grant, 02 - professor of political science at Duke University (Ruth, "THE ETHICS OF INCENTIVES: HISTORICAL ORIGINS AND CONTEMPORARY UNDERSTANDINGS," Economics and Philosophy, 18 (2002) 111, proquest)

Increasingly in the modern world, incentives are becoming the tool we reach for when we wish to bring about change. In government, in education, in health care, between and within institutions of all sorts, incentives are offered to steer people's choices in certain directions. But despite the increasing interest in ethics and economics, the ethics of the use of incentives has raised very little concern. From a certain point of view, this is not surprising. When incentives are viewed from the perspective of market economics, they appear to be entirely unproble-matic. An incentive is an offer of something of value, sometimes with a cash equivalent and sometimes not, meant to influence the payoff structure of a utility calculation so as to alter a person's course of action. In other words, the person offering the incentive means to make one choice more attractive to the person responding to the incentive than any other alternative. Both parties stand to gain from the resulting choice. In effect, it is a form of trade, and as such, it meets certain ethical requirements by definition. A trade involves voluntary action by all parties concerned to bring about a result that is beneficial to all parties concerned. If these conditions were not met, the trade would simply not occur. And as inducements in a voluntary transaction, incentives certainly have the moral high ground over coercion as an alternative.

Incentives are distinct from tax credits – they require linking behavior to future action, not credit for actions already taken

Bingel, 04 - senior manager of state and local taxes with Smart and Associates LLP(Gary, "Getting to the STATE'S CAPITAL: Negotiating Business Incentives", Pennsylvania CPA Journal. Summer, proquest)

When considering financial assistance from governmental authorities, it is important to keep in mind the definitions of "incentive" and "credit." "Incentive" is something that stimulates one to take action,1 and "credit" is to give deserved commendation for; to commend one for.2 These concepts are at the root of why governments give assistance to businesses in the form of incentives and tax credits. Incentive programs are usually offered to stimulate businesses to take some form of action, and are considered forward-looking. Tax credits are often offered to reward businesses that took some form of desired action, and are a reaction to steps already taken. There are some programs, however, that combine these concepts, such as negotiated tax credits and those that require preapproval, that are used to promote some future action. There are also incentives programs that, while negotiated and subject to preapproval, are only rewarded once a specified action, or promise, has been fulfilled. The following discussion will focus on true incentives programs, those that require preapproval and negotiation, as opposed to pure tax credits, which merely reward past behavior and that do not require any form of preapproval or negotiation.

Incentives are distinct from tax credits – they require linking behavior to future action, not credit for actions already taken

Bingel, 04 - senior manager of state and local taxes with Smart and Associates LLP(Gary, "Getting to the STATE'S CAPITAL: Negotiating Business Incentives", Pennsylvania CPA Journal. Summer, proquest)

When considering financial assistance from governmental authorities, it is important to keep in mind the definitions of "incentive" and "credit." "Incentive" is something that stimulates one to take action,1 and "credit" is to give deserved commendation for; to commend one for.2 These concepts are at the root of why governments give assistance to businesses in the form of incentives and tax credits. Incentive programs are usually offered to stimulate businesses to take some form of action, and are considered forward-looking. Tax credits are often offered to reward businesses that took some form of desired action, and are a reaction to steps already taken. There are some programs, however, that combine these concepts, such as negotiated tax credits and those that require preapproval, that are used to promote some future action. There are also incentives programs that, while negotiated and subject to preapproval, are only rewarded once a specified action, or promise, has been fulfilled. The following discussion will focus on true incentives programs, those that require preapproval and negotiation, as opposed to pure tax credits, which merely reward past behavior and that do not require any form of preapproval or negotiation.

Incentives are limited to cash or in-kind transfers to speed up adoption

Cooley, 07 - CRANFIELD UNIVERSITY, Thesis submitted for a degree in Masters of Science (Suzannah, "GROWTH OF THE UK LOW CARBON DIOXIDE AND ALTERNATIVE TECHNOLOGY VEHICLE MARKET: INVESTIGATING INFLUENTIAL FACTORS IN THE ADOPTION OF LOW CARBON VEHICLES," September, https://dspace.lib.cranfield.ac.uk/bitstream/1826/2401/1/Sue%20Cooley%20Thesis%20final%20v2.pdf)

Incentives can be used to introduce or increase actual or perceived relative advantages. Rogers (2003) defines incentives as a direct or indirect payment of cash or in kind that is given to an individual or system in order to encourage behaviour change and speed up adoption. Incentives can take many forms for example, taxes, grants, penalties, finder's fees, bonuses. Oltra & Saint-Jean (2006) suggest that government grants to support alternative fuel infrastructure, tax exemptions for inconvenience and negative taxation for ICEV could secure the switch from ICEVs to LCVs. Akerman & Hojer (2006) observes in the 1980's tax incentives on unleaded petrol and lower emitting vehicles successfully promoted three-way-catalytic-converters. For high mileage users, Vries & Rouwendal (1999) and Wissen & Golob (1992) also found financial incentives encouraged LCV adoption. Moreover, Lane & Potter (2007) emphasises that the benefit of incentives in combating the barriers of high purchase price, serving costs and long payback periods associated with many LCVs, concluding that the UK company car tax is a crucial factor in determining employee's car choice and the UK Government's Powershift grant to be an important factor encouraging the purchase of the Toyota Prius hybrid.

Incentives are any policy that incites someone to action

Menezes, 90 – JD at Thomas Cooley Law School (Marco, 7 Cooley L. Rev. 139 (1990) "P.A. 198: Michigan's Industrial Property Tax Abatement Law: Fortuity or Futility", Hein Online)

Any analysis of the public policies underlying PA 198 must focus on the Act's intended function as an incentive to economic development. The term "incentive" is generally defined as "something that incites or has a tendency to incite to determination or action."200 Since tax abatement. policies reduce business costs, they can be broadly defined as "incentives."'201 Lower costs are "good for business" and generally tend to incite, or actually do incite, in-dustrial development.202 Obviously, what may be an incentive to one industry may not be an incentive to another.203 Thus, incen- tives generally tending to incite action are distinguishable from incentives actually inciting action in a specific case.204

Bibliography

1. Aspa, J. (2018, January 16). *What is the Cybersecurity Act?* Retrieved from Investing News: https://investingnews.com/daily/tech-investing/cybersecurity-investing/cybersecurity-act/

2. Bedard, P. (2019, January 24). *New EMP Warning: US Will 'cease to exist,' 90 percent of population will die*. Retrieved from Washington Examiner: https://www.washingtonexaminer.com/washington-secrets/new-emp-warning-us-will-cease-to-exist-90-of-population-will-die

3. Bertrand, N. (2019, February 2). *Russia Is Attacking the U.S System From Within*. Retrieved from The Atlantic: https://www.theatlantic.com/politics/archive/2019/02/new-mueller-filing-shows-how-russia-misuses-us-courts/581884/

4. Blanco, E., & Woodruff, B. (2019, February 19). *Trump's DHS Guts Task Forces Protecting Elections From Foreign Meddling*. Retrieved from The Daily Beast: https://www.thedailybeast.com/trumps-dhs-guts-task-forces-protecting-elections-from-foreign-meddling

5. Brown, M. L., Gardner, M. J., Burd, J. W., Diakiwski, M. L., & Scott, K. L. (2018, September 21). *National Cyber Strategy Emphasizes Private Sector's Shared Responsibility for Cyberspace*. Retrieved from Wiley Rein LLP: https://www.wileyrein.com/newsroom-articles-National_Cyber_Strategy_Emphasizes_Private_Sectors_Shared_Responsibility_for_Cyberspace.html

6. Burt, A. (2019). Privacy and Cybersecurity Are Converging. Here's Why That Matters for People and for Companies. *Harvard Business Review*.

7. Chertoff, M., & Grant, J. (2017). 8 Ways Governments Can Improve Their Cybersecurity. *Harvard Buisness Review*.

8. D, C., T, B., & H., L. (2014). *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues.* Washintgon DC: National Research Council.

9. Emma-Iwuoha, L. (2017, January 22). Retrieved from https://www.michalsons.com/blog/what-is-a-national-critical-information-infrastructure/17701

10. Fazinni, K. (2019, January 14). *How the Government Shutdown is Putting Cybersecurity at Risk.* Retrieved from CNBC: https://www.cnbc.com/2019/01/14/government-shutdown-putting-national-cybersecurity-at-risk.html

11. Fidler, D. (2019, January 2). *Year in Review: Cyber Threats and the Mid-Term U.S. Elections*. Retrieved from Council on Foreign Relations: https://www.cfr.org/blog/year-review-cyber-threats-and-mid-term-us-elections

12. Fruhlinger, J. (2017, August 22). *What is Stuxnet, who created it and how does it work?* Retrieved from CSO: https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

13. Graham, W., Pry, P. (2018, October 16). *Ignoring EMP threat is a death sentence for Americans*. The Hill. https://thehill.com/opinion/cybersecurity/411451-ignoring-emp-threat-is-a-death-sentence-for-americans

14. Healthcare & Public Health Sector Coordinating Councils. (2018). *Health Industry Cybersecurity Practices.*

15. Huffman, M. (2018, April 17). *Survey finds increasing level of consumer concern about privacy protection*. Retrieved from Consumer Affairs: https://www.consumeraffairs.com/news/survey-finds-increasing-level-of-consumer-concern-about-privacy-protection-041718.html

16. Information Security Forum. (2019). *Threat Horizon 2021*. ISF.

17. Kaplan, R. D. (2019, January 7). *A New Cold War Has Begun*. Retrieved from Foreign Policy: https://foreignpolicy.com/2019/01/07/a-new-cold-war-has-begun/

18. Lipton, E., Sanger, D., and Shane, S. (2016, December 14). *How Russian Hackers Hijacked the US Election*. The Irish Times. https://www.irishtimes.com/news/world/us/how-russian-hackers-hijacked-the-us-election-1.2905839.

19. Liwer, D. (2019, January 16). *Voices: It's time for the federal government to incentivize cybersecurity*. Accounting Today. https://www.accountingtoday.com/opinion/its-time-for-the-federal-government-to-incentivize-cybersecurity

20. Maryland Department of Commerce. (n.d.). *Buy Maryland Cybersecurity (BMC) Tax Credit*. Retrieved from Maryland.gov: http://commerce.maryland.gov/fund/programs-for-businesses/buy-maryland-cybersecurity-tax-credit

21. McKew, M. (2018, February 16). *Did Russia Affect the 2016 Election? It's Now Undeniable*. Retrieved from Wired: https://www.wired.com/story/did-russia-affect-the-2016-election-its-now-undeniable/

22. Mikolic-Torreira, I., Henry, R., Snyder, D., Beaghley, S., Pettyjohn, S. L., Harting, S., . . . Weinbaum, C. (2016). *A Framework for Exploring Cybersecurity Policy Option.* Santa Monica: RAND.

23. National Research Council. (2017). *At the Nexus of Cybersecurity and Public Policy.* Washington, DC: The National Academic Press.

24. Organisation for Economic Co-Operation and Development. (2012). *Cybersecurity Policy Making at a Turning Point.*

25. Richardson, R. (2018, February 19). *UC cybersecurity expert to Senate subcommittee: U.S. midterm elections at high risk for cyberattacks.* University of Cincinnati. https://magazine.uc.edu/editors_picks/recent_features/harknett_cybersecurity.html

26. Palmer, D. (2019, January 16). *Cyber Security: This Giant Blind Spot Will Cost Us Dear*. Retrieved from ZDNET: https://www.zdnet.com/article/cyber-security-this-giant-blind-spot-will-cost-us-dear/

27. Perloth, N., & Rosenberg, M. (2019, June 6). Election Rules Are an Obstacle to Cybersecurity of Presidential Campaigns.

28. Pry, D. P. (2017). *Nuclear EMP Attack Scenarios and Combined-Arms Cyber Warfare.* Report to the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack.

29. Sanger, D. E. (2018). *Cyber Strategy.* New York City: Crown Publishing.

30. Sivan-Sevilla, G. S. (2018). The Role of the State in the Private-Sector Cybersecurity Challenge. *Georgetown Journal of International Affairs*.

31. Stampler, L. (2019, January 16). *Government Shutdown Puts U.S. at Major Hacking Risk, Cybersecurity Experts Warn*. Retrieved from Forbes: http://fortune.com/2019/01/16/cybersecurity-hacking-government-shutdown/

32. Subcommittee on Cybersecurity, Science, and Research and Development. (2004). *Cybersecurity for the Homeland.*

33. Thielman, S. (2015, October 27). *Senate passes Controversial Cybersecurity Bill CISA 74 to 21*. Retrieved from The Guardian: https://www.theguardian.com/world/2015/oct/27/cisa-cybersecurity-bill-senate-vote

34. Tumbler, R. (2019, January 12). *3 Compelling Reasons To Invest In Cyber Security - Part 1*. Retrieved from Forbes: https://www.forbes.com/sites/rajindertumber/2019/01/12/3-compelling-reasons-to-invest-in-cyber-security-part-1/#7e12ed426df6

35. Tumbler, R. (2019, January 16). *3 Compelling Reasons to Invest in Cyber Security - Part 2*. Retrieved from Forbes: https://www.forbes.com/sites/rajindertumber/2019/01/16/3-compelling-reasons-to-invest-in-cyber-security-part-2/#3fe48fb016df

36. U.S. Department of Homeland Security. (2018). *Cybersecurity Strategy.* Washington D.C.

37. United States Government Accountability Office. (2019, March). *High-Risk Series.* Retrieved from https://www.gao.gov/assets/700/697245.pdf

38. University of San Diego. (n.d.). *Top Cyber Security Threats in 2019*. Retrieved from University of San Diego: https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

39. Valeriano, B., & Maness, R. C. (2015). *Cyber War versus Cyber Realities.* New York City: Oxford University Press.

40. Valeriano, B., Jensen, B., & Maness, R. C. (2018). *Cyber Strategy.* New York City: Oxford University Press.

41. Vincent, W. R. (2018, October 16). *Ignoring EMP threat is a death sentence for Americans*. Retrieved from The Hill: https://thehill.com/opinion/cybersecurity/411451-ignoring-emp-threat-is-a-death-sentence-for-americans

42. Weintraub, R., Borenstein, J. (2017, June 1). *11 Things the Health Care Sector Must Do to Improve Cybersecurity*. Harvard Business Review. https://hbr.org/2017/06/11-things-the-health-care-sector-must-do-to-improve-cybersecurity

43. Wheeler, T. (2018, September 12). *In Cyberwar, There are No Rules*. Retrieved from Foreign Policy: https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/

44. Wheeler, T. (2018, September 12). In Cyberwar, There are No Rules. *Foreign Policy*. Retrieved from Foreign Policy.

Potential Topic Paragraph

Cybersecurity has never before been as large of a threat or received as much coverage as it has since the 2016 Presidential election, in which Russia used disinformation campaigns and hacking to sow discord and destroy confidence in our institutions. Soon after that election, the Cambridge Analytica scandal rocked Facebook, then Yahoo and Marriott were hacked and millions (billions in Yahoo's case) of people were affected. A 2018 survey by Harris Poll finds that "78 percent of U.S. consumers believe a company's ability to protect user data is "extremely important" and only 20 percent now "completely trust" organizations to protect their data. The survey also showed that more people are concerned about cybersecurity than they are about America going to war.

There has never been a better time to have a cybersecurity topic. The 2020 election will provide a huge array of literature on the topic right in the middle of the season, ensuring quality evidence and sparking conversations in other cybersecurity areas of concern.

Potential Resolution Wordings

1. The United States federal government should substantially increase cybersecurity infrastructure incentives in the United States.
2. The United States federal government should substantially increase its cybersecurity investment for the United States government.
3. The United States federal government should substantially increase its election security investment in the United States.
4. The United States federal government should substantially increase its management and oversight of civilian cybersecurity infrastructure in the United States.
5. The federal government should substantially increase its cybersecurity standards for the protection of critical infrastructures in the United States.