The Public Sector's Responsibility to the Private Sector for a Secure Cyber Environment: A Framework to Create a Workable Private Sector Cybersecurity Defense

Andrew Jackson Coley*

* Andrew Jackson Coley is a graduate from the Catholic University of America, Columbus School of Law and a Federal Government Attorney.

INTRODUCTION

"Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace."[1]

The Department of Homeland Security's (DHS) mission to protect critical infrastructure and the private sector is one of the most significant and complex national security challenges in recent history. Some of DHS's recent obligations have been dealing with the Russian interference in the 2016 presidential election, frequently handling major data breaches of private institutions, tackling the national security risks posed by 5G networks, and sanctioning or banning 'private' international companies like Huawei that provide technical hardware.[2] In efforts to secure the United States's "daily life, economic vitality, and national security," the current administration and DHS have issued a number of cyber strategies and an executive order.[3]

Regardless of these strategies and new policy postures, there seems to be no significant effect on the cybersecurity of private sector institutions. For example, in 2018, Saks and Lord & Taylor were subject to data breaches affecting over 5 million credit and debit cards.[4] Facebook was subject to a breach affecting 29 million users, and Google to a breach affecting over 59.5 million users, both from breaches initially occurring in 2017 and 2015 respectively.[5] In 2015, the Office of Personnel Management, the office tasked with investigating and conducting security clearances for national security

[1] Cybersecurity, DEP'T OF HOMELAND SEC., https://www.dhs.gov/topic/cybersecurity.
[2] *See 2016 Presidential Campaign Hacking Fast Facts*, CNN (May 2, 2019), https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html; *see also* Klon Kitchen, *The U.S. Must Treat China as a National Security Threat to 5G Networks*, HERITAGE FOUND. (Apr. 16, 2019), https://www.heritage.org/technology/report/the-us-must-treat-china-national-security-threat-5g-networks.
[3] DEP'T OF HOMELAND SEC., *supra* note 1; *see also* WHITE HOUSE, NATIONAL CYBER STRATEGY OF THE UNITED STATES (2018) [hereinafter National Cyber Strategy]; *see also* WHITE HOUSE, PRESIDENT DONALD J. TRUMP IS STRENGTHENING AMERICA'S CYBERSECURITY (2018) [hereinafter Strengthening America's Cybersecurity].
[4] Paige Leskin, *The 21 Scariest Data Breaches of 2018*, BUS. INSIDER (Dec. 30, 2018), https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12.
[5] *See id.*

reasons, was subject to a data breach affecting the information of 21.5 million people.[6] Further, a recent Senate Intelligence Committee report named U.S. critical infrastructure as vulnerable to attack from cyber-capable adversaries.[7] 5G remains subject to the threat of Chinese telecommunication companies building back doors into critical telecommunications infrastructure.[8]

Evident from the significant increase in breaches and cyberattacks is that private institutions are not entirely equipped to secure themselves, and they should not have to be. The dynamic of cyber warfare postures companies to defend themselves from nation states.[9] In order to effectively secure U.S. cyberspace, DHS must offer protection to at-risk organizations in the private sector without overreaching its authority.

Efforts to increase private–public sector partnerships are underway, yet proposed legislation is too ambitious and impractical to implement, and has become stagnant waiting for Congressional approval.[10] This article serves to explore cybersecurity as it is today and recommend a simplified framework for a private-public sector partnership. First, this article reviews the recent improvements to the U.S. cybersecurity strategy. Second, this article looks to threats posed - both now and in the future - and how current strategy confronts or falls short of confronting such threats. Third, this article looks to the strategy of two primary adversaries, China and Russia, to determine

[6] OFF. OF PERSONNEL MGMT., CYBERSECURITY RESOURCE CENTER, https://www.opm.gov/cybersecurity/.

[7] Daniel R. Coats, *World Wide Threat Assessment of the U.S. Intelligence Community*, SENATE SELECT COMMITTEE ON INTELLIGENCE (Jan. 29, 2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

[8] Brett Simpson, *The Quest for 5G Technology Dominance: Impact on US National Security*, (Jan. 15, 2019), https://thediplomat.com/2019/01/the-quest-for-5g-technology-dominance-impact-on-us-national-security/.

[9] Steve Grobman, *When Nation-States Hack the Private Sector for Intellectual Property*, THE HILL (Mar. 31, 2018), https://thehill.com/opinion/technology/380948-when-nation-states-hack-the-private-sector-for-intellectual-property.

[10] *See* Cybersecurity Asset Protection of Infrastructure under Terrorist Attack Logistical Structure Act, H.R 54, 115th Cong. (2017); *see also* Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. (2017) (both bipartisan bills were introduced in 2017 and have yet to be passed by Congress, despite the urgent need for action in the private sector cybersecurity realm).

whether U.S. strategy adequately combats Chinese and Russian strategy. Lastly, this paper presents several frameworks of legislative options to simplify U.S. strategy into a more workable format.

I. THE BUREAUCRACY'S DELAY OF A SECURE CYBERSPACE

"We have sanctioned malign cyber actors. We have indicted those that committed cybercrimes. We have publicly attributed malicious activity to the adversaries responsible and released details about the tools they employed. We have required departments and agencies to remove software vulnerable to various security risks. We have taken action to hold department and agency heads accountable for managing cybersecurity risks to the systems they control, while empowering them to provide adequate security."[11] – President Donald Trump

President Trump's words echo true, as his administration has worked to hold malign cyber actors accountable, and to direct agency heads to combat the cyber threats of today.[12] However, if anything is apparent from watching the media report on such threats, it is that the scale of malicious action in cyberspace is broad in nature and difficult to combat. From data breaches occurring more frequently and on a larger scale to the threats posed to critical U.S. infrastructure by foreign, government-owned companies such as Huawei and ZTE, the U.S. currently faces a vast technological threat.[13]

In 2018, the Government Accountability Office (GAO) released a document titled "Urgent Actions Are Needed to Address

[11] National Cyber Strategy, *supra* note 3; *see also* Strengthening America's Cybersecurity, *supra* note 3.

[12] Countering America's Adversaries Through Sanctions Act (CAATSA), Pub. L. No. 115-44.

[13] Gary Bloom, *Why Data Breaches Will Get Worse Before Things Get Better*, FORBES (Nov. 29, 2017, 8:00 AM), https://www.forbes.com/sites/forbestechcouncil/2017/11/29/why-data-breaches-will-get-worse-before-things-get-better/#44b57df1339f.

Cybersecurity Challenges Facing the Nation."[14] The report focused primarily on "four major cybersecurity challenges and 10 critical actions that the federal government and other entities should address."[15] The four major challenges include establishing a comprehensive cybersecurity strategy with effective oversight, securing federal systems and information, protecting critical cyber infrastructure, and protecting privacy and sensitive data.[16] The GAO report is based in part on the White House's 2018 National Cyber Strategy, DHS's 2018 National Cybersecurity Report,[17] and various news reports and legislation.[18] The GAO, like the White House and DHS, provides a vision with steps necessary for a secure cyber environment.[19] Generally, each report states that DHS is primarily responsible for ensuring a secure federal civilian infrastructure and generally overseeing the federal government's relationship with the private sector's most significant industries, which are primary cyber targets.[20] The reports focus on similar objectives like ensuring emerging technologies are approached from a security-first perspective by improving security measures of the global supply chain and strengthening the overall cyber ecosystem.[21] The Trump administration has made clear that it is taking the increasingly dangerous threats from cyberspace seriously and building upon the prior administration's policies in a positive way.[22]

[14] GOV'T ACCOUNTABILITY OFF., URGENT ACTIONS ARE NEEDED TO ADDRESS CYBERSECURITY CHALLENGES FACING THE NATION (2018), https://www.gao.gov/assets/700/694355.pdf.

[15] *Id.*

[16] *Id.*

[17] *See generally* National Cyber Strategy, *supra* note 43 DEP'T OF HOMELAND SEC., CYBERSECURITY STRATEGY (2018), https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

[18] *See generally* GOV'T ACCOUNTABILITY OFF., *supra* note 14 (primarily, the reports referenced in the GAO are linked to large data breaches, such as the Equifax breach).

[19] *See generally id.*; *see also* National Cyber Strategy, *supra* note 3; DEP'T OF HOMELAND SEC., *supra* note 17.

[20] *See generally id.*

[21] *See generally id.*

[22] National Cyber Strategy, *supra* note 3; *see* Strengthening America's Cybersecurity, *supra* note 3; *see also* WHITE HOUSE, FACT SHEET: CYBERSECURITY NATIONAL ACTION PLAN (2016), https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

However, despite a renewed focus on confronting cybersecurity challenges, the GAO report contains an alarming statistic: "Of the roughly 3,000 recommendations [addressing cybersecurity challenges] made since 2010, nearly 1,000 had not been implemented as of August 2018."[23] Citizens anticipate that government bureaucracies will move slowly, but this is an alarming lapse for an issue of significant importance. While the federal civilian sector and private sector have been subject to significant delay in implementation of cyber recommendations, the Department of Defense (DoD) prepares to implement its vision detailed in the 2018 DoD Cyber Strategy.[24] In fact, Brigadier General Dennis Crall recently told the Senate Armed Services Committee that 2019 would be a year of outcomes and "actionable lines of effort that come from our cyber strategy."[25] DoD's objectives in cyberspace are:

> 1. Ensuring the Joint Force can achieve its missions in a contested cyberspace environment;
> 2. Strengthening the Joint Force by conducting cyberspace operations that enhance U.S. military advantages;
> 3. Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident;
> 4. Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks; and
> 5. Expanding DoD cyber cooperation with interagency, industry, and international partners.[26]

In addition to its more focused strategy within Cyber Command (CYBERCOM), DoD has made major movements in

[23] *See* GOV'T ACCOUNTABILITY OFF., *supra* note 14.

[24] DEP'T OF DEF., DEPARTMENT OF DEFENSE 2018 CYBER STRATEGY (2018).

[25] Billy Mitchell, *Top Pentagon Cyber Leadership Targets 'Outcomes, Results' in 2019*, FEDSCOOP (Jan. 30, 2019), https://www.fedscoop.com/cybersecurity-dod-pentagon-2019-outcomes-resultes/.

[26] DEP'T OF DEF., SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 2018 (2018); Mark Pomerleau, *For DOD Cyber, 2019 Is the Year of Doing*, FIFTH DOMAIN (Jan. 31, 2019), https://www.fifthdomain.com/dod/2019/01/30/for-dod-cyber-2019-is-the-year-of-doing/.

cyberspace, including "the elevation of U.S. Cyber Command to a full unified combatant command — which affords new and exquisite authorities — the full staffing of Cyber Command's cyber teams, an update to DoD's cyber doctrine and new authorities delegating certain responsibilities from the president to DoD to conduct cyber operations abroad."[27] Despite the reputation of both DHS and DoD as lumbering bureaucracies, DoD has reached a point where positive action in the cyber domain is imminent, whereas DHS and the federal civilian sector are implementing improvements at comparatively delayed rates.[28]

II. THREATS POSED, TODAY AND TOMORROW

"There's no way that that our military power will not erode if a robust American economic revival is not part of the cards."[29] - General James Mattis

As a U.S. Senate Intelligence report points out, cyberspace is a forum where U.S. adversaries enjoy broad freedom of action in

[27] Mark Pomerleau, *DoD Releases First New Cyber Strategy in Three Years*, FIFTH DOMAIN (Sept. 18, 2018), https://www.fifthdomain.com/dod/2018/09/19/department-of-defense-unveils-new-cyber-strategy/.

[28] Benni G. Thompson & Cedric L. Richmond, *Delayed Cyber Strategy Shows DHS is Behind*, COMMITTEE ON HOMELAND SEC. (May 15, 2018), https://homeland.house.gov/news/press-releases/thompson-richmond-delayed-cyber-strategy-shows-dhs-behind; *see also* Kate Polit, *CDM Demand Has Plenty of Room to Grow as Agencies Inch to Deployment Goals*, MERITALK (Jan. 8, 2019) (stating that "Federal agency demand for Continuous Diagnostics and Mitigation security technologies has plenty of room for continued growth based on a GAO report released in late December, which showed mixed progress on agency deployment figures for the first half of 2018. The report underlined the importance of CDM progress and chided Federal agencies for being slow to implement the government's approach to network security); *see also* Jared Serbu, *DoD Slow to Implement New Rules On Cybersecurity Breaches*, FEDERAL NEWS NETWORK (2015).

[29] Brian Jones, *One Quote From A Legendary Marine General Perfectly Captures The Risk From Political Gridlock*, BUS. INSIDER (Oct. 16, 2013), https://www.businessinsider.com/general-james-mattis-captures-risk-political-gridlock-2013-10.

unconventional ways.[30] Perhaps the most aggressive and successful strategic threats posed thus far have been through aggressive Russian cyber strategy. Russia is a pioneer in cyber strategy, given evidence showing that it compromised critical U.S. infrastructure in a number of sectors,[31] and its prominent disinformation campaigns.[32] Most notable is the Russian interference with the 2016 American Presidential election, and hacking of the Democratic National Committee's central database.[33] While foreign threats are traditionally demonstrated by a foreign nation's ability to exert force, such as intercontinental ballistic missile capabilities and nuclear proliferations, such threats remain unlikely due to fear of retaliation in kind.[34] However, attacks conducted via the domain of cyberspace are difficult to qualify and provide perpetrating nations with plausible deniability.[35] Russia exemplifies this feature through its "hybrid" methods, where Russian criminal organizations carry out state sponsored cyberattacks, while simultaneously allowing Russia to claim

[30] Daniel R. Coats, *World Wide Threat Assessment of the U.S. Intelligence Community*, SENATE SELECT COMMITTEE ON INTELLIGENCE (Jan. 29, 2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

[31] Brian, Naylor, *Russia Hacked U.S. Power Grid — So What Will The Trump Administration Do About It?*, NPR (Mar. 23, 2018), https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the-trump-administration-do-about-it.

[32] Tim Maurer & Garrett Hinck, *Russia's Cyber Strategy*, IT. INST. FOR STRATEGIC STUD. (Dec. 21, 2018), https://www.ispionline.it/en/pubblicazione/russias-cyber-strategy-21835.

[33]John Swayne & Andrew Roth, *US Indicts 12 Russians for Hacking DNC Emails During the 2016 Election*, THE GUARDIAN (July 13, 2018), https://www.theguardian.com/us-news/2018/jul/13/russia-indictments-latest-news-hacking-dnc-charges-trump-department-justice-rod-rosenstein.

[34] John Mueller, *Nuclear Weapons Don't Matter*, FOREIGN AFF. (Oct. 15, 2018), https://www.foreignaffairs.com/articles/2018-10-15/nuclear-weapons-dont-matter.

[35] Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, SCI. AM. (June 11, 2011), https://www.scientificamerican.com/article/tracking-cyber-hackers/; Lucas Laursen, *Russia-Linked Hackers Responsible for Vast European Cyber Attacks, Says Microsoft*, FORTUNE (Feb. 20, 2019), http://fortune.com/2019/02/20/microsoft-russia-hacking-europe/; Madeline Roache, *Hacker From Russian Crime Group Jailed In Multi-Million Dollar Global Blackmail Conspiracy*, TIME (Apr. 9, 2019), http://time.com/5566519/russian-cyber-crime-hacker-nca/.

that the attacks were not conducted by Russian state agencies.[36] While this method is no longer the cover it once was, and the U.S. is well aware of the connection that criminal organizations have to the Russian government, it remains difficult to respond to such aggressive actions.[37] Further, Russia has exemplified hybrid and forward thinking in regard to cybersecurity, evidenced by the Kremlin's efforts to control internet access within Russian borders.[38]

China has engaged in a similar type of cyber strategy, although in the context of a different, broader state strategy.[39] For example, the "Trump administration, found that Chinese theft of American IP currently costs between $225 billion and $600 billion annually."[40] While Russia has recently focused primarily on sowing doubt in the American government, China has successfully leveraged cyber operations to gain a significant economic advantage and this has resulted in a looming trade war, which presents another non-traditional national security threat.[41] While kinetic force and the capability to project force defined the 20th century, 21st century warfare

[36] *Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements*, U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMMITTEE ON INTELLIGENCE, https://intelligence.house.gov/social-media-content/ (last visited May 10, 2019).

[37] *Id.*

[38] Jacqueline Thomsen, *Kremlin Seeks More Control Over Internet in Russia*, THE HILL (Feb. 18, 2019), https://thehill.com/policy/cybersecurity/430201-kremlin-seeks-more-control-over-internet-in-russia.

[39] Dingding Chen, *China Has a New Grand Strategy and the West Should Be Ready*, THE DIPLOMAT (Oct. 31, 2017), https://thediplomat.com/2017/10/china-has-a-new-grand-strategy-and-the-west-should-be-ready/; Andy Aikin, *What Do We Know About Russia's 'Grand Strategy?,'* WASH. POST (May 2, 2017), https://www.washingtonpost.com/news/monkey-cage/wp/2017/05/02/what-do-we-know-about-russias-grand-strategy/?utm_term=.37e0a183c85f.

[40] Sherisse Pham, *How Much Has the US Lost from China's IP Theft?*, CNN BUSINESS (Mar. 23, 2018), https://money.cnn.com/2018/03/23/technology/china-us-trump-tariffs-ip-theft/index.html; Ron Nixon, *Smuggling of U.S. Technology is Outpacing Cold War Levels, Experts Say*, N.Y. TIMES (Mar, 18, 2018), https://www.nytimes.com/2018/03/17/world/asia/us-technology-smuggling-foreign-weapons.html.

[41] *A Quick Guide to the US-China Trade War*, BBC (Jan. 7, 2019), https://www.bbc.com/news/business-45899310.

hardly resembles war at all.[42] Rather, today's conflict is more of a "Cold War 2.0" with the defining feature being direct state confrontation through the domain of cyberspace.[43]

China's stated goal is to become a "leading world power," by 2050.[44] Although it has not stated as grand a strategy as Chinese President Xi Jinping did, Russia has worked toward "the goal of shaping the international community to Russia's liking."[45] While Russia and China have engineered alternative methods to directly confront the United States's position in the world, the United States has been encumbered by a conventional view of national security strategy.[46] In fact, Mark Kelton, former Deputy Director for Counterintelligence at the CIA's National Clandestine Service, said it best: "Although U.S. counterintelligence (CI) professionals have long viewed the Chinese intelligence threat with concern, there has been little broader consideration of the potential cumulative impact of that effort on broader U.S. national security…."[47] Only recently has the U.S. made significant attempts to counter its determined foes. That is not to say that the U.S. should turn away from "hard power" methods. Rather, the U.S. must refocus on sustainable and long-term cyber dominance. Recent years have seen increases in awareness and the need for an improved approach to cybersecurity strategy, made

[42] *See generally* Eric Hobshaw, *War and Peace*, THE GUARDIAN (Feb. 22, 2002), https://www.theguardian.com/education/2002/feb/23/artsandhumanities.highereducation.

[43] Robert Kaplan, *A New Cold War Has Begun*, FOREIGN AFF. (Jan. 27, 2019), https://foreignpolicy.com/2019/01/07/a-new-cold-war-has-begun/.

[44] Ting Si, *Xi Plans to Turn China Into a Leading Global Power by 2050*, BLOOMBERG (Oct. 17, 2017), https://www.bloomberg.com/news/articles/2017-10-17/xi-to-put-his-stamp-on-chinese-history-at-congress-party-opening.

[45] Aikin, *supra* note 46.

[46] *See* William McHenry, *We Face Greater Threats than Conventional Forces from Moscow; NATO Strategy Should Reflect That*, THE HILL (Aug. 24, 2018 11:30 AM), https://thehill.com/opinion/national-security/402898-we-face-greater-threats-than-conventional-forces-from-moscow-nato; Anthony H. Cordesman, *China and the U.S,*, CTR. FOR STRATEGIC & INT'L STUD. (Oct. 3, 2018), https://www.csis.org/analysis/choosing-between-four-cs-conflict-and-containment-versus-competition-and-cooperation.

[47] Mark Kelton, *The Coming Chinese Storm*, THE CIPHER BRIEF (Feb. 5, 2019), https://www.thecipherbrief.com/article/asia/the-coming-chinese-storm.

evident by the Cybersecurity Enhancement Act of 2014 signed by President Obama,[48] and the more recent Cybersecurity Executive Order and Cybersecurity Strategy, issued by the Trump Administration.[49]

III. U.S. National Cyber Strategy Overview: Is it Working?

DHS Cyber Security Vision: By 2023, the Department of Homeland Security will have improved national cybersecurity risk management by increasing security and resilience across government networks and critical infrastructure; decreasing illicit cyber activity; improving responses to cyber incidents; and fostering a more secure and reliable cyber ecosystem through a unified departmental approach, strong leadership, and close partnership with other federal and nonfederal entities.[50]

U.S. cyber strategy is not working. Despite invigorated efforts by the Trump administration and various federal agencies, notably DHS and DoD, to take action against malicious cyber actors and threats, there does not seem to be a legitimate deterrent effect of employed tactics.[51] While the nonpartisan nature of cybersecurity has generated support, the role of federal agencies must still be clearly defined in their respective roles in cybersecurity.[52] The National Cyber Strategy does make efforts to further centralize the management and oversight of federal civilian cybersecurity by clarifying DHS's role in securing federal department and agency networks, while making the exception of national security systems that fall under the DoD and

[48] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014).

[49] Exec. Order No. 13,800, 82 Fed. Reg. 22391 (2017); National Cyber Strategy, *supra* note 3; *see also* Olivia Beavers, *Trump Signs Bill Cementing Cybersecurity Agency at DHS*, The Hill (Nov. 16, 2018, 3:47 PM), https://thehill.com/policy/cybersecurity/417185-trump-signs-bill-cementing-cybersecurity-agency-at-dhs.

[50] Dep't of Homeland Sec., *supra* note 1, at 1.

[51] National Cyber Strategy, *supra* note 3, at 2.

[52] Derek B. Johnson, *Trump's Cyber Strategy: What They Are Saying*, FCW (Sept. 21, 2018), https://fcw.com/articles/2018/09/21/cyber-strategy-react-johnson.aspx.

Intelligence Community (IC) systems.[53] In fact, President Trump further clarified DHS's role as the protectorate of civilian cybersecurity in a 2018 bill, renaming DHS's National Protections and Programs Directorate (NPPD) as the Cybersecurity and Infrastructure Security Agency (CISA).[54] "Top DHS officials have been pushing for the bill to pass, arguing it would better communicate their mission to the private sector and help DHS recruit top cyber talent."[55] President Trump's bill is clarification, which simultaneously makes apparent a significant gap in all cyber strategies promulgated in the U.S.: the civilian cybersecurity sector is largely uncertain of how and with whom to work with in the federal government to combat cybersecurity threats.[56]

Cyberspace is complex because it levels playing fields. For years, the U.S. government has struggled to grasp the appropriate response to a nation-state attack on a U.S.-based corporate entity. While DHS is tasked primarily with overseeing the security of the federal civilian cyberspace and critical infrastructure, there is an apparent gap where private sector corporations fall within the confines of the broader U.S. national security architecture. A common example would be a major data breach of a large private sector corporation, such as the Equifax data breach.[57] While the Equifax breach exposed millions of financial and credit records of private U.S. citizens, the U.S. government's primary response to the breach was purely advisory.[58] If the United States is serious about protecting the private sector from cyberattacks, defensive measures and preemptive support are required. A single breach, although significant on the scale of records stolen, does not necessarily exemplify a national security threat.

[53] National Cyber Strategy, *supra* note 3, at 6.

[54] Beavers, *supra* note 56.

[55] *Id.*

[56] National Cyber Strategy, *supra* note 3, at 6.

[57] *See* Steve Symanovich, *Equifax Data Breach Affects Millions of Consumers. Here's What to Do.*, LIFELOCK, https://www.lifelock.com/learn-data-breaches-equifax-data-breach-2017.html, (last visited May 14, 2020).

[58] *See, e.g. Equifax Data Breach*, FED. TRADE COMM'N, https://www.ftc.gov/equifax-data-breach (last visited May 10, 2019); Tamar Hallerman & J. Scott Trubey, *Congressional Report: Equifax Breach 'Entirely Preventable'*, GOV TECH (Dec. 11, 2018), https://www.govtech.com/security/Congressional-Report-Equifax-Breach-Entirely-Preventable.html.

However, in the aggregate, such breaches offer soft targets and can have grave economic impacts on U.S. global standing. By failing to mitigate isolated breaches, like the Equifax breach, the U.S. succumbs to the broader, ambitious goals of global competitors such as China and Russia.

IV. CYBER SECURITY'S ROLE IN A BROADER STRATEGY

"War is a mere continuation of policy by other means."[59] - Carl von Clausewitz

Carl von Clausewitz's observation on war as a continuation of politics by other means rings true to this day. However, while existential pressures and threats of internal crises have always put pressure on nations, never in history has a forum existed allowing the indirect engagement of a foe as it does now through cyberspace. Through cyberspace, adversaries are capable of waging war by alternative means.[60] Through cyberspace, adversaries are capable of challenging the U.S.'s position as a global superpower without waging combat operations.[61] The most notable example is China's decades-long strategy to embody its "middle kingdom," and Russia's efforts to redefine its role as a superpower.[62] The U.S. must first understand that although it is unlikely to enter direct combat operations with China or Russia, each country poses a severe and real threat to the U.S.'s position in the world. As a country, the U.S. must ask itself: "Is the U.S. prepared to relinquish its role as the world's superpower?"

Other countries have distinct advantages in their ability to access and control cybersecurity operations and defenses through their own systems of governance. For example, China's pseudo hybrid communist and capitalist version of governance has resulted in a lack

[59] CARL VON CLAUSEWITZ, ON WAR (J.J. Graham trans., 1873), https://clausewitz.com/readings/OnWar1873/BK1ch01.html#a.

[60] *See generally* Isaac R. Porche III, *Getting Ready to Fight the Next (Cyber) War*, RAND CORP. (Mar. 3, 2018), https://www.rand.org/blog/2018/03/getting-ready-to-fight-the-next-cyber-war.html.

[61] Samm Sacks, *Beijing Wants to Rewrite the Rules of the Internet*, THE ATLANTIC (June 18, 2018), https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/.

[62] Si, *supra* note 51; *see also* Maurer, *supra* note 39.

of distinction between private and public sector companies.[63] Such control also applies to China's cybersecurity policies, allowing for little to no data privacy protections of private citizens.[64] Further, China's president Xi Jinping recently modified the Chinese constitution, allowing for his presidency to reign for an undetermined amount of time.[65] The result is a forward-looking and driven vision for China's future, allowing a consistent approach in methodology due to the lack of democracy or alternatives.[66] To be clear, the U.S. should not be envious of the lack of freedoms in China. However, there is merit in the efficiency of the Chinese form of governance. Particularly, China utilizes an exceptionally restricted internet within its territory, both restricting and governing internet access of Chinese citizens.[67] Furthermore, China maintains tight control over the private sector by mandating cybersecurity standards under the guise of

[63] *See* Li Yuan, *Private Businesses Built Modern China. Now the Government Is Pushing Back*, N.Y. TIMES (Oct. 3, 2018), https://www.nytimes.com/2018/10/03/business/china-economy-private-enterprise.html.

[64] *See generally* Samm Sacks, *China's Emerging Cyber Governance System*, CTR. FOR STRATEGIC & INT'L STUDIES, https://www.csis.org/chinas-emerging-cyber-governance-system (last visited Apr. 28, 2019); *see also* Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, LAWFARE, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense (July 20, 2017); *see also* Anna Mitchel & Larry Diamond, *China's Surveillance State Should Scare Everyone*, THE ATLANTIC, https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/ (Feb. 2, 2018).

[65] James Doubek, *China Removes Presidential Term Limits, Enabling Xi Jinping To Rule Indefinitely*, NPR (Mar. 11, 2018), https://www.npr.org/sections/thetwo-way/2018/03/11/592694991/china-removes-presidential-term-limits-enabling-xi-jinping-to-rule-indefinitely.

[66] *Six Advantages of China's Political System*, CHINA DAILY (Mar. 19, 2010), http://www.chinadaily.com.cn/opinion/2010-03/19/content_9615376.htm.

[67] *See Businesses, Consumers Uncertain Ahead of China VPN Ban*, REUTERS (Mar. 30, 2018), https://www.reuters.com/article/us-china-vpns/businesses-consumers-uncertain-ahead-of-china-vpn-ban-idUSKBN1H612F.

recommendations.[68] The result is a uniform (or close to uniform) cyber-secure state.[69]

Similar to China, Russia is in the process of passing a bill to test and work toward developing the capability of "disconnecting" Russia from the broader internet.[70] Such control over internet within Russia's own borders would provide a significant advantage for Russia in defending itself from cyberattacks or retaliation.[71] In fact, on December 23, 2019, the Russian government announced that it had successfully disconnected from the worldwide internet, relying solely on a Russian based intranet.[72] Despite apparent risks, particularly the often unknown dependency of infrastructure on the internet, the ability of the Russian government to disconnect from the broader internet would allow a significant advantage in secluding Russia from consequences of its own aggressive offensive cyber policies.[73]

Distinct in each of these examples is not necessarily the willingness of Russia or China to invest in major initiatives to secure their internet, but rather their central governments' capability to mandate and direct each country's respective private sector to comply.[74] While the U.S. has adopted recommended cybersecurity

[68] Colin Zick, *China Expands Its Cybersecurity Regulations*, SEC., PRIVACY, & THE LAW (Oct. 9, 2018), https://www.securityprivacyandthelaw.com/2018/10/china-expands-its-cybersecurity-regulations/.

[69] Samm Sacks & Manyi Kathy Li, *How Chinese Cybersecurity Standards Impact Doing Business In China*, CTR. FOR STRATEGIC & INT'L STUDIES (Aug. 2, 2018), https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china.

[70] Louise Matsakis, *What Happens if Russia Cuts Itself Off From the Internet*, WIRED (Feb. 12, 2019), https://www.wired.com/story/russia-internet-disconnect-what-happens/.

[71] *Id.*

[72] Catalin Cimpanu, *Russia Successfully Disconnected From the Internet*, ZDNET, https://www.zdnet.com/article/russia-successfully-disconnected-from-the-internet/ (Dec. 23, 2019).

[73] Charlotte Jee, *Russia Wants to Cut Itself off from the Global Internet. Here's What that Really Means*, TECH. REV. (March 21, 2019), https://www.technologyreview.com/s/613138/russia-wants-to-cut-itself-off-from-the-global-internet-heres-what-that-really-means/.

[74] CHINA DAILY, *supra* note 75; *see also* Andrei Kolesnikov & Denis Volkov, *Pragmatic Paternalism: The Russian Public and the Private Sector*, CARNEGIE MOSCOW CTR. (Jan. 18, 2019), https://carnegie.ru/commentary/78155.

standards via NIST, and worked toward a more inclusive approach to the private sector in cyber security, the interagency process and private sector engagement in the U.S. have a long way to go.[75] Frequently voiced concerns in the cyber security arena include the growing rise of automated systems (artificial intelligence) and Quantum Information Systems (an aspect of Quantum Science which could render modern IP-infrastructure obsolete).[76] However, the U.S. should be focused primarily on developing a coordinated and inclusive approach to cybersecurity.[77] Because cybersecurity by nature involves the private sector, the U.S. must find a way to secure an industry in which it has little power to control, and often regulates from a distance. U.S. investment in research and development (R&D) for future technologies is significant and effective, yet such technologies will provide isolated benefits if the U.S. does not formulate effective and efficient methods for consolidating security throughout the broader internet infrastructure.

U.S. government agencies are not blind to the need for more efficient coordination. DHS's 2018 cyber strategy notes the importance of forming partnerships with federal and non-federal entities alike, and the DoD's 2018 cyber strategy similarly acknowledges the need for such a partnership.[78] When it comes to coordination and assistance provided to the private sector, the U.S. federal government often falls short. However, there are multiple

[75] *Cybersecurity Framework*, NIST (last visited May 10, 2019), https://www.nist.gov/cyberframework.

[76] *See* Zack Whittaker, *US Intelligence Community Says Quantum Computing and AI Pose an 'Emerging Threat' to National Security*, TECHCRUNCH, https://techcrunch.com/2018/12/13/us-intelligence-quantum-computing-artificial-intelligence-national-security-threat/ (Dec. 13, 2018).

[77] DEP'T OF HOMELAND SEC., *supra* note 17; *see also* NATIONAL CYBER STRATEGY, *supra* note 3.

[78] *U.S. Department of Homeland Security Cybersecurity Strategy*, DEP'T OF HOMELAND SEC., at 7-11 (May 15, 2018), https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf; *see also* DEP'T OF DEF., *supra* note 24; Rhys Dipshan, *DoD Latest Federal Department to Push Private-Sector Focus on Cybersecurity*, LEGALTECH NEWS (last visited May 10, 2019), https://www.law.com/legaltechnews/2018/09/25/dod-latest-federal-department-to-push-private-sector-focus-on-cybersecurity/?slreturn=20190120151254.

frameworks focused on public and private sector coordination that have proven successful, and may contribute to a broader framework for increased public and private sector coordination. Reform and improvement to U.S. federal and civilian infrastructure must be the result of sound policy and legislative efforts aimed at closing gaps between industry and public sector entities. While such partnerships can be exceedingly difficult to implement efficiently in democratic governments, one of the United States' oldest and closest allies, the United Kingdom (U.K.), has excelled. The next section addresses the U.K.'s success.

V. U.K. CYBER DEFENSE INITIATIVE

Although primary aggressors in the cyber domain have been successful in leveraging the private sector, neither Russia nor China serves as an adequate model for the U.S. to base its own cybersecurity initiatives off of due to vast distinctions in form of government. However, the United Kingdom has implemented an Active Cyber Defense (ACD) initiative that has seen success particularly in blocking spoof email messages and blocking access to malicious websites by actively utilizing the U.K.'s National Cyber Security Centre (NCSC) "[t]o protect its networks from harm and from hackers using the government brand to cause harm to others."[79] As described in a U.K. Kings College report on the ACD program, ACD "draws on established practices across industry, which see cybersecurity analysts developing an understanding of the threats to their networks, and then devising and implementing measures to proactively combat, or defend, against these threats."[80] The report rightly points out that some view ACD as a strategy that allows for implementing organizations to mitigate cyber threats and attacks through offensive action.[81] Offensive strategies historically receive significant criticism

[79] Stuart Russell & Nadiya Kostyuk, *Evaluating the U.K.'s 'Active Cyber Defence' Program*, LAWFARE (Feb. 14, 2018, 12:00 PM), https://www.lawfareblog.com/evaluating-uks-active-cyber-defence-program.

[80] TIM STEVENS ET AL., KING'S COLL. LONDON, UK ACTIVE CYBER DEFENCE: A PUBLIC GOOD FOR THE PRIVATE SECTOR 9 (2019).

[81] *See id.*

for the potential to escalate a conflict with little to no oversight.[82] In fact, the U.S. has dealt with this specific issue before, and debated whether offensive action by the private sector could be legal in these turbulent times.[83] However, the ACD program makes a point to only utilize defensive measures. Doing so substantially mitigates any controversy that the program would have previously had, leaving offensive measures to the government and military.[84]

The ACD report states that the goal of the program is: "to protect the majority of people in the UK from the majority of the harm, caused by the majority of the attacks, for the majority of the time."[85] As such, the objective of ACD has never been portrayed as being completely secure, or completely successful, but there have been tremendous results in its goal of providing realistic security most of the time.[86] ACD seeks to protect organizations from "'commodity attacks,' understood as the high volume of relatively unsophisticated malicious software (malware)."[87] While ACD is only one part of a broader cybersecurity strategy, it has the potential to serve as a template for future government cybersecurity efforts in the private sector.

As visiting fellow at Harvard's Kennedy School Belfer Center, Stuart Russel, points out in his recent Lawfare comment, "the ACD program now has proven ability to better protect both the government and the general public from cybersecurity threats. The standard approach of simply telling people how best to protect themselves has not worked over the last twenty years."[88] In fact, the U.S. government

[82] *See, e.g.,* Tom Kulik, *Why The Active Cyber Defense Certainty Act Is A Bad Idea*, ABOVE THE LAW (Jan. 29, 2018, 5:30 P.M.), https://abovethelaw.com/2018/01/why-the-active-cyber-defense-certainty-act-is-a-bad-idea/.

[83] PAUL ROSENZWEIG ET AL., HERITAGE FOUND., NEXT STEPS FOR U.S. CYBERSECURITY IN THE TRUMP ADMINISTRATION: ACTIVE CYBER DEFENSE 1 (2017).

[84] *See* STEVENS, *supra* note 89, at 3.

[85] STEVENS ET AL., *supra* note 89, at 11.

[86] IAN LEVY, NAT'L CYBER SEC. CTR., ACTIVE CYBER DEFENCE – ONE YEAR ON 8, 68 (2018), https://www.ncsc.gov.uk/information/active-cyber-defence---one-year-on; Russell, *supra* note 89.

[87] STEVENS, *supra* note 89, at 11-12.

[88] Russell, *supra* note 88.

has traditionally relied on creating standards recommended to the private sector as a primary means of increasing private sector cyber resiliency.[89] Evident by the current climate, such standards have not functioned as intended. The ACD program takes a more proactive government approach. Notably, the UK's "NCSC aims to make most ACD initiatives publicly available for people to see, tweak, or even adopt wholesale."[90] As pointed out by the UK Kings College report, the ACD initiative has the potential to function as a "public good."[91] ACD also focuses on fixing "systemic security failures at scale to benefit everyone," and maintaining transparency throughout the program.[92]

Although the program is still in early stages, the results speak for themselves. The first year of ACD offered email processing to analyze and protect from malicious spam mail, web checks on suspicious websites, public sector domain name checks blocking access to detected malicious websites, signaling and routing services making "source and destination address spoofing in IP space much harder," and the ACD integration program, "the Threat-o-Matic, that links all the Active Cyber Defense measures and the early experiments [it has] done with others to prove event sharing and the benefits it could bring."[93] The report outlines significant success, detailing a significant amount of potential threats verified, blocked, and reported.[94] While ACD may not protect organizations from more intrusive attacks, the program has the potential to be scalable and offer a broader range of protection.[95] Specifically, ACD recognizes that "much of the business of countering commodity attacks is generic and can be automated."[96] If ACD is broadly adopted, the publicly available

[89] *See* MATTHEW P. BARRET, NAT'L INST. FOR STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY vi (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[90] Russell, *supra* note 88.

[91] STEVENS, *supra* note 89, at 4 ("Public goods are ordinarily provided by governments or civil authorities and refer to publicly available goods or services that are provided to all and the use of which by one person does not diminish its availability to another").

[92] Russell, *supra* note 88.

[93] LEVY, *supra* note 95, at 1-4; Russell, *supra* note 85.

[94] LEVY, *supra* note 95, at 1-3.

[95] *See* STEVENS, *supra* note 89, at 19.

[96] STEVENS, *supra* note 89, at 12; LEVY, *supra* note 95, 7-8.

government initiative that automates a significant array of cybersecurity systems has the potential to decrease the exponentially increasing costs of the private sector's expenses on cybersecurity, while simultaneously increasing the cost of executing attacks on enterprise institutions.[97]

ACD's first year is a step in the right direction toward providing government services for the protection of private sector institutions. Further, the concept as a whole is feasible to implement in the United States. In fact, the United States proposed the Active Cyber Defense Certainty Act (ACDCA) on October 12, 2017.[98] However, the ACDCA is similar to the UK's ACD strategy only in name. The ACDCA's primary purpose would allow private sector companies that have been infiltrated to conduct offensive measures in the event of a breach.[99] While a more aggressive and offensive cybersecurity strategy is necessary, the offensive nature of the ACDCA has the potential to increase the complexity of the cyber operating space.

VI. THE ACTIVE CYBER DEFENSE CERTAINTY ACT AND CAPITALS ACT: STEPS IN THE RIGHT DIRECTION?

"Crises there will continue to be. In meeting them, whether foreign or domestic, great or small, there is a recurring temptation to feel that some spectacular and costly action could become the miraculous solution to all current difficulties. A huge increase in newer elements of our defense; development of unrealistic programs to cure every ill in agriculture; a dramatic expansion in basic and applied research - these and many other possibilities, each possibly promising in itself, may be suggested as the only way to the road we wish to travel. But each proposal must be weighed in the light of a broader consideration…"[100]
– Dwight D. Eisenhower

[97] *See* STEVENS, *supra* note 89, at 4; LEVY, *supra* note 95, at 7-8.
[98] Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. (2017).
[99] *Id.* at §2(5), (6), (11).
[100] President Dwight D. Eisenhower, Farewell Address "Military – Industrial Complex" (Jan. 17, 1961), U.S. EMBASSY & CONSULATE IN THE REPUBLIC OF KOREA,

As cyberattacks on private sector companies become more frequent and severe, the agencies charged with the cyber protection of the American private sector - namely, DHS and the Federal Bureau of Investigations (FBI) - do not possess the means to "protect our nation against the magnitude of the threat we are facing today."[101] In recognition of this current lack of resources, the ACDCA, with bipartisan support and referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations on November 1, 2017, was drafted to alleviate this burden.[102] The ACDCA was reintroduced to again on June 13, 2019, and again referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations on June 28, 2019.[103] In addition to providing safeguards for the use of Active Cyber Defense measures by the private sector, the bill lifts restrictions imposed by the CFAA in certain specified scenarios, which prohibit unauthorized access to another's computers.[104] "The ACDCA would lift this restriction, allowing a company to implement active defensive measures to not only identify the attackers, but even destroy information originally stolen from its network."[105] Although the prospect of empowering companies to take matters into their own hands has the potential to offer significant increases in protections, the implications of a U.S. based private sector corporation hacking and destroying information - even stolen information - from a foreign nation state or private sector company may cause significant harm to U.S. foreign policy interests.[106] Additionally, the practicability of private sector corporations

https://kr.usembassy.gov/education-culture/infopedia-usa/famous-speeches/dwight-d-eisenhower-farewell-address-military-industrial-complex/.

[101] Irving Lachow, *The Promise and Peril of Active Cyber Defense*, THE HILL (Oct. 18, 2018), https://thehill.com/opinion/cybersecurity/383704-the-promise-and-peril-of-active-cyber-defense.

[102] *Bills in the 115th Congress, H.R. 4036 Active Cyber Defense Certainty Act*, C-SPAN: CONGRESSIONAL CHRONICAL (Jan. 2, 2019), https://www.c-span.org/congress/bills/bill/?115/hr4036; H.R. 4036, §2(2).

[103] H.R. 4036.

[104] Kulik,*supra* note 91; *see also* Robert Chesney, *Hackback Is Back: Assessing the Active Cyber Defense Certainty Act*, LAWFARE (June 14, 2019), https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act.

[105] *Id.*

[106] *Id.*

empowering their IT departments to "hack back" may not be realistic or feasible.[107]

Tom Kulik, an Intellectual Property & Information Technology Partner at Scheef & Stone, LLP and contributor to the *Above the Law*, states, "The technical proficiency required to effectively counter-attack hackers is high — it requires constant vigilance, significant expertise, and dedicated focus. Most IT staff are not positioned to undertake such actions, and bolstering IT staff to do so as part of their existing responsibilities is simply not feasible."[108] Kulik continues by asking, "If large companies like Yahoo and Equifax cannot properly prevent or contain their own data breaches, how can they be expected to take on organized cyber attackers on their own digital turf?"[109] The ACDCA operates under the assumption that the primary cause for escalations in severity and frequency of cyberattacks on private corporations is the fact that corporations are constrained by their inability to properly defend themselves.[110] However, the reality is that these corporations have only added a defensive option to counterattack hackers that the corporation was not adequately capable of defending itself against in the first place.[111] While the option of "hacking back" would allow companies to operate with more sovereignty over their own data, the option does not appear feasible, nor would it have any significant effect on current threats.[112] Moreover, hacking back opens up a litany of potentially severe foreign policy fallout.

Irving Lachow, an opinion contributor to *The Hill*, points out two possible risks related to hacking back: "collateral damage to third parties and inadvertent escalation of tension with other countries."[113]

[107] *Id.*

[108] *Id.*

[109] *Id.*

[110] *See* H.R. 4032, §2(2).

[111] *See* Kulik, *supra* note 91.

[112] *See id; see also* Andrea Limbago, *The 'Hacking Back' Bill Isn't The Answer to Cyberattacks*, WAR ON THE ROCKS (Oct. 31, 2017), https://warontherocks.com/2017/10/the-hacking-back-bill-isnt-the-solution-to-cyberattacks/.

[113] Lachow, *supra* note 109.

Lachow is right to point out these risks because the nature of a cyberattack is never straightforward, and often involves a hacker routing attacks through multiple servers. This makes it difficult, if not impossible, to effectively and accurately trace any attack to the original source.[114] The result of a misidentified threat being "hacked back" could be a country or company that had no involvement in a hack suffering from a cyberattack sourced from a private sector corporation based in the U.S.[115] The result of such an attack is difficult to characterize, but there is potential that the U.S. could be held legally culpable.[116] Kristen Eichensehr from *Just Security* poses the following scenario:

> If the United States is responsible for international law violations committed by private actors, then international law permits aggrieved foreign governments to take countermeasures against the United States—that is, actions that would be violations of international law but for the prior U.S. violation of international law. Such countermeasures may be cyber-related (like retaliatory hacking of U.S. government computers) or outside the cyber realm (like breach of existing treaty commitments).[117]Recently, the U.S. has been involved in negotiations with the Chinese government due to the Chinese infringing on U.S. patented technology and stealing trade secrets.[118] It would not be difficult to imagine other countries fostering similar angst against the U.S. in the event of U.S.-based corporations being effectively "unleashed" on other countries. Such a stance in policy has the potential to damage the U.S.'s ability to negotiate in

[114] *See* Chris Cook, *Hacking Back in Black: Legal and Policy Concerns with the Updated Active Cyber Defense Certainty Act*, JUST SEC. (Nov. 20, 2017), https://www.justsecurity.org/47141/hacking-black-legal-policy-concerns-updated-active-cyber-defense-certainty-act/; *See* Limbago, *supra* note 120.

[115] *See* Limbago, *supra* note 120.

[116] *See* Cook, *supra* note 122.

[117] Kristen Eichensehr, *Would the United States Be Responsible for Private Hacking?*, JUST SEC. (Oct. 17, 2017), https://www.justsecurity.org/46013/united-states-responsible-private-hacking/#more-46013.

[118] *See* Jodi Klein, *China Accused by US and Allies of 'Massive Hacking Campaign to Steal Trade Secrets and Technologies'*, SOUTH CHINA MORNING POST (Dec. 20, 2018), https://www.scmp.com/news/world/united-states-canada/article/2178981/us-and-more-dozen-allies-condemn-china-economic; Rachel Brown & Preston Lim, *U.S.-China Trade Talks Continue with an Emphasis on Tech*, LAWFARE (Apr. 3, 2019), https://www.lawfareblog.com/us-china-trade-talks-continue-emphasis-tech.

other realms, such as trade, and may result in sanctions or legal action against the U.S. government or private sector.[119] While the actions of a private corporation may be viewed as its own, and result only in legal action against that specific private corporation, the risks associated may increase overall hostility toward the U.S. While the prospect of empowering the private sector may be appealing, the U.S. should walk before it runs.

The Cybersecurity Asset Protection of Infrastructure under Terrorist Attack Logistical Structure Act, or CAPITALS Act, may be more sensible legislation to empower the U.S. private sector, and embody the ideas utilized in the U.K.'s ACD program. The CAPITALS Act requires DHS to "report to Congress regarding the feasibility of establishing a DHS Civilian Cyber Defense National Resource."[120] The act calls for the report to specifically address estimations of workforce requirements to defend critical infrastructure, identify the best resources and sectors to recruit and train for defensive purposes, gauge response capabilities for response to incidents in different regions, identify the impact of a lack of government involvement and experience in protecting the private sector, detail logistics required to allow governors to request resources from DHS during cyber emergencies, and determine whether developing a resource to defend U.S. networks would be a worthy investment.[121]

Such reporting and an official establishment of what DHS can actually provide the U.S. private sector and critical infrastructure are much needed steps. However, another report on shortcomings of private sector security should not be required to initiate action. While the ACDCA and the CAPITALS Act each propose unique legislative solutions to flaws in U.S. cyber strategy, each fails at opposite ends of the spectrum. Looking to the flaws in each proposed act reveals a middle ground for cyber strategy that is practical for implementation and alleviates the burden on the federal government's broad mission

[119] *See* Cook, *supra* note 122.

[120] Cong. Research Serv., *Summary: H.R. 54 – 115th Congress (2017-2018)*, CONGRESS.GOV (Jan. 3, 2017), https://www.congress.gov/bill/115th-congress/house-bill/54?overview=closed.

[121] *See id.*

of securing the private sector and the private sector's continuous struggle to secure itself.

VII. PRINCIPAL SHORTCOMINGS IN U.S. CYBERSECURITY STRATEGY: WHAT IS THE WAY FORWARD FROM HERE?

The ACDCA and the CAPITALS Act each uniquely exemplify the principle shortcomings in U.S. cybersecurity strategy for the private sector. First, the ACDCA, as established, would likely give unpredictable and unpractical power to private sector corporations, effectively increasing legal action against the U.S. by empowering unequipped private sector associates to defend themselves.[122] This act, while in theory an act of empowerment, chooses to ignore the reality of a private corporation facing off against a nation state.[123] In essence, the ACDCA shifts responsibility at a tremendous increase in risk to U.S. foreign policy.[124]

Second, the CAPITALS Act, while an initiation and acknowledgement of the need to secure the private sector, is merely an order directed at DHS to investigate and create a report.[125] As attacks become more sophisticated and corporations more frequently fall victim to cyberattacks, DHS must take the initiative and act.[126] While a report to Congress is a good first step toward securing the U.S. private sector from cyberattacks, it also highlights the significant shortcomings in Congressional ability to take action.[127] As evident by the fact that the bill was introduced in 2017 and again in 2019, and requires the report to be submitted no later than 240 days after the enactment of the act (which has not yet been enacted), it does not seem likely that the report will be issued to Congress in a meaningful

[122] *See* Cook, *supra* note 122; Lachow, *supra* note 109.

[123] *See* Cook, *supra* note122; Lachow, *supra* note 109.

[124] *See* Cook, *supra* note122; Lachow, *supra* note109.

[125] H.R. 54.

[126] *See* Kylie Bielby, *GAO: DHS and Agencies Must Work to Improve Cybersecurity,* HOMELAND SECURITY TODAY (Feb. 5, 2020) https://www.hstoday.us/subject-matter-areas/infrastructure-security/gao-dhs-and-agencies-must-work-to-improve-cybersecurity/; *see also* Michael Kans, *A Congressional Cybersecurity To-Do List*, JUST SEC. (Nov. 15, 2018), https://www.justsecurity.org/61480/congressional-cybersecurity-to-do-list/.

[127] *See id.*

amount of time.[128] In fact, it is much more likely that by that time DHS issues a report to Congress, the rapid pace at which technology evolves will have altered the reality of the situation for which the report was intended.[129]

Contrast both the ACDCA and the CAPITALS Act with the U.K.'s ACD program. The most glaring difference is the fact that ACD has actually been implemented in the U.K., while the bi-partisan legislation in the U.S. has stalled in Congress, resulting in no action, and only debate.[130] Legislation passed by Congress is required at some point in the future to strengthen the U.S.'s cyber strategy. However, the amount of time it takes to pass a bill will only allow malicious actors in cyberspace to continue their activities.[131] A review of both U.K. and U.S. cyber strategy reveals that this should not be the case. Both strategies are substantially similar in their goals: they each look to raise the price of conducting a cyberattack and recognize the dependencies of their respective nations on digital forums.[132] The only true problem with U.S. cyber strategy is the failure to implement action for the private sector.[133] While organizations - primarily DHS - have consulted and partnered with the private sector for cyber security reasons, and have even come up with sector-specific security plans and partnerships,[134] the U.S. desperately needs a broader and more

[128] H.R. 54.

[129] *See* Carten Dordell, *DHS Overhauls Its Science & Technology Directorate*, FEDSCOOP (Oct. 2, 2018), https://www.fedscoop.com/dhs-overhauls-science-technology-directorate-office/.

[130] *See* Tim Starks & Eric Geller, *Where Cybersecurity Legislation 'goes to die' in Congress*, POLITICO (Feb. 11, 2019), https://www.politico.com/story/2019/02/11/cybersecurity-ron-johnson-1160081.

[131] *See id.*

[132] See Kans, *supra* note 134; National Cyber Strategy, *supra* note 3; UK National Cyber Security Strategy 2016-2021, HM GOVERNMENT (2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

[133] Amitai Etzioni, *Cybersecurity in the Private Sector*, ISSUES IN SCI. AND TECH. (2011), https://issues.org/etzioni-2/.

[134] *See generally Cybersecurity Risk Information Sharing Program*, U.S. DEP'T OF ENERGY (last visited May 10, 2019), https://www.energy.gov/sites/prod/files/2018/09/f55/CRISP%20Fact%20Sheet.pdf; *DHS Cyber Security Initiative Plans To Partner Public & Private Sectors*, CYBER SEC.

encompassing service for the general public.[135] In this sense, and regardless of any deficiencies in the program itself, the ACD program has succeeded by simply existing.[136] The U.S. must follow suit and release some sort of protection to the private sector. That solution may exist in the form of a service already in existence: the EINSTEIN program.

DHS's much touted EINSTEIN program may present a solution in the form of an appropriate mechanism for the federal government's securing of private sector cyberspace.[137] The EINSTEIN program is intended to secure federal civilian agencies from cyberattacks.[138] However, the program has received significant criticism for many shortcomings.[139] The program, which as of FY2018 cost $5.7 billion and the first iteration of which was deployed in 2003, was required to be implemented in all 23 non-defense federal civilian agencies.[140] However, only "5 of the 23 agencies were receiving intrusion prevention services."[141] In 2018, the Government

HUB (last visited May 10, 2019), https://www.cshub.com/executive-decisions/news/dhs-cyber-security-initiative-plans-to-partner-public-private-sectors.

[135] Etzioni, *supra* note141.

[136] Phil Muncaster, *Active Cyber Defense Should Be Rolled Out UK-Wide: Report*, INFO SECURITY (Jan. 22, 2019), https://www.infosecurity-magazine.com/news/active-cyber-defence-should-be/.

[137] Liam Tung, *US auditors slam Homeland Security's $5.7bn Einstein firewall: But are they missing the point?*, ZDNET (Feb. 2, 2016), https://www.zdnet.com/article/us-auditors-slam-homeland-securitys-5-7bn-einstein-firewall-but-are-they-missing-the-point/; Eduard Kovacs, *DHS's Einstein Security System Has Limited Capabilities: Audit*, SEC. WEEK (Feb. 2, 2016), https://www.securityweek.com/dhss-einstein-security-system-has-limited-capabilities-audit.

[138] *See* EINSTEIN, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/einstein (Feb. 20, 2020).

[139] *EINSTEIN 3 Accelerated*, DHS (last visited May 10, 2019), https://www.dhs.gov/publication/einstein-3-accelerated.

[140] Eduard Kovacs, *DHS's Einstein Security System Has Limited Capabilities: Audit*, SEC. WEEK (Feb. 2, 2016), https://www.securityweek.com/dhss-einstein-security-system-has-limited-capabilities-audit.

[141] Jon Slye, *DHS's $5.7 Billion EINSTEIN Ain't So Smart*, GOVWIN (Feb. 2, 2016), https://iq.govwin.com/neo/marketAnalysis/view/169?researchTypeId=1&researchMarket=; Mike Rogers, *Fix the Inadequate Systems that Protect .gov Networks*, DEFENSE ONE (Sept. 23, 2017), https://www.defenseone.com/ideas/2017/09/fix-inadequate-systems-protect-gov-networks/141228/; *EINSTEIN*, DHS CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY (last visited May 10, 2019),

Accountability Office (GAO) produced a report on National Cybersecurity Protection Systems and the EINSTEIN program, indicating that implementation of the program has been inconsistent and produced significantly varied results.[142] In fact, the report noted that "although the system's intrusion detection capabilities provided the ability to detect known patterns of malicious activity on agency networks, it was limited in its capabilities to identify potential threats using anomaly-based detection."[143] While the current state of the system is not perfect, GAO also noted that EINSTEIN "has provided increasing capabilities to detect and prevent potential cyberattacks involving the network traffic entering or exiting the networks of participating federal agencies."[144] EINSTEIN is still a work in progress. While the program is not complete, the program's template, which works as an intrusion detection and protection service for implementation within federal agencies, is one which may benefit from looking to the U.K.'s ACD initiative.

VIII. The Solution: EINSTEIN, the ACD Initiative, and Presidential Action

Action is where the U.K.'s ACD initiative can greatly benefit the U.S. and DHS. The U.K.'s ACD program has created a potentially new template, modeling cyber security services as a public good and likely capable of rollout into the private sector.[145] There is no reason to think that ACD cannot serve as a template for the U.S. to forge a

https://www.dhs.gov/cisa/einstein; Joseph Marks, *Nearly 90% of Civilian Agencies Run DHS' Einstein 3A Cyber Program*, NextGov (Nov. 11, 2016), https://www.nextgov.com/cybersecurity/2016/11/latest-dhs-cyber-system-running-nearly-90-percent-civilian-agencies/133117/.

[142] *Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting against Intrusions*, GAO (Dec. 2018), https://www.gao.gov/assets/700/696105.pdf; Ms. Smith, *DHS EINSTEIN firewall fails to detect 94% of threats, doesn't monitor web traffic*, CSO (Feb. 4, 2016), https://www.csoonline.com/article/3030028/dhs-einstein-firewall-fails-to-detect-94-of-threats-doesnt-monitor-web-traffic.html.

[143] Slye, *supra* note 149.

[144] GAO, *supra* note 150.

[145] Muncaster, *supra* note 144.

different version of non-retaliatory defense.[146] Moving forward, options such as the ACDCA and CAPITALS Act, although well-intentioned, should be scrapped. The most promising option for U.S. cybersecurity should follow the U.K.'s ACD initiative, with the focus on providing the public a "public good" service to all.[147] The focus of this program can follow more closely in the ACD's footsteps, in that it "protect[s] the majority of people in the UK from the majority of the harm, caused by the majority of the attacks, for the majority of the time," and does not seek to be a one size fits all solution.[148] In consideration of the type of software and security measures produced, the U.S. has options to either closely replicate the ACD program, or continue to improve the EINSTEIN program for release as a public good.

The U.S. should not waste any more time. The most effective tool for ensuring action by federal agencies would be the issuance of a presidential executive order. President Trump has shown through his numerous actions in cybersecurity strategy, and research and development, that he takes the nation's cybersecurity seriously. In an effort to create definitive action in the cybersecurity realm, an executive order mandating DHS to expand its EINSTEIN program to serve as a public good would not only meet the goals of the ACDCA and CAPITALS Act by providing cybersecurity options to the public, but could also serve as a foundation to build increasing layers of security for threats of the future.

Conclusion

Although there are many ways that the United States can improve cybersecurity protections, the U.S. remains at the forefront of

[146] Michael Hill, *NCSC's 'Active Cyber Defence' Initiative Boasts Impressive First-Year Results*, INFOSECURITY (Feb. 5, 2018), https://www.infosecurity-magazine.com/news/ncscs-active-cyber-defence/ (stating that "This 'active defense' experiment by the NCSC – if adopted by other countries and even other large organizations – could radically change the attacker/defender landscape").

[147] STEVENS, *supra* note 89, at 4.

[148] STEVENS, *supra* note 89, at 11 (quoting I. Levy, *Active Cyber Defence – tackling cyber attacks on the UK*, NAT'L CYBER SEC. CTR.: INSIDE THE NCSC (Nov. 1, 2016), https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk.

technological innovation in the world.[149] The U.S. must predominantly focus efforts in response to the ever-growing threat of an unsecure cyberspace and on more efficient and effective governance.[150] As exemplified by Chinese and Russian governance, the U.S.'s central focus on the protection of the people's freedoms creates a disadvantage in cybersecurity.[151] However, by utilizing the provision of a public service and "light-touch" regulations, the U.S., through DHS, can provide a template for security. Rather than impose a cybersecurity regime on the private sector, the U.S. must be willing to invest in a service that the private sector cannot match, and thus, will need. Such a task is easier said than done, but the private sector is currently spending comparably significant sums of money on cybersecurity.[152] The most rational way forward is to increase cybersecurity investment in a practical program. While the EINSTEIN program has been heavily criticized, the program's focus on intrusion detection and prevention is a practical solution, and one the U.K.'s ACD has used with very positive results. By following the U.K.'s lead and creating a public good in the form of a cybersecurity threat detection and prevention system, the U.S. can effectively protect the private sector. Moreover, an executive order directing DHS to either improve EINSTEIN and release the program for public use or create a new program more closely following the ACD program is the most efficient way to mobilize the government. In time, and with positive results, Congress may legislate on the issue, and potentially approve and direct the much-needed funding required to vastly improve cybersecurity protections for the private sector. The costs may seem

[149] *See* OFFICE OF SCI. & TECH. POLICY, OFFICE OF THE PRESIDENT, SCIENCE & TECHNOLOGY HIGHLIGHTS IN THE FIRST YEAR OF THE TRUMP ADMINISTRATION (2017); OFFICE OF SCI. & TECH. POLICY, OFFICE OF THE PRESIDENT, SCIENCE & TECHNOLOGY HIGHLIGHTS IN THE SECOND YEAR OF THE TRUMP ADMINISTRATION (2018).

[150] Starks & Geller, *supra* note139; *see also* Julian Barnes & David E. Sanger, *Congress, Warning of Cybersecurity Vulnerabilities, Recommends Overhaul*, THE NEW YORK TIMES, (March 11, 2020) https://www.nytimes.com/2020/03/11/us/politics/congress-cyber-solarium.html.

[151] Maurer & Hinck, *supra* note 39; *see also* Chen, *supra* note 46.

[152] Steve Morgan, *Why J.P. Morgan Chase & Co. Is Spending A Half Billion Dollars On Cybersecurity*, FORBES (Jan. 30, 2016), https://www.forbes.com/sites/stevemorgan/2016/01/30/why-j-p-morgan-chase-co-is-spending-a-half-billion-dollars-on-cybersecurity/#34898fbb2599.

significant, but the long-term benefits to a secure private sector will show the necessity of action.