RETHINKING THE GOVERNMENT'S ROLE IN PRIVATE SECTOR CYBERSECURITY

Devon H. Draker

RETHINKING THE GOVERNMENT'S ROLE IN PRIVATE SECTOR CYBERSECURITY

Devon H. Draker*

ABSTRACT

Cyber-attacks on the private sector through the theft of trade secrets and ransomware attacks threaten US interests at a federal level by undermining US economic competitiveness and funding groups with interests adverse to those of the US. The federal government can regulate cyberspace under the Commerce Clause, but the current cybersecurity regulatory landscape is ineffective in addressing these harms. It is ineffective because legislation is either bad-actor focused and punishes the proverbial "hacker," which has no teeth due to jurisdictional reach limitations, or because it attempts to punish the victim-company in hopes of motivating the development of sufficient safeguards. The missing puzzle piece in solving this issue is "intelligence." Intelligence in military terms is the process of combining information to create an actionable plan that anticipates what the enemy will do based on operational factors. The utility of intelligence in cyberspace is that it provides companies the ability to anticipate not only when they may be attacked based on trends in their sector, but also what methods would likely be used to carry out the attack. There are two ways that cybersecurity intelligence could be achieved. The first approach involves integrating cybersecurity units from the United States Military into the private sector to collect information on attacks and provide intelligence to private sector companies based on this information gathering. This approach also allows the US Military to continue its proficiency in the cyberspace domain, which is a rising concern for US military leaders. The second approach involves expanding the Cybersecurity and Infrastructure Security Agency's (CISA) regulatory powers to enact mandatory reporting regulations for more than just "critical infrastructure." Each approach has its own drawbacks, but both offer significant advantages as compared to the current regulatory landscape.

INTRODUCTION

Cybersecurity in the private sector has become the responsibility of private companies and not the US government, even when the threat is sometimes another nation-state. This means that nation-state actors who threaten US national security, are met only with resistance by what the individual companies implement for cybersecurity programs. Resulting in various cybersecurity readiness across the country. Companies' cybersecurity programs are based on a patchwork of regulatory frameworks depending on the sector they do business in. A company cannot effectively assess what specific threats may exist without the assistance and guidance of some intelligence agency that can conduct an intelligence analysis of current threats.

Cyber breaches are occurring at an alarming rate with each year seeing a greater number of attacks than the year before.[1] As the world continues to digitize and people become more

* J.D. Candidate, University of Maine School of Law, class of 2023. Devon is also an intelligence officer in the Maine Army National Guard.

[1] Lawrence J. Trautman and Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 U. MIA L. Rev. 761 (2018) (stating that cyber breaches continue at an alarming pace with

reliant on the internet , the US government needs to take more responsibility for developing readiness in the private sector to proactively respond to nation-state threats from abroad, rather than reactively relying on patchwork regulations to incentivize companies to implement their own sufficient programs. Cybersecurity measures should rest on the government, and the government must provide private companies more direct guidance to better protect national security as trends continue to demonstrate that cybersecurity is a nation-level vulnerability.[2]

In this paper, I will first explain why the US government must prioritize cybersecurity and how certain private sector harms resulting from cyber-attacks threaten national security and the public sector. Next, I will discuss how the current cybersecurity regulation landscape is ineffective in preventing harms from occurring. I will then provide an overview of why Congress has the authority to regulate cyberspace to address these harms. Finally, I will propose two recommendations for how the US government can better solve the national cybersecurity deficiencies through novel measures or through adjustments to existing frameworks and will discuss the drawbacks of each approach.

I. WHY THE US GOVERNMENT MUST PRIORITIZE CYBERSECURITY IN THE PRIVATE SECTOR

Cybersecurity harms are often thought of as synonymous with privacy harms in that the underlying harm is the invasion of privacy itself. While it is important for the US government to consider individual's loss of data, the US government must concern itself with not only protecting individual privacy but more importantly protecting national security. Cybersecurity threats and the data that nation-state actors are attempting to steal pose greater risks to the US's national security than the invasion of individual privacy. Two specific harms that cybersecurity threats pose to the US is the use of ransomware to fund campaigns against US interests and the theft of trade secrets to undermine US competitiveness in the global market.

a. Nation States Use Ransomware Attacks to Fund Campaigns to Undermine US Interests

Bad actors often employ ransomware which allows these actors to develop certain computer code, known as malware, that is designed to encrypt files stored on a given device. The malware is typically placed on a computer or device by means of a phishing campaign that targets employees with email links that automatically download the malware on the device once the link is accessed. Once the malware is planted, it encrypts the files on the machine or network. The bad actor will require some amount of payment, usually in bitcoin, to decrypt the files they encrypted. [3] Malicious actors may also delete entire system backups, if their malware is capable, to further extort the victim of these ransomware attacks more effectively. As part of the

---

new vulnerability warnings being a daily occurrence and estimating that over 30 billion Internet of Things (IoT) devices will soon exist, increasing vulnerabilities).

[2] The White House, *Executive Order--Improving Critical Infrastructure Cybersecurity* (2013), *(https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity)*(in 2013, an Obama Administration Executive Order acknowledged that cybersecurity is one of the biggest threats to national security).

[3]Cybersecurity & Infrastructure Security Agency, *Ransomware Guide* (2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf.

extortion, the attacker may even threaten to release the information publicly if the victim company does not pay the ransom to have the information decrypted.[4]

In May of 2017, the WannaCry 2.0 ransomware infected hundreds of thousands of systems worldwide.[5] The malware spread to around 300,000 computers across 150 nations and caused billions of dollars in damage not just in the public sector, but the private sector as well.[6] The malware was designed to automatically encrypt the files on target machines and require a payment of $300 in bitcoin. If the ransom amount was not paid within a couple of days, the amount would double. If after around a week payment was not received, all the files being held for ransom would automatically be deleted. This attack was performed by North Korean nationals and is an example of a nation-state actor that is not only causing billions of dollars in damage but also receiving payments from US organizations and citizens to fund North Korean government interests. Additionally, three North Korean-backed hacker groups, known by the names Labyrinth Chollima, Stardust Chollima, and Velvet Chollima, also deployed malicious cryptocurrency applications to generate revenue. [7]

Ransomware has become increasingly popular as a method of attack since the Covid-19 pandemic, which prompted more private companies to shift their work to a remote format.[8] This remote work created an unprecedented opportunity for bad actors to attack key vulnerabilities where companies' employees began accessing networks from their home devices. In fact, during the first year of the Covid-19 pandemic, the FBI reported a 37% annual increase in ransomware attacks and a 147% increase in annual losses due to ransomware attacks in the private sector.[9] Employees unfamiliar with working remotely can be easy targets of phishing attacks and weak remote access authentication are both explanations for the rise in ransomware attacks since the Covid-19 pandemic.[10]

Ransomware has become a valuable low-cost tool for nation-states to employ against the US with the intent of generating revenue as well as causing disruption of services. The payment of these ransoms threatens national security interests as it enables criminals and adversaries to profit and advance their aims against the US.[11] With these threats in mind, the Office of Foreign Assets Control (OFAC) designated malicious cyber actors, and the payment of a ransom to any

---

[4] Dep't of the Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

[5] Dep't of Justice, *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*, Office of Public Affairs (Sep. 6, 2018), https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

[6] BBC, *Cyber-attack: US and UK blame North Korea for WannaCry* (Dec.19, 2017), https://www.bbc.com/news/world-us-canada-42407488.

[7] Crowdstrike, *2021 Global threat Report,* 45 (2021), https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf.

[8] U.S. Bureau of Labor Statistics, *Telework during the COVID-19 pandemic: estimates using the 2021 Business Response Survey*, Monthly Labor Review (Mar. 2022), https://www.bls.gov/opub/mlr/2022/article/telework-during-the-covid-19-pandemic.htm (33 percent of establishments increased telework for some or all employees during the pandemic)

[9] Cybersecurity & Infrastructure Security Agency, *Ransomware Guide* (Oct. 1, 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf.

[10] Int'l Monetary Fund, *Cybersecurity of Remote Work During the Pandemic*, Monetary and Capital Markets, https://www.imf.org/-/media/Files/Publications/covid19-special-notes/en-special-series-on-covid-19-cybersecurity-of-remote-work-during-pandemic.ashx.

[11] Dep't of the Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

of these designated groups could render civilians or private sector companies civilly liable. However, the OFAC's policy does not prevent payment of all ransom payments, just payments made to those designated by OFAC. The problem with this approach is that not all cyber actors are identified when the ransom payment is demanded and attribution of the source of attacks is challenging. The result is that while OFAC sanctions can prevent some ransomware harms, it is insufficient to effectively minimize the threat to national security that these ransomware attacks pose.

b. Nation State Actors Steal US Trade Secrets to Gain an Economic Advantage

Trade secrets are one of a corporation's most valuable assets.[12] However, they lack adequate protection under federal law, leaving them vulnerable to theft and misappropriation.[13] [14] As technology advances, it becomes easier and less time consuming for bad actors to steal trade secrets to a corporation's detriment.[15] The theft and misuse of trade secrets directly affects national security in two key ways. First, some trade secrets of government contractors contain classified information that could give the enemy a competitive edge in kinetic warfare.[16] Furthermore, trade secrets containing information that pertains to military technologies can endanger US and allied military personnel as trade secrets give an enemy the ability to understand US capabilities and develop countermeasures to US innovations. Second, trade secrets that aren't military in nature, can be misappropriated by nation-state actors and further developed or manufactured for lower cost.[17] This use directly impacts national competitiveness in a growing global market that is continuously more interconnected and interrelated. Aside from tariffs and other forms of political influence, the lack of jurisdictional reach into foreign countries makes theft of US trade secrets more valuable than the potential costs those nation-states face from engaging in this behavior.[18] This has incentivized one of the US's largest economic competitors: China.

---

[12] World Intellectual Property Organization, *Trade Secrets* https://www.wipo.int/tradesecrets/en/ (last visited Nov. 12, 2022).

[13] Defend Trade Secrets Act of 2016, S.1890, 114th Cong. (2016), https://www.congress.gov/bill/114th-congress/senate-bill/1890 (Congress passed the Defend Trade Secrets Act (DTSA) in 2016 which provides a civil cause of action for victims of trade secret espionage or theft. The problem is that this Act suffers the same jurisdictional governance issues as many other laws when it comes to foreign nation attackers).

[14] Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-1839 (1996)(criminalizing the theft of trade secrets as a felony. The punishments for violating the EEA are a potential 10-year imprisonment and $250,000 penalty. However, this Act falls victim to the same issues as more traditional cybersecurity laws, which is that the inability to enforce this against individual foreign nationals who are often backed by foreign governments to conduct these attacks, means that there is no disincentive for nation states to stop stealing US trade secrets aside from foreign relations pressures).

[15] Alissa Cardillo, *Another Bite at the Apple for Trade Secret Protection: Why Stronger Federal Laws Are Needed to Protect a Corporation's Most Valuable Property*, 10 Brook. J. Corp. Fin. & Com. L. (2016).

[16] Federation of American Scientists, *Appendix A. Classification of Information Principles and Trade Secret Law* (Apr. 1993), https://sgp.fas.org/library/quist2/app_a.html.

[17] David Orozco, *Amending the Economic Espionage Act to Require the Disclosure of National Security-Related Technology Thefts*, 62 Cath. U. L. Rev. 877 (2013).

[18] Patricia Bellia, *Cyberlaw Problems of Policy and Jurisprudence in the Information Age*, 71 (5th ed. 2018).

China is the largest threat to US cyberspace and national security in the realm of stealing trade secrets.[19] In August of 2019 and August of 2020, the DOJ identified several Chinese nationals responsible for attacks on over 100 victim companies' computers in the US and abroad, including software development companies, computer hardware manufacturers, social media companies, video game companies, non-profits, think tanks, and others. These nationals were a part of a group known as "Wicked Panda," a group notorious for facilitating the theft of source code and other trade secrets.[20] In 2019, Chinese-backed hackers targeted pharmaceutical and aerospace sectors to steal blueprints for producing materials in those given sectors. [21] In 2020, four Chinese nationals working in connection with the Chinese Ministry of State Security, were charged by the U.S. with a global computer intrusion campaign targeting intellectual property and confidential business information, which included infectious disease research. [22] This corroborates the 2015 plan China made to "achieve economic dominance by 2025," which stated China's call for advancements in manufacturing in the aerospace and biomedical fields. The 2015 economic dominance plan and recent attacks on private sectors in the US demonstrate China's efforts to achieve this end-state of economic dominance by stealing the intellectual property of US companies to degrade the US's economic competitiveness.

China's share in the market of trade secret theft is so significant that 80% of all economic espionage prosecutions involve conduct that would benefit China, and China is involved in 60% of all trade secret theft cases in its entirety. [23] The targeting of US companies with ransomware by enemy nation-states like China, North Korea, and Iran constitutes an attempt to use the US economy to fund activities counter to US economic and security interests. More specifically, China's theft of US trade secrets poses a significant competitive economic risk to the US in the global market. For these reasons, the US government must address the national security risks that the current cybersecurity posture of the private sector poses.

II. THE CURRENT CYBERSECURITY REGULATIONS ARE INEFFECTIVE AT PREVENTING CYBER RISKS TO NATIONAL SECURITY

---

[19] Greenberg Traurig Law, *DOJ's 'China Initiative' Focuses on Trade Secret Theft, Shows No Signs of Slowing Down in the Biden Administration* (Jun. 9, 2022), https://www.gtlaw.com/en/insights/2021/6/dojs-china-initiative-trade-secret-theft-biden-administration(stating that China is largest threat to US cyberspace evidenced by the Trump administration's "China Initiative" which focused on ensuring enough resources were dedicated to resolving trade secret theft cases involving China. Also, that 80% of all economic espionage prosecutions by DOJ would benefit the Chinese state in some way).

[20] Dep't of Justice, *Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally*, Office of Public Affairs (Sep. 16, 2020), https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

[21] Sean Lyngaas, *Chinese hackers cast wide net for trade secrets in US, Europe and Asia, researchers say*, CNN (May 4, 2022), https://www.cnn.com/2022/05/04/politics/china-hackers-economic-espionage-manufacturing/index.html.

[22] Dep't of Justice, *Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research*, Office of Public Affairs (Jul. 19, 2021), https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.

[23] Dep't of Justice, *Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018*, Nat'l Security Division (Nov. 19, 2021), https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related#:~:text=About%2080%20percent%20of%20all,all%20trade%20secret%20theft%20cases.

Cybersecurity regulations can be categorized based on the desired outcome. Cybersecurity laws are either victim-centered or perpetrator-centered depending on who the law seeks to punish. [24] Over the past 30 years, cybersecurity laws have evolved to a hybrid between victim-centered and perpetrator-centered, but the key distinction is that these laws have shifted away from treating the hacker as the perpetrator. The US initially attempted to use the Computer Fraud and Abuse Act and the Stored Communications Act to prevent these harms by punishing the bad actor, but began to realize that a great deal of cyber-attacks were taking place by actors who were outside of the jurisdiction of US courts.[25] [26] Now, the laws are acknowledging that the covered entity is the perpetrator due to the victim company not implementing strong enough cybersecurity programs to prevent the harm from occurring initially.[27] This is likely the result of difficulty stemming from the enforcement of perpetrator(hacker)-centered laws because often the bad actor lives outside the US and is likely a foreign-national, jurisdictionally limiting the US's enforcement of these laws. The resulting shift in the focus of cybersecurity laws, thus, highlights the underlying tension of trying to solve this problem, which is preventing these harms from occurring within the US.

a. Sector-Specific Cybersecurity Regulations

The Federal Trade Commission ("FTC") is authorized under the Unfair and Deceptive Trade Practices Act to regulate cybersecurity measures implemented by for-profit organizations. The Unfair and Deceptive Trade Practices Act prohibits unfair or deceptive acts or practices in or affecting commerce.[28] Section 45(a)(4)(A) of the Act provides that the term "unfair trade practices" includes acts that are likely to cause substantial injury to consumers, cannot be reasonably avoided, and is not outweighed by countervailing benefits.[29] Deceptive trade practices is where there is a representation or omission that is likely to mislead the consumer and their interpretation was reasonable.[30] In the absence of comprehensive privacy or cybersecurity legislation, the FTC has used this authority to create [31] If the FTC determines that a company is engaging in an unfair or deceptive practice, the FTC will draft a consent decree, prescribing certain requirements that the company must meet while being subject to recurring audits. If a company enters into a consent decree with the FTC, they are essentially able to circumvent an admission of fault by agreeing to make changes specified by the FTC. [32] If a company refuses to enter into a consent decree or enters into a consent decree and later violates it, the FTC may commence an action against the company. [33]

The Health Insurance Portability and Accountability Act (HIPAA) is considered one of the more mature sectoral cybersecurity regulations enacted in the US. Under the HIPAA Security

---

[24] Carol M. Hayes, *Comparative Analysis of Data Breach Laws: Comprehension, Interpretation, and External Sources of Legislative Text*, 23 Lewis & Clark L. Rev. 1221 (2020).
[25] 18 U.S.C. § 1030.
[26] *Id*. § 2701.
[27] *Id*.
[28] 15 U.S.C § 45.
[29] *Id*.
[30] 15 U.S.C § 45.
[31] Federal Trade Commission, *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority* (May 2021), https://www.ftc.gov/about-ftc/mission/enforcement-authority.
[32] *Id*.
[33] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

Rule, for example, covered entities must protect personally identifiable information against any reasonably anticipated threats or hazards to the security or integrity of that information.[34] The rule allows covered entities to employ any security measures that reasonably and appropriately protect information and enable covered entities to determine which measures are feasible to implement based on an entity's size, complexity, and capabilities. The rule additionally prescribes specific administrative, physical, and technical safeguards that must be implemented, such as data backup plans, information system activity reviews, and unique user identification.[35] The Office of Civil Rights (OCR) is an agency that is responsible for enforcing both the HIPAA Privacy and HIPAA Security rules. When the OCR finds indications of noncompliance due to willful neglect or when the nature and scope of the noncompliance warrants additional enforcement action, the OCR pursues a resolution agreement with a payment of a settlement amount and an obligation to complete a corrective action plan (CAP).[36] In 2020 alone, the OCR received 27,000 complaints, which was a 4% decrease from the previous year.[37]

The Gramm-Leach Bliley Act (GLBA) is another long-standing US regulation that applies to a specific sector: the financial sector. The GLBA seeks to protect financial information, thus preventing ransomware attacks protects against unauthorized access to financial information. In 2021, more than half of all financial service firms were targeted by a ransomware attack at least once, a 34% increase from the prior year.[38] The high rate of ransomware attacks on financial service firms is clear evidence that the provisions of the GLBA Safeguards Rule, which requires a "reasonable information security program," is insufficient on its own to prevent ransomware attacks from occurring.[39] [40]

Regulations like HIPAA and GLBA often promote compliance after the fact. The regulators impose fines for non-compliance and, accordingly, can be considered reactive, not proactive.[41] While these regulations have certainly improved the cybersecurity hygiene of private companies, bad actors have become more sophisticated and can outpace the reactive nature of current cybersecurity regulations. Furthermore, these regulations pose three primary issues for preventing cyber-attacks. First, the regulations generally require companies to implement "reasonable cybersecurity measures." The definition of what is "reasonable" can often be difficult for organizations to determine. If the regulation does not require "reasonable cybersecurity measures" to be implemented, then it is likely a descriptive regulation that

---

[34] 45 CFR § 164.306.

[35] 45 CFR §§ 164.308 - 164.312

[36] Dep't of Health & Human Services, *Enforcement Process* (last visited Nov. 28, 2022), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html

[37] Off. of Civil Rights, *Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance*, 2 (2020), https://www.hhs.gov/sites/default/files/compliance-report-to-congress-2020.pdf

[38] Sophos, *The State of Ransomware in Financial Services 2022*, 3 (Aug. 2022), https://assets.sophos.com/X24WTUEQ/at/29t7bmfvtz659x8xj86wfggb/sophos-state-of-ransomware-financial-2022-wp.pdf.

[39] 16 C.F.R. § 314.4.

[40] Nine Safeguards Rule Elements: designate a qualified individual to implement and supervise information security program, conduct a risk assessment, design and implement safeguards to control risks identified, regularly monitor and test effectiveness of your safeguards, train your staff, monitor your service providers, keep your information security program current, create a written incident response plan, require your qualified individual to report to your Board of Directors.

[41] Carol Li, *A Repeated Call for Omnibus Federal Cybersecurity Law*, 94 NOTRE DAME L. REV. 2211, 2228 (2019).

specifically outlines the cybersecurity measures to be implemented.[42] This specificity subjects the company to rigid regulatory requirements that cannot adapt to new and developing cybersecurity threats.

Second, punitive incentives are relatively non-existent with FTC consent decrees and corrective action plans. While the onus is placed on the organization to implement these reasonable measures, significant fines are not imposed by private sector regulators unless the company violates the consent decree or corrective action plan. In essence, companies have little incentive, other than avoiding regulatory oversight in a consent decree, to implement reasonable measures in the first place. Furthermore, many organizations do not consider cybersecurity until they have been attacked, and at that point they may become subject to a consent decree which could easily become outdated and ineffective at preventing sophisticated nation-state cyber-attacks within a few years.[43] Lastly, even companies that have achieved compliance may still be vulnerable to cyber breaches in many scenarios.[44] Companies who are compliant with regulations still experience breaches, which begs the question of how effective these regulations are. For example, in 2013 Target experienced a breach two-months after the company was deemed compliant with payment card industry standards.[45] Regardless of whether companies treat cybersecurity as a check-the-box compliance or a continuously evolving requirement, it is often not enough to prevent these cyber harms from occurring.[46] For these reasons, sector-specific cybersecurity regulations are ineffective at preventing the threats to national security that nation-state actors pose.

b. National Policy Directives

In 2018, the United States Cyber Command announced an operational concept known as "defend forward" that essentially acts as a policy recognition that there is a need to use offensive cyber measures to prevent the country from suffering attacks.[47] This was a policy extension from the April 2015 DoD CyberStrategy, which focused on protecting not only DoD systems but also the civilian and private sector networks. [48] Professor Kosseff of the Naval Academy, in assessing the international law implications of this strategy, concluded that the US would have leeway in its implementation, and that the defend forward strategy could result in the US taking more forward-leaning defensive cyber operations.[49] What Professor Kosseff did not consider in his

---

[42] *LabMD v. FTC*, 894 F.3d 1221 (11th Cir., 2018)(holding that the consent decree must be specific enough to give the party reasonable notice of what they must do to be compliant with the law under notions of due process of the law).

[43] Consent decrees last a decade or longer, thus they can easily become extremely outdated towards the end of the decree term.

[44] Christian Moldes, *Compliant but Not Secure: Why PCI-Certified Companies Are Being Breached*, J. Cyber Security & Info. Sys. (May 9, 2018), https://csiac.org/articles/compliant-but-not-secure-why-pci-certified-companies-are-being-breached/

[45] Carol Li, *A Repeated Call for Omnibus Federal Cybersecurity Law*, 94 NOTRE DAME L. REV. 2211, 2228 (2019).

[46] *Id.* at 2227.

[47] Eric Talbot Jensen and Sean Watts, *Due Diligence and the US Defend Forward Cyber Strategy*, Hoover Working Group on National Security, (Oct. 15, 2020), https://www.lawfareblog.com/due-diligence-and-us-defend-forward-cyber-strategy.

[48] Jeff Kosseff, *The Contours of Defend Forward Under International Law*, United States Naval Academy, 3 (2019), https://ccdcoe.org/uploads/2019/06/Art_17_The-Contours-of-Defend-Forward.pdf

[49] *Id*. at 5.

paper, however, is the negative impact that the "defend forward" strategy will likely have on the US. The US, by establishing a defensive cyber strategy that is premised on offensive operations and sounded in international law, merely creates a justification for the US's enemies to implement similar policies under the same international law. If anything, utilizing this international law framework to justify purportedly offensive cyber operations will only increase the frequency of overall cyberattacks as other nations adopt a similar interpretation. Furthermore, this policy creates ambiguity around which cyberattacks are considered offensive or are used only for the purpose of "defending forward," perpetuating retortion. The "defend forward" strategy is unlikely to reduce private-sector attacks and, if anything, is likely to lead to an increase in the harms previously identified.

Congress established the National Institute of Standards and Technology (NIST) as an agency to develop standards for technological inventions. Most relevant to the field of cybersecurity is the NIST Cybersecurity Framework, a voluntary cybersecurity framework that provides standards, guidelines, and best practices to manage cybersecurity and reduce risk within an organization.[50] The framework is frequently updated and is regarded as a strong foundation for any organization to utilize.[51] The framework focuses on five key principles with respect to cyberattacks: identify, protect, detect, respond, and recover.[52] Furthermore, while most cybersecurity regulations are relatively vague in their requirements, the NIST framework provides descriptive measures for organizations to implement. However, use of this framework is primarily required for government agencies and is not currently required for private sector companies.

In 2013, pursuant to Executive Order 13636, President Obama directed NIST to develop the Cybersecurity framework primarily to reduce cyber risks to critical infrastructure. In Presidential Policy Directive 21 (PPD-21), President Obama split the critical infrastructure designation into 16 discrete sectors.[53] In 2015, Congress passed the Cybersecurity Act of 2015, which created an information sharing framework to help promote the US's ability to defend against cybersecurity attacks.[54] The most notable feature of the information sharing network was its reliance on voluntary participation." This voluntary participation feature was seen as one of the biggest drawbacks of the Act.[55] Because participation was voluntary, very few critical infrastructure operators participated. And, since widespread participation is necessary to increase the relevance of the information shared by the Cybersecurity and Infrastructure Security Agency (CISA), it became apparent to critical infrastructure operators that it'" was not worth the costs to engage with this framework.

---

[50] Robert M. Chesney, *Chesney on Cybersecurity Law, Policy, and Institutions*, University of Texas, 173 (Aug. 23, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547103.

[51] Federal Trade Comm'n, *Understanding the NIST Cybersecurity Framework*, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

[52] NAT'L INST. OF STANDARDS AND TECH., *Cybersecurity Framework*, https://www.nist.gov/cyberframework.

[53] Chemical Sector; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors and Waste; Transportation Systems; Water and Wastewater.

[54] Cyber Security Information Sharing Act of 2015, S.754, 114th Cong. (2015).

[55] Robert M. Chesney, *Chesney on Cybersecurity Law, Policy, and Institutions*, University of Texas, 178 (Aug. 23, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547103.

In response to the shortcomings of the 2015 Act, Congress signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 into law.[56] The Act requires covered entities operating in the critical infrastructure sectors to report cyber incidents within 72 hours and ransom payments within 24 hours.[57] This mandatory reporting is a step in the right direction towards improving the nation's cybersecurity defensiveness against sophisticated attacks. While the Act does require private sector companies to report relevant cybersecurity information, it still misses a large portion of the country's private sector and leaves the US's overall cyber readiness diminished. Unless there is a change in the way critical infrastructure is defined to include more companies in the private sector, the NIST framework and CISA mandatory reporting framework will continue to fail to solve the nation's cybersecurity problem.

The sector-specific cybersecurity regulations and national policy directives have all been ineffective at preventing these harms in fundamental ways. Due to their failure and the rising threat that foreign nation-states pose to US national security in the form of ransomware and theft of trade secrets, the US government must reimagine the way it regulates cyber risks.

III. CONGRESS HAS THE AUTHORITY TO FEDERALLY REGULATE CYBERSPACE UNDER THE COMMERCE CLAUSE

The Commerce Clause grants Congress the power to regulate commerce with foreign nations, and among the several states.[58] The Commerce Clause has been used broadly to regulate numerous interstate activities and even some activities that may not be inherently thought of as interstate but happen to "affect" interstate commerce. Congress has used its Commerce Clause authority to regulate new "spaces" in the past, including airspace. For example, before the passing of the Air Commerce Act (ACA) in 1926, pilots would fly 500 feet from the ground and use roads to guide their direction, and because of what is considered dangerous travel practices today, fatal plane accidents were commonplace. Aviation industry leaders, with the help of Congress, sought to improve safety standards across the country to help the commercial travel industry take-off, and the ACA was enacted.[59] The legislation charged the Secretary of Commerce with establishing air traffic rules, pilot licensure requirements, and operating and maintaining aids to air navigation. Then, in 1958, President Eisenhower signed the Federal Aviation Act that created a new federal agency responsible for civil aviation safety. President Eisenhower, in signing the Act, believed that a single department was needed to aid in the development of industry standards and provide and ensure safety at all airports. Nearly a decade later, Department of Transportation ("DOT"), became fully operational on April l, 1967. On that day, the Federal Aviation Agency became one of several modal organizations within the DOT and received a new name, the Federal Aviation Administration (FAA). Additionally, the Federal government began employing armed guards and border patrolmen recruited from the U.S. Immigration and Naturalization Service on civilian planes to ensure safety on flights.

The history of cyberspace is similar to that of airspace but without federal agency oversight. The harms caused by cyberspace being relatively unregulated are preventable, much

---

[56] Cyber Incident Reporting for Critical Infrastructure Act of 2021, H.R. 5440, 117th Cong. (2022).
[57] *Id*.
[58] U.S. Const. art I, § 8, cl. 3.
[59] Federal Aviation Adm., *A Brief History of the FAA*, Dept. of Transportation (last visited Dec. 1, 2022), https://www.faa.gov/about/history/brief_history#:~:text=This%20new%20Department%20of%20Transportation,Federal%20Aviation%20Administration%20(%20FAA%20).

like the harms in civil air travel were preventable by consolidated and industry-level standards being established and enforced by one authority. Imagine the harms that would be perpetuated by a confederate approach to regulating air travel. It is in the consumer's best interest that the standard of care exercised at airports is relatively similar when traveling between states. This comfort in knowing these standards that airports are held to are found within all states in the country is analogous to the comfort individuals would likely want to experience with their data in cyberspace.

The potential concern of federalist innovation being undermined by a federal approach to cybersecurity regulation is not found in history. The current cybersecurity regulation landscape is the result of experimentation in letting states fill in the holes left by industry-specific federal regulations with their own privacy laws.[60] This has resulted in a landscape of cybersecurity where compliance is difficult and minimum compliance or "check the box compliance," rather than holistic security, is incentivized. [61] With each passing year, the call for a federal answer to the nation's cybersecurity problem becomes more persuasive to lawmakers, as evidenced by Congress' consideration of passing new laws such as the American Data Privacy Protection Act (ADPPA). [62] The next step is to determine how to specifically utilize Congress' Commerce Clause authority to address cybersecurity deficiencies.

IV. HOW THE GOVERNMENT SHOULD HELP SOLVE THIS PROBLEM

Individual companies have an interest in preventing cyber-attacks from taking place, but they need relevant threat intelligence to help properly respond to increasingly sophisticated attacks. Threat intelligence is the missing puzzle piece to solving the nation's cybersecurity problem that cybersecurity regulations fail to address. There are two potential solutions to this deficiency, each with its own concerns, but these concerns are ameliorable. The first potential solution is to empower the United States Military to be responsible for defending US cyberspace, to include the private sector. The second potential solution is to expand the NIST framework and broaden the Cybersecurity Infrastructure Security Agency's (CISA) authority to enable more intelligence sharing in the private sector.

a. Empower the United States Military to be Responsible for Defending US Cyberspace and Preventing Cyberattacks by Foreign Nation States

The 9/11 attacks not only affected public entities, but it greatly affected private entities as well. [63] The response to the 9/11 attacks was not the assignment of blame or expectation of the private companies that suffered physical damages to have prevented the attacks because their property was privately owned. Rather, President Bush responded to the kinetic attack by utilizing the US Military.[64] Attacks from foreign nations in cyberspace should be treated similarly, and

---

[60] Carol Li, *A Repeated Call for Omnibus Federal Cybersecurity Law*, 94 NOTRE DAME L. REV. 2211, 2232 (2019).
[61] *Id.*
[62] American Data Privacy and Protection Act of 2022, H.R. 8152, 117th Cong. (2022).
[63] Mark Davis, *The Impact of 9/11 on Business*, Investopedia (Aug. 24, 2022), https://www.investopedia.com/financial-edge/0911/the-impact-of-september-11-on-business.aspx (Stating that after 9/11 stock markets nosedived and almost every sector of the economy was damaged for a short while).
[64] Nat'l Archives, *Global War on Terror*, George W. Bush Presidential Library and Museum (last visited Dec. 10, 2022), https://www.georgewbushlibrary.gov/research/topic-guides/global-war-terror.

the military should not be considered excluded from the discussion merely because the harms are taking place within privately owned organizations. Cyberspace is a new domain of the battlefield and should involve US military presence. The "Defend Forward" policy previously mentioned indicates that the government is interested in assuming a more proactive role in preventing cyber harms from occurring, but action beyond interest has been limited by the government's failure to suggest whether the military or a federal agency like the CIA/NSA/CISA would take the lead.

Relying on the US Military to prevent cyber harms involves some assumptions about the training level of the cyber specialist military occupational specialty ("MOS") and whether they can detect unauthorized breaches and employing defensive technical measures. A benefit of this approach is that personnel security offices in the military could vet Soldiers through the Office of Personnel Management to ensure that the Soldiers are cleared to handle classified information. This would grant them a security clearance, which is the military's way of saying that these individuals have the character and history of truthfulness to not release this sensitive information to unauthorized individuals.[65] Another benefit in leveraging the military to address the nation's cybersecurity problem is that it could also employ intelligence officers alongside cybersecurity specialists. Intelligence officers can critically analyze threats and assess vulnerabilities to determine when and where enemies will attack or threaten national security. These intelligence officers, paired with cybersecurity personnel, would be able to effectively map the cyber battlefield and assist in preempting attacks on private companies in the interest of protecting national security. The next step is determining how this approach would practically be carried out.

Congress has already tasked the Secretary of Defense with ensuring that all armed forces branches, such as the Army, Navy, and Air Force, are ready to conduct military cyber activities or operations in cyberspace to defend the United States and its allies, including in response to malicious cyber activity carried out against the United States by a foreign power.[66] The chain of command in the military at a high-level runs from the President to the Secretary of Defense, and then runs from the Secretary of Defense to the commander of a given specific combatant command. [67] The combatant commands receive their mission from the Secretary of Defense through its authority under Title 10. [68]

For example, the Army has already begun reorganizing and training cyber Soldiers. Army TRADOC is the command responsible for training Soldiers in their specific MOS. One of the newer MOS codes or job titles to be added in the Army is the Cyber Operations Specialist (17C). This is an enlisted Soldier who uses their cybersecurity skills to defend the Army's crucial and complex weapon systems, which includes satellites, navigation, and aviation systems against both foreign and domestic threats. To become a qualified 17C, Soldiers must undergo 10 weeks of Basic Training, 45 Weeks of Advanced Individual Training (AIT), and meet standardized test score requirements.[69] The skills learned at AIT include conducting defensive cyberspace

---

[65] Off. Of Personnel Mgmt, *Strategic Plan*, Mission Vision Values (last visited Dec. 12, 2022) https://www.opm.gov/about-us/strategic-plan/mission-vision-values/#:~:text=We%20are%20champions%20of%20talent,service%20to%20the%20American%20people.

[66] 10 U.S.C. § 394.

[67] 10 U.S.C. § 162.

[68] U.S. Cyber Cmnd., *Cyber 101: US Army Cyber Command*, Public Affairs (Nov. 30, 2022), https://www.cybercom.mil/Media/News/Article/3232195/cyber-101-us-army-cyber-command-arcyber/ (While there is a US Cyber Command and an Army Cyber Combatant Command, the missions of these are to defend and protect the cyber integrity of military and DOD systems only).

[69] Advanced Individual Training (AIT) is where enlisted Soldiers learn their specific MOS skills.

operations.[70] The Officer counterpart of a 17C is a 17A and is responsible for carrying out the operations in conjunction with an organized plan by targeting adversary activities and capabilities. [71] The mission statements found in Army Cyber Command, Department of the Army, and the job descriptions of the Soldiers set to become 17Cs do not reflect the need to defend critical infrastructure in the private sector like Title 10 USC Section 394 states. Cyber Operations Specialists train and fight to defend US Army systems, not the private sector. Employing these specialists in the private sector presents a unique opportunity to defend the US from foreign nation-state actor attacks where the nation remains vulnerable.

The foundation is already laid for the Army to take a more hands-on role in controlling cyberspace and preventing the national security risks that the country faces from inadequacies in the private sector. This is not a completely new branch of the military that requires a new TRADOC training program. TRADOC has already developed training to prepare these specialists for operating in the cyber realm, and with some modifications, this training could be transferred in the US private sector as well. With this in mind, Congress must authorize the Department of Defense to create more 17C and 17A positions within the Army and empower these Soldiers to aid the private sector in two varying approaches: The first would be to attach individual cyber Soldiers to each Battalion and assume responsibility of a geographic area that the Battalion operates within. The second approach would be to either establish new cybersecurity units or strengthen existing ones within each state's National Guard.

The first method for achieving this integration with the private sector, and likely the least disruptive to current Army organization, is to add 17C and 17A positions in each battalion in the U.S. Army where the 17As would lead the 17Cs in Cybersecurity Teams that fall under the chain of command of the battalion. The Army does this currently in other battalions where Soldiers are assigned to "Field Feeding Teams." Then, the Department of Defense and Secretary of the Army would need to create a Title 10 mission, which falls under the authority of Title 10 of USC, and tasks either the National Guard Bureau/Reserves ("NGB") or the Active Army with providing cyber assistance to certain geographic regions. At this point, there could be two additional branched courses of action. First, the Title 10 mission could activate only the individually qualified Soldiers (17C/17A). Second, the entire battalion could be tasked with the mission of providing cybersecurity support to a given region. There are drawbacks to both courses of action. Under the first approach, there could be fewer resources the cyber specialist would be able to leverage. Whereas under the second approach, the battalion may be spread too thin when considering other missions.

The second comprehensive approach is to task the Department of Defense, through the NGB, with establishing new cybersecurity units in each state. Under this approach, each state would be assessed based on the overall risk of cybersecurity attacks and the frequency of such attacks that the state faces. Based on that risk level, new cybersecurity units would be tasked with supporting the entire state, to include the private sector, by providing real-time intrusion detection. This approach would be more favorable than the first approach because it does not require adjusting the missions of already existing units. Moreover, the size and demand for these units would vary depending on the state that they are located in. For example, Maine's cybersecurity unit would be smaller than New York's.

---

[70] Army National Guard, *Cyber Operations Specialist* (last visited Dec. 14, 2022), https://www.nationalguard.com/17c-cyber-operations-specialist

[71] U.S. Army Recruiting, *MOS 17C Cyber Operations Specialist* (Jan. 23, 2018), https://www.youtube.com/watch?v=ev2j6KFZ-Ys

Having the National Guard defend cybersecurity at home aligns with its mission stateside. The Guard's mission is to maintain a deployable force that can assist overseas or at home.[72] For example, in defending the nation "at home," the Guard is frequently activated to support states in the event of natural disasters, such as Hurricane Katrina. These activations are coined Defense Support to Civil Authorities (DSCA).[73] During these activations, the Guard provides units that are flexible in responding to whatever needs the nation may have at a given moment. Activating the cybersecurity unit within each state to respond to civil cyber-attacks could easily be an extension of what is considered DSCA. An example of something like this type of mobilization took place recently in Maine.

In 2022, the Maine Army National Guard's Cybersecurity Team responded to a cyber-attack on its NATO State Sponsored Partner, Montenegro.[74] Maine deployed its cyber team to help Montenegro respond to this attack. While this was not a DSCA mission at home, it is an example of how these cybersecurity units can be integrated quickly and effectively. Furthermore, the cybersecurity units in each state could have an Intelligence Officer as well as their own Intelligence Analysts. These 35Ds and 35Fs, respectively, would provide the cybersecurity unit with their intelligence analysis on where the enemy may attack next and what indicators would show that planned attack. The role of these positions is to conduct Intelligence Preparation of the Battlefield (IPB), assessing real world impacts on the mission and to anticipating what the enemy will do next to negate their efforts.

The Army has an institutionalized history of intelligence analysis. Another benefit of this approach is that the Army has a great deal of access to relevant classified information and knows how to share it safely. While private companies have technically trained cybersecurity professionals, companies lack the necessary threat intelligence analysis to preemptively defend against certain attacks. These Soldiers can compile information and glean from it valuable information that can help prevent private sector cyber-attacks that would otherwise be unpreventable absent this necessary information. When Cyber Operations Specialists conduct anticipatory defensive measures based on the intelligence prepared by Intelligence Officers, the cybersecurity posture and national security of the U.S. improves drastically. It is for this reason that empowering already trained cybersecurity specialists and Intelligence Officers to assist the private section respond to threats against national security is an appealing approach to the nation's cybersecurity problem.

b. Expand the NIST Framework and CISA Authority Beyond Critical Infrastructures and Require All "At Risk" Organizations to Report Cyber-Attacks to CISA and Implement a Specific Tier of the NIST Framework

This approach is administratively easier to implement than the first approach. While there are private solutions, such as NetScout, these privatized intelligence solutions will always be steps behind the capability of the federal intelligence agencies due to their vast authority and

---

[72] *About the Guard*, NAT'L GUARD (last visited Feb. 6, 2023), https://www.nationalguard.mil/about-the-guard/#:~:text=The%20National%20Guard%20continues%20its,to%20protect%20life%20and%20property.

[73] LTG Daniel O'Donohue, *Defense Support to Civil Authorities*, JP-28 (Oct. 29, 2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_28.pdf.

[74] Predrag Milic, *FBI's team to investigate massive cyberattack in Montenegro*, ASSOCIATED PRESS (Aug. 31, 2022), https://apnews.com/article/russia-ukraine-technology-hacking-montenegro-2a8eb2df87f657b6d7b9971b7419bff9

reach under the Foreign Intelligence Surveillance Act (FISA).[75] In this way, requiring private companies to conduct their own threat analysis and intelligence collection on potential cyber-attacks is ineffective. The framework for intelligence and cyber threat information sharing has already been laid by the Obama Administration with CISA and Executive Order 13636, wherein Section 8 establishes this reporting framework as voluntary for the private sector but mandatory for federal agencies.

The Cybersecurity Enhancement Act of 2014 tasked NIST with developing a cybersecurity framework that could be flexible and adopted on a voluntary basis by critical infrastructures.[76] Then, under the Biden Administration, Executive Order 14028 was published providing that the federal government must partner with the private sector to help remove the barriers to sharing threat information to create a more effective information sharing environment.[77]

The federal government has been on the fence about how mandatory they want to make the reporting of cyber threat information. With the 2014 Cybersecurity Enhancement Act, reporting by private sector critical infrastructure was voluntary.[78] Then, the government took it one step further with the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Enactment of CIRCIA aims to improve America's cybersecurity environment by requiring CISA to develop and implement regulations requiring covered entities to report covered cyber incidents to CISA. This will allow CISA to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims. This is exactly what both the private sector and the nation need to better protect trade secrets and prevent the loss of data or the payment of ransomware to the nation's enemies.

Most organizations have developed some level of cybersecurity. Considering the holding in *FTC v. Wyndham*, though it may not be at the same baseline across the nation.[79] The problem with this baseline adoption of cybersecurity protocols is that bad actors are capable of adapting their methods of attack faster than companies can develop defenses because companies are operating in the dark without the necessary threat intelligence. Without intelligence on the enemy, it is almost impossible to prevent attacks. As mentioned with the military approach to solving the issue of a lack of actionable threat intelligence in cyber space, these Executive Orders and amendments empowering CISA are essentially attempting to create a federal cybersecurity intelligence agency that provides intelligence to companies within the private sector. The problem is that CISA can only force covered entities, being critical infrastructure entities, to report once the rulemaking process ends for CIRCIA. The critical infrastructure definition, which includes sixteen specific sectors, is not broad enough to effectively mitigate the risks and harms previously mentioned in Section II of this paper.

The CIRCIA must be further amended to fuse both the NIST framework for assessing organizational cybersecurity risk levels and CISA mandatory reporting to create a dynamic method of determining which organizations are at a higher risk of undermining national security if they suffer a cyber-attack and how likely they are to suffer a cyber-attack. Then, these

---

[75] NETSCOUT, *Omnibus ATLAS Intelligence Feed Product* (last visited Feb. 6 2023), https://www.netscout.com/product/omnis-atlas-intelligence-feed.

[76] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 297.

[77] Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021).

[78] Cybersecurity Enhancement Act, *supra* note 74.

[79] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

organizations must be required to implement a certain tier of the NIST cybersecurity framework as well as report attacks to CISA. The NIST framework already assesses organizations into different tiers ranging from 1-4, and these tiers reflect the rigor and sophistication of the organization in cybersecurity risk management practices, with tier 1 being "partial" and tier 4 being "adaptive."[8081] Due to the pervasiveness of cyber-attacks in the private sector, the CIRCIA must be amended to require all companies to conduct a self-assessment under the NIST framework to determine what tier they are in. This tiered approach, which is already in the NIST framework, can help include more information sharing through mandatory reporting than only requiring entities involved in critical infrastructure to engage in the NIST program and the CISA mandatory reporting requirement for cyber-attacks.[82]

For instance, an entity that is a tier 1 on the NIST framework but is a likely target for cyber-attacks due to it being a traditionally considered critical infrastructure should be required to implement the NIST framework guidelines and engage in mandatory reporting with CISA to better share necessary threat intelligence. On the other hand, a shoe cobbler business with three employees that is a tier 1 should not be forced to implement the NIST framework because a cyber-attack on this business poses little risk to national security. However, a biomedical company that patents, researches, and develops drugs that is a tier 2 in their cybersecurity under the NIST framework should be required to implement NIST and engage in mandatory reporting with CISA because the theft of those trade secrets poses a threat to national security by way of economic competitiveness. CISA would increase the cybersecurity readiness of companies that may not be deemed traditional critical infrastructure by forcing them to create a current implementation tier profile and a target profile, which helps them visualize how to progress to a higher tier of a cybersecurity program within the NIST framework.[83] This helps improve cybersecurity in a more modular and beneficial way than the current cybersecurity regulations.[84] To better assist this modular approach, the NIST Framework Core could be reworked to delineate the number of subcategories per function that an entity must implement to achieve a certain tier.[85] This would give private entities a better understanding of what requirements are necessary based on their risk profile tier.

Lastly, the mandatory reporting to CISA will help CISA develop better tailored guidance to companies at high risk of suffering an imminent attack. CISA will provide the cybersecurity teams of the organization with cyber threat intelligence to help them protect their information and systems. This threat intelligence is the product of intelligence analysis that is conducted by CISA with valuable information from companies across many sectors. The more companies that participate in this mandatory reporting, the more useful the intelligence output becomes.[86] This information can better ensure that threat intelligence is current and accurate as well as include predictions about which companies could suffer an attack next. With greater participation, CISA would be able to analyze threat patterns, trends, and tactics on a larger scale than are possible currently. This would enable intelligence output to become so advanced that it could be used to

---

[80] NAT'L INST. OF STANDARDS AND TECH., *Framework for Improving Critical Infrastructure Cybersecurity*, 9 (Apr. 16, 2018).

[81] Tier 1 is "Partial," Tier 2 is "Risk Informed," Tier 3 is "Repeatable," and Tier 4 is "Adaptive."

[82] NAT'L INST. OF STANDARDS AND TECH., *Framework for Improving Critical Infrastructure Cybersecurity*, 9 (Apr. 16, 2018).

[83] *Id*. at 4.

[84] *Id*. at 11.

[85] *Id*. at 24.

[86] This is often referred to as the "bad information input = bad intelligence output" concept.

provide an early warning to companies who could be targets for a potential attack and what attack methods are expected to be utilized by bad actors. From this, organizations can develop specifically tailored defensive measures for the anticipated attack, prevention that is vital to the success of organizations and the defense of national security. With the mandatory implementation of the NIST framework and mandatory reporting to CISA for those certain risk profile companies, the cybersecurity posture of the country would increase significantly.

c. Concerns with These Approaches

The first, concern with these approaches is the expansion of government and cost of implementation. These approaches would likely be expensive and cost substantial taxpayer dollars, whereas requiring individual companies to foot the bill means the consumers would not be paying the cost for cybersecurity protections. However, individual organizations are already shifting the costs of implementing current cybersecurity requirements onto the consumer by increasing the costs of goods and services. These approaches merely alter the exchange of the cost but should not result in an increased cost on consumers by way of taxes because, theoretically, the costs that companies forward onto consumers from resulting data breaches or third-party cyber intelligence should regress after the initial implementation of these approaches.

Another concern arising from the implementation of these approaches is increased government oversight and the possibility of a transition to a surveillance state. The era of Snowden and the NSA controversies created a heightened awareness of government surveillance and public resentment of a surveillance state with respect to intelligence agencies.[87] CISA or the military would likely be subject to no less controversy. Integrating cybersecurity units with private organizations or forcing information sharing by private companies with the federal government will create different privacy concerns. However, FISA still grants the government authority to surveil this type of data and activity because it concerns foreign actors abroad that are clearly threatening national security. Furthermore, information provided to CISA under the second approach could be scrubbed of all personal data or consist of only de-identified metadata as is currently required by CIRCIA. Anonymizing data or only reporting metadata could mitigate this concern.

The last concern associated with the implementation of these approaches is that these federal-level approaches could preclude company and state legislative innovation. While this is the classic federalism debate, the government can still leverage the creativity of the private-sector and employ them at a federal-level within CISA. For example, the NIST framework has become widely recognized as the standard for companies to implement and is itself the product of government innovation.[88] Additionally, the theory that government involvement eliminates all private sector innovation is over-exaggerated. Furthermore, society has accepted federal-level involvement in airspace travel; regulating the security of our personal data in cyberspace is analogous. Lastly, much of the current privacy and cybersecurity regulations have been left to

[87] Steven Aftergood, *Snowden Leak Prompted "Considerable Public Interest," Says FISA Court*, Federation of American Scientists (Sep. 13, 2013), https://fas.org/blogs/secrecy/2013/09/snowden-fisc/.

[88] Rebecca King, *Should government leave innovation to the private sector?*, World Economic Forum (Mar. 31, 2022), https://www.weforum.org/agenda/2022/03/should-government-leave-innovation-to-the-private-sector/ (stating that governments are often behind the private-sector with respect to innovation and can serve as an obstacle when it comes to market competition and consumer protection being tested by technological growth).

state innovation, but the resulting fragmented approach has degraded the cybersecurity posture of the nation.[89] A unified federal approach to this problem is a necessity.

CONCLUSION

The harm caused by foreign cyber-attacks against the U.S. private sector are matters of national security. Congress has the authority and responsibility to regulate cybersecurity more effectively. The current cybersecurity regulatory landscape does not incentivize or provide enough guidance to the private sector on how to prevent cyber-attacks effectively, as compliance does not equal prevention. The steps Congress has taken with the NIST framework and CISA framework certainly remediates the lack of a cohesive cybersecurity regulatory landscape, but these steps are short of providing the critical missing puzzle piece that is reliable private sector cybersecurity intelligence provided to companies at the first sign of a potential attack. If the government integrated U.S. Army cybersecurity specialists and intelligence officers with the private sector, these individuals could assist with coordinating cybersecurity governance in private sector companies by providing real-time valuable intelligence to the company's decisionmakers. The government could also utilize the existing frameworks of CISA and NIST to expand the mandatory reporting of relevant cybersecurity threat information and require implementation of a minimum NIST implementation tier to help prevent future attacks. Either approach by the government would increase the cybersecurity readiness of the private sector without imposing undue burdens and compliance requirements with difficult to interpret language.

[89] Carol Li, *A Repeated Call for Omnibus Federal Cybersecurity Law*, 94 NOTRE DAME L. REV. 2211, 2232 (2019).