Prepared Statement of Jamil N. Jaffer[1]
on
U.S. Cybersecurity Preparedness and H.R. 7331, the National Cyber Director Act
before the
Committee on Oversight and Government Reform
of the
United States House of Representatives

July 15, 2020

I. Introduction

Chairwoman Maloney, Ranking Member Comer, and Members of the Committee: thank you for inviting me to discuss our nation's cybersecurity preparedness and the proposed legislation to establish a new National Cyber Director (NCD).

I appreciate the opportunity to discuss these important matters and am honored to appear on a panel with such distinguished private sector leaders as former House Intelligence Committee Chairman Mike Rogers, Cyber Threat Alliance President and CEO J. Michael Daniel, Cyberspace Solarium Commission member Suzanne Spaulding, and Tenable Chairman and CEO Amit Yoran. I'm likewise honored that our panel is testifying after Congressman Jim Langevin (D-RI) and Congressman Mike Gallagher (R-WI), both of whom have established strong reputations on Capitol Hill as leaders on cyber issues and as bipartisan consensus builders who are focused on the substance of these critically important issues.

I look forward to hearing from my fellow panelists and to answering the Committee members' questions.

II. The Current Threat Environment

As the members of this Committee all too well know, the cyber threats facing the United States—including our public and private sector—are, in a word, massive. It is no overstatement to say that, for all practical intents and purposes, we are at war in cyberspace.

[1] Jamil N. Jaffer currently serves as Founder & Executive Director of the National Security Institute and as an Assistant Professor of Law and Director, National Security Law & Policy Program at the Antonin Scalia Law School at George Mason University and is affiliated with Stanford University's Center for International Security and Cooperation. Mr. Jaffer also serves as Senior Vice President for Strategy, Partnerships & Corporate Development at IronNet Cybersecurity, a startup technology products company headquartered in the Washington, DC metropolitan area. Among other things, Mr. Jaffer previously served as Chief Counsel & Senior Advisor to the Senate Foreign Relations Committee, Senior Counsel to the House Intelligence Committee, Associate Counsel to President George W. Bush, and Counsel to the Assistant Attorney General for National Security in the U.S. Department of Justice. Mr. Jaffer also served as an outside advisor to the Cyberspace Solarium Commission. Mr. Jaffer is testifying before the Committee in his personal and individual capacity and not on behalf of any organization or entity, including but not limited to any current or former employer. Mr. Jaffer would like to thank Austin Shaffer and Taylor Nelson for their excellent research and other assistance in the preparation of this testimony.

And, unfortunately, as a nation we still remain woefully underprepared to deal with this ongoing and serious conflict.

There are, of course, many experts (lawyers in particular) that may quibble with this characterization of the current environment, rightly noting that the usual definitions of an "armed attack" under international law may not have been met or that the activities that have taken place thus far fall below the classic thresholds of armed conflict. These same experts will also likely point out that neither the U.S. government nor any of our adversaries have acknowledged the existence of an affirmative state of war.

And yet the fact is that for the better part of a decade, and certainly more so in recent years, our nation has been involved in a consistent and ongoing series of conflicts in cyberspace, albeit fairly low-level conflicts.[2]

Regardless whether we call this state of affairs war or not, there can be no question that it has had a huge impact on our nation and its allies. It is estimated that the cyber-enabled economic warfare conducted by China—primarily focused on the U.S. private sector—drains private companies of billions of dollars a year, with total damage estimates running well into the trillions of dollars.[3] As former NSA Director (and Founding Commander of U.S. Cyber Command) GEN (Ret) Keith B. Alexander noted over nearly a decade ago[4]—and as FBI Director Chris Wray recently reiterated (albeit without citation) earlier this month[5]—this activity represents the

---

[2] *See, e.g.*, GEN (Ret) Keith B. Alexander, *Prepared Statement on Cyber Warfare Today: Preparing for 21st Century Challenges in an Information-Enabled Society* at 1, House Armed Services Committee (Apr. 11, 2018), available online at <https://nationalsecurity.gmu.edu/wp-content/uploads/2018/05/Alexander-Testimony-Cyber-Warfare-Today.pdf>. ("[W]e are not yet ready as a nation to grapple with the reality that cyberspace has become a domain for warfare and that we very much are in the throes today of a series of ongoing—albeit currently low-level—conflicts in cyberspace")

[3] *See, e.g.,* Sen. Angus King, Rep. Mike Gallagher, Ms. Suzanne Spaulding, and Mr. Tom Fanning, *Testimony on the Report of the Cyberspace Solarium Commission* at 5, Senate Committee on Homeland Security and Government Affairs (May 12, 2020), *available online at* <https://www.hsgac.senate.gov/imo/media/doc/Testimony-King,%20Gallagher,%20Spaulding,%20&%20Fanning-2020-05-13-REVISED.pdf>. ("Chinese cyber campaigns have enabled the theft of trillions of dollars in intellectual property.").

[4] *See* Dennis Blair, et al., *The IP Commission Report* at 2 (May 2013), The Commission on the Theft of Intellectual Property *available online at* <http://ipcommission.org/report/IP_Commission_Report_052213.pdf>. ("The members of the Commission agree with the assessment by the Commander of the United States Cyber Command and Director of the National Security Agency, General Keith Alexander, that the ongoing theft of IP is 'the greatest transfer of wealth in history.'"); *see also* GEN. (Ret.) Keith B. Alexander, *Prepared Statement on Digital Acts of War: Evolving the Cybersecurity Conversation*, Subcommittees on Information Technology and National Security of the Committee on Oversight and Government Reform (July 13, 2016), *available online at* <http://nationalsecurity.gmu.edu/wp-content/uploads/2018/05/Gen-Alexander-Statement-Digital-Acts-of-War-7-13.pdf> ("[T]he rampant theft of intellectual property from American private sector companies by nation-states and their proxies[] constitut[es] what I have previously described as the greatest transfer of wealth in human history…").

[5] See Christopher Wray, *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States*, The Hudson Institute (July 7, 2020), available online at <https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states> ("It's the people of the United States who are the victims of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history.")

the greatest transfer of wealth in human history. Indeed, Chairman Rogers, who is on this panel today, nearly a decade ago also called our attention to the significant economic threat posed by China, noting that:

> There is an economic cyber war going on today against U.S. companies. There are two types of companies in this country, those who know they've been hacked, and those who don't know they've been hacked. Economic predators, including nation-states, are blatantly stealing business secrets and innovation from private companies.[6]

In addition, over the years, our enemies have conducted the types of attacks against the United States and our allies—both abroad and at home—that, had they taken place in domains of warfare other than cyberspace, we might have regarded as tantamount to acts of war. For example, we have seen foreign nation-states like North Korea and Iran engage in the affirmative destruction of data and the bricking of computer systems, rendering them unusable, here in the United States for over half a decade.[7] And we know that this threat continues, given that the Director of National Intelligence told Congress last year that Iran is actively "preparing for cyber attacks against the United States and our allies" and is "capable of causing localized, temporary disruptive effects—such as disrupting a large company's corporate networks for days to weeks—similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017."[8]

We've also seen the highly corrosive effects of Russia's ongoing active measures campaign on the American body politic. This effort—which I predict will eventually be determined to be the single-most effective covert influence operation to date—has had the effect of undermining the American public's confidence not only in our electoral system and a range of candidates for office, but has likewise tainted elected officials from both parties, turned Americans against one another in our federal and state legislatures, on cable television, and in the streets, and has undermined our core rule of law institutions, including the Justice Department, the FBI, and key elements of our Intelligence Community. To be sure our own institutions and their members—including top elected officials, media, online platforms, and others—certainly have played roles in this problem also, whether by failing to lead effectively (or worse by actively creating additional discord amongst our people), engaging in illegal or unethical activities, or providing the fora where these manipulative activities by foreign nation-states can flourish. Nonetheless, it

---

[6] *See* House Permanent Select Committee on Intelligence, *Rogers & Ruppersberger Introduce Cybersecurity Bill to Protect American Businesses from "Economic Predators,"* Press Release (Nov. 30, 2011), *available online at* <https://ruppersberger.house.gov/newsroom/press-releases/ruppersberger-rogers-introduce-cybersecurity-bill-to-protect-american>.

[7] See Director of National Intelligence James R. Clapper, *Opening Statement to Worldwide Threat Assessment Hearing*, Senate Armed Services Committee (Feb. 26, 2015), *available online at* <https://www.dni.gov/files/documents/2015%20WWTA%20As%20Delivered%20DNI%20Oral%20Statement.pdf> ("2014 saw, for the first-time, destructive cyber attacks carried out on U.S. soil by nation state entities, marked first by the Iranian attack on the Las Vegas Sands Casino a year ago this month and the North Korean attack against Sony in November.").

[8] *See, e.g.*, Office of the Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community* at 6, Senate Select Committee on Intelligence (Jan. 29, 2019), *available online at* <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>.

is clear Russia's efforts to taint American politics through online manipulation has been—and continues to be—all too successful.

Worse still, because of our collective inability or unwillingness to recognize this activity for what it is and to join hands across the political divide to confront it aggressively and head-on, the Russians have paid little, if any, price for this behavior. And unfortunately, this fact that has not gone unnoticed other adversaries, like the Chinese, who are already engaging in similar overt and covert influence campaigns around the COVID virus and the killing of George Floyd. These same players may very well seek to engage in similar activities in the upcoming election cycle.

Likewise, we've seen the significant threat that both nation-state and criminal actors can pose to key critical infrastructure entities, including those in the financial services and energy sectors. For example, as Chairwoman Maloney noted over three years ago, "[c]ybersecurity is posing a greater and greater risk to the safety and soundness of our financial system."[9] J.P. Morgan Chase Chairman and CEO Jamie Dimon underlined this same concern in an April 2019 letter to shareholders, where he stated that "[t]he threat of cyber security may very well be the biggest threat to the U.S. financial system."[10] That same year—and for the fourth year in a row—IBM assessed that the finance and insurance sector was the number one most attacked sector, with attacks on these institutions accounting for 17 percent of all cyber attacks in the top 10 most attacked industries.[11] And we know that at least some nation-states, like North Korea, have profited significantly from these attacks, with the Director of National Intelligence noting last year that North Korea's "cybercrime operations include attempts to steal more than $1.1 billion from financial institutions across the world—including a successful cyber heist of an estimated $81 million from the New York Federal Reserve account of Bangladesh's central bank,"[12] the very hack that led Chairwoman Maloney to seek answers from various American financial institutions in 2016.[13]

And yet, even given the significant cyber threat already facing the financial sector, in mid-April 2020—just three months ago—the U.S. Secret Service and FBI jointly issued a warning that "the COVID-19 pandemic provides criminal opportunities on a scale likely to dwarf anything seen before," noting specifically that "[t]he speed at which criminals are devising and executing their schemes is truly breathtaking" and that the "sheer variety of frauds already uncovered is itself

---

[9] *See* Rep. Carolyn B. Maloney, *Combatting Cyber Security Threats at Our Banks* (Aug. 30, 2016), *available online at* <https://maloney.house.gov/media-center/newsletters/combatting-cyber-security-threats-at-our-banks-0>.

[10] *See* Jamie Dimon, *Letter to Shareholders* at 35, JP Morgan Chase (Apr. 2019), *available online at* <https://www.jpmorganchase.com/corporate/investor-relations/document/ceo-letter-to-shareholders-2018.pdf>.

[11] *See* IBM Security, *X-Force Threat Intelligence Index 2020* at 30 (2020), *available online at* <https://www.ibm.com/downloads/cas/DEDOLR3W>.

[12] *See, e.g.*, ODNI, *Worldwide Threat Assessment, supra* n. 8 at 6. And the number may actually be higher. *See, e.g.,* Sen. Angus King, et al, *Testimony on the Report of the Cyberspace Solarium Commission*, *supra* n. 3 at 5 ("According to UN estimates, North Korean cyber operations earn $2 billion in illicit funds for the regime each year.").

[13] *See* Rep. Maloney, *Combatting Cyber Security Threats*, *supra* n. 9; *see also* Rep. Carolyn B. Maloney, *Bangladesh Bank Heist*, available online at <https://maloney.house.gov/issues/bangladesh-bank-heist>.

shocking."[14] This assessment, moreover, is backed by the very real and troubling statistics. According to CarbonBlack, ransomware attacks increased 148% in March 2020 over the baseline from the prior month, with the financial sector being the biggest single sectoral target, with a 38% increase in attacks.[15] In April 2020, Google reported that it was seeing 18 million daily malware and phishing emails related to COVID-19, not to mention more than 240 million COVID-related daily spam messages.[16]

That same month, the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the U.K.'s National Cyber Security Centre (NCSC) put out an alert highlighting a number of financially related threats conducted by malicious cyber actors seeking to exploit the pandemic.[17] Specifically, CISA and NCSC indicated that malware campaigns were actively taking advantage of interest in the coronavirus pandemic, often for financial gain.[18] Likewise, CISA and NCSC reported an increase efforts by threat actors to take advantage of the new work-from-home environment, with threat actors seeking exploit publicly known vulnerabilities in remote access software platforms.[19] With approximately 300 million workers across the globe working from home, including up to 90% of banking and insurance employees,[20] these efforts represent a uniquely challenging threat. And in May, we learned that Washington State suffered massive cyber-enabled unemployment fraud losing the state hundreds of millions of dollars.[21]

Likewise, in testimony before Congress early last year, the Director of National Intelligence noted the serious cyber threat to the energy sector posed by nation-states with advanced capabilities. Specifically, the DNI noted that "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States."[22] The DNI also stated that Russia is actively "mapping our critical infrastructure with the long-term goal of being able to cause

---

[14] *See* Federal Bureau of Investigation, *FBI and Secret Service Working Against COVID-19 Threats* (Apr. 15, 2020), *available online at* <https://www.fbi.gov/news/pressrel/press-releases/fbi-and-secret-service-working-against-covid-19-threats>.

[15] *See* VMWare Carbon Black, *Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted* (Apr. 15, 2020), available online at <https://www.carbonblack.com/2020/04/15/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/>.

[16] *See* Steven Musil, *Google Blocking 18M Malicious Coronavirus Emails Every Day*, CNET (Apr. 15, 2020), *available online at* <https://www.cnet.com/news/google-seeing-18m-malicious-coronavirus-emails-each-day/>.

[17] *See* Department of Homeland Security, *COVID-19 Exploited by Malicious Cyber Actors*, CISA Alert AA20-099A (Apr. 8, 2020), *available online at* <https://www.us-cert.gov/ncas/alerts/aa20-099a>.

[18] *Id*.

[19] *Id.*

[20] *See* Juan Carlos Crisanto and Jermy Prenio, *Financial Crime in Times of COVID-19 – AML and Cyber Resilience Measures* at 2, FSI Briefs, No. 7 (May 2020), *available online at* <https://www.bis.org/fsi/fsibriefs7.pdf>.

[21] *See* Paul Roberts, et al, *'Hundreds of Millions of Dollars' Lost in Washington to Unemployment Fraud Amid Coronavirus Joblessness Surge*, Seattle Times (May 21, 2020), *available online at* <https://www.seattletimes.com/business/economy/washington-adds-more-than-145000-weekly-jobless-claims-as-coronavirus-crisis-lingers/>.

[22] *See, e.g.*, ODNI, *Worldwide Threat Assessment, supra* n. 8 at 5.

substantial damage" and specifically "has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016."[23]

None of this even accounts for the significant threat of collateral damage to private industry and government alike posed by nation-state attacks that conducted for strategic or tactical advantage. For example, the NotPetya attack conducted by Russia and aimed at Ukraine is estimated to have cost over $10 billion worldwide, with the significant majority of that damage being suffered by American and allied private sector companies, who bore the brunt of the otherwise targeted attack.[24] Moreover, it is estimated that between 2019 and 2024, U.S. companies risk losing $5.2 trillion in value creation opportunities—nearly the size of the economies of France, Italy, and Spain combined—as a result of cybersecurity attacks, with the largest scope of threats facing the high-tech industry, with more than $753 billion potentially at risk.[25] And lest we forget, in recent years, China successfully obtained massive amounts of highly personal and confidential data on Americans through their targeted breaches of the Office of Personnel Management, Equifax, Marriott, and Anthem.[26] This data could be used for intelligence purposes, empowering decades of highly targeted HUMINT and other campaigns, as well as to train advanced machine learning models on sensitive American data.[27]

These threats, taken together, demonstrate the extremely challenging cyber threat environment facing the nation at the present time.

III. The Cyberspace Solarium Commission Report

Released in March of this year amongst the backdrop of an expanding coronavirus outbreak, a major oil price war, and a rising tide of cyber threats, the Cyberspace Solarium Commission's report represents critically important way of reconceptualizing cyber defense. For example, the Commission's ideas around planning for the continuity of the economy and strengthening systemically important critical infrastructure entities with direct government support both break fundamentally new ground in an area otherwise chock full of studies and reports.

---

[23] *Id*. at 5-6.

[24] *See* Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired Magazine (Aug. 22, 2018), available online at <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

[25] *See* Accenture Strategy, *Securing the Digital Economy: Reinventing the Internet for Trust* at 16 (2019), *available online at* <https://www.accenture.com/us-en/insights/cybersecurity/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf>.

[26] See Department of Justice, *Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax* (Feb. 10, 2020), *available online at* <https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military> ("For years, we have witnessed China's voracious appetite for the personal data of Americans, including the theft of personnel records from the U.S. Office of Personnel Management, the intrusion into Marriott hotels, and Anthem health insurance company, and now the wholesale theft of credit and other information from Equifax.").

[27] *Id*. ("This data has economic value, and these thefts can feed China's development of artificial intelligence tools as well as the creation of intelligence targeting packages.")

In addition, by providing clear, concise, and actionable recommendations for both Congress and the Executive Branch, the report provides policymakers like this Committee with a roadmap for moving out. This face, combined with the caliber of the Commission's members and staff, including two U.S. Senators and two Members of Congress, all of whom have reputations for working across the aisle, means that Commission's Report can certainly have a substantive impact. And we've seen exactly that. A number of the Commission's recommendations are likely to make it through the legislative process over the next few weeks as the House and Senate complete their consideration of the National Defense Authorization Act, and today's hearing is likewise a testimony to the value of the ideas the Commission put together.

IV. U.S. Cybersecurity Preparedness

Before turning to the specific legislative question before the Committee today on the National Cyber Director Act, it is perhaps also important to discuss the other key issue before the Committee: namely, our nation's preparedness to confront the key cyber threats facing our nation.

The Commission's report addresses this issue squarely, saying that "[t]he United States now operates in a cyber landscape that requires a level of security, resilience, and trustworthiness that neither the U.S. government nor the private sector alone is currently equipped to provide."[28] Worse still, the Commission's report notes that "shortfalls in agility, technical expertise, and unity of effort, both within the U.S. government and between the public and private sectors, are growing."[29]

This stark assessment is, of course, deeply troubling. Given the reliance of our nation on cyber-enabled systems to function on a day-to-day basis, as well as the fundamentally innovation-focused nature of our modern economy, the notion that neither the government nor the private sector are where we need them to be in order to provide an effective defense for our nation is wholly unacceptable.

One of the key challenges that our nation faces in this regard is the core way in which we think about defending the nation in this new domain of warfare. Historically, our approach to national-level threats, particularly those brought to bear upon us by foreign nation-states, is that the federal government will take on these threats. After all, in the traditional environment we don't expect individual Americans or companies to protect themselves against Russian Bear bombers coming over the horizon.[30] Rather, we expect American companies to defend

---

[28] *See* Cyberspace Solarium Commission, *Commission Report* (March 2020), at 1, *available online at* <https://www.solarium.gov/report> (emphasis added).

[29] *Id*.

[30] Keith B. Alexander, Jamil N. Jaffer, and Jennifer S. Brunet, *Clear Thinking about Protecting the Nation in the Cyber Domain*, Cyber Defense Review 2, no. 1 at 29, 33 (2017), *available online at* <https://nationalsecurity.gmu.edu/wp-content/uploads/2017/03/CDRV2N1_Clear-Thinking_Alexander_Jaffer_Brunet_032217-1.pdf> ("The fact is that commercial and private entities cannot be expected to defend themselves against nation-state attacks in cyberspace. Such organizations simply do not have the capacity, the capability, nor the authority to respond in a way that would be fully effective against a nation-state

themselves against the typical criminals, using appropriately tall fences and armed guards, not surface-to-air missiles. Buttressing this view, in 2012, then-Secretary of Defense Leon Panetta made clear that the U.S. government's policy was that "the Department [of Defense] has a responsibility…to be prepared to defend the nation and our national interests against an attack in or through cyberspace."[31]

And yet today in cyberspace there is little question that the government does not provides an effective or comprehensive defense of the nation. While we have established U.S. Cyber Command, and provided it with resources, we have not provided it with anywhere near the kind of resources or authorities it would take to actually defend the nation in cyberspace. Indeed, there is every reason to believe that there is not yet a consensus in our nation today on what role government ought have in defending our cyber infrastructure.

Nonetheless, the opposite approach, that we ought leave the private sector to fend for itself in defending against foreign nation-state threat actors is likewise untenable. Requiring American companies to stand alone to defend themselves against nation-states which have virtually unlimited resources—both human capital and economic—is to consign ourselves to failure.[32] After all, American private sector companies are generally not in the business of defending themselves against cyberattacks; rather, they operate in order to provide products and services to their customers, whether individuals or other businesses, and to generate economic returns from such business.[33] Such companies will inherently be constrained from deploying alone the type of defenses it would take to effectively stop a committed nation-state attacker. And yet, this is exactly where we find ourselves today: as a general matter, we expect every private sector company in our economy—from the largest banks to the smallest bake shop--to defend itself against every attacker, whether the Russian FSB or a script kiddie in a basement room.[34]

This, of course, makes little sense and it therefore should come as no surprise that we are failing at this effort. The Cyberspace Solarium Commission recognized this challenge and provided its

---

attacker in cyberspace. Indeed, in most other contexts, we do not (and should not) expect corporate America to bear the burden of nation-state attacks. For example, we do not expect Target to employ surface-to-air missiles to defend itself against Russian planes dropping bombs in the United States. Rather, that responsibility belongs to the DoD. Today, however, in cyberspace, that expectation is flipped on its head.")

[31] *See* Department of Defense, *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security* (Oct. 11, 2012), *available online at* <http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136>.

[32] *See, e.g.*, GEN (Ret) Keith B. Alexander & Jamil N. Jaffer, *Iranian Cyberattacks Are Coming, Security Experts Warn*, Barron's (Jan. 10, 2020) ("Expecting individual companies to defend themselves against a nation state with virtually unlimited financial resources and human capital does not make sense. Yet today that is our national policy in cyberspace. This is so even though, in every other context, defense against nation-state attacks is the province of the government. We don't expect Target or Walmart to have surface-to-air missiles to defend against Russian Bear bombers. Yet when it comes to cyberspace, we expect exactly that of every American company, large or small.").

[33] *Id*.

[34] *Id*.

bold support and clear explanation of an idea long discussed by many[35] but understood by few: the need for collective defense in cyberspace.

Noting that the vast majority of the cyber infrastructure is in the private sector, the Commission argued that "[t]he U.S. government and industry … must arrive at a new social contract of shared responsibility to secure the nation in cyberspace."[36] According to the Commission, "[t]his 'collective defense' in cyberspace requires that the public and private sectors work from a place of truly shared situational awareness and that each leverages its unique comparative advantages for the common defense."[37]

Specifically, the Commission argued that "[w]hile the U.S. government has taken a number of steps to develop situational awareness in cyberspace, there continue to be significant limitations on its ability to develop a comprehensive picture of the threat…the data or information is not routinely shared or cross-correlated at the speed and scale necessary for rapid detection and identification."[38]

To that end, among key recommendations like the creation of a cyber joint planning cell and a new public-private center, the Commission recommended the creation of a joint collaborative environment, namely "a common, cloud-based environment in which the federal government's unclassified and classified cyber threat information, malware forensics, and network data from monitoring programs are made commonly available for query and analysis."[39] Ensuring that the government is able to combine all of its data with that of the private sector to truly create broad situational awareness in cyberspace is a critical step towards increasing our national preparedness in the cyber realm.

And in doing so, the government must be willing to use the national means at its disposal to collect and share actionable cyber threat intelligence with industry at scale and speed, a commitment which has long been made but rarely if ever actually met. Of course, simply creating situational awareness is not sufficient; in order to truly protect our nation in this new domain of warfare, government and industry must train and fight together, collaborating in real-time to protect both public and private sector networks against common threats.

Likewise, of course, individual companies ought also engage in collective defense by sharing cyber threat information across multiple companies and industries. We already see quite a bit of valuable sharing taking place within specific industries through ISACs and through collaborative organizations like the Cyber Threat Alliance. It is important to build upon these efforts by

---

[35] *See, e.g.*, GEN (Ret) Keith B. Alexander & Jamil N. Jaffer, *Defending the Nation in Cyberspace — A Call to Action*, The Hill (Apr. 24, 2019), available online at <https://thehill.com/opinion/cybersecurity/440053-defending-the-nation-in-cyberspace-a-call-to-action>.

[36] *See* Cyberspace Solarium Commission, *Commission Report* (March 2020), at 96, *available online at* <https://www.solarium.gov/report>.

[37] *Id.*

[38] *Id.* at 101.

[39] *Id.* at 102.

broadening and deepening these sharing relationships and turning them into true, real-time collaborations.

To that end, and to the extent this Committee is willing to consider additional recommendations from the Commission's reports, rapid full implementation of the Commission's recommendations on collective defense could represent a strong step forward in protecting our nation.

V. Proposals to Establish National Cyber Director

In addition to the recommendations described above, one of the Commission's core recommendations for reforming the government's cyber policy and operations structure is to establish a National Cyber Director (NCD), within the Executive Office of the President.[40] Under the Commission's proposed construct, which finds itself largely embodied in the legislation being considered by the Committee today, H.R. 7331, the National Cyber Director Act, the NCD would be appointed by the President, with the advice and consent of the Senate, and be supported by an Office of the National Cyber Director which would have two Deputy National Cyber Directors and a core staff of up to 75 individuals, as well as other experts, consultants, and government agency personnel.[41]

The NCD would, among other things: (1) serve as the President's principal advisor for cybersecurity strategy and policy; (2) develop the U.S. National Cyber Strategy and supervise its implementation; (3) making recommendations on changes to organization, personnel, resource allocations, and policies of various departments and agencies; (4) reviewing agency budget proposals for consistency with the strategy; (5) assessing integration and interoperability of various federal cybersecurity operations centers; (6) reporting to Congress on the nation's cybersecurity posture; leading join interagency planning for an integrated federal response to cyberattacks and cyber campaigns of significant consequence; (7) coordinating the development of joint integrated operational plans, processes and playbooks for the President's approval, including the integration of offensive and defensive plans; (8) exercising and updating such plans; (9) ensuring coordination of such plans with the private sector; and (10) directing the federal government's response to cyberattacks and cyber campaigns of significant consequence, including developing operational priorities, requirements and tasks, ensuring deconfliction and execution of operational activities; and coordinating operational activities with relevant private sector entities.[42] The NCD would also be permitted to attend and participate in National Security Council meetings and would further be empowered to convene meetings of the National Security Council, the Homeland Security Council, and the National Economic Council with the concurrence of the relevant Presidential advisor responsible for such entity.[43]

---

[40] *Id*. at 37.

[41] *See* H.R. 7331, National Cyber Director Act, § 2(b)(1)-(2) & § 2(e), 116th Cong., 2d Sess., *available online at* <https://langevin.house.gov/sites/langevin.house.gov/files/documents/6.25%20LANGEV_085_xml.pdf>.

[42] *Id*. at § 2(c)(1)

[43] *Id*. at § 2 (c)(2)(B) & § 2(d).

According to the Commission, the idea would be to position the NCD and his or her office similarly to that of the Office of the U.S. Trade Representative and that the NCD "would not direct or manage day-to-day cybersecurity policy or the operations of any one federal agency, but instead will be responsible for the integration of cybersecurity policy and operations across the executive branch."[44] Moreover, in the Commission's view, the NCD would "coordinate interagency efforts to defend against adversary cyber operations against domestic U.S. interests" without "imping[ing] on DoD responsibility for Title 10 activities, Office of the Director of National Intelligence (ODNI) responsibility for Title 50 activities, or the U.S. Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) responsibility for counterintelligence activities," although according to the Commission, the NCD "would be kept fully apprised of those activities."[45]

There is no question that the idea of having a senior individual appointed by the President in the White House charged explicitly with the authority to coordinate the various members of the interagency who have responsibilities in the cyber arena—including offensive and defensive efforts—is a good one. Indeed, given the wide range of agencies that have some piece of the government's offensive and defensive cybersecurity missions, there is every reason to believe that strong, centralized leadership in the White House will help get things done and move the ball faster than without such a strategic position. Indeed, if one just counts the primary action agencies with core responsibilities, which includes (but is not limited to) DHS's CISA, DOD's U.S. Cyber Command and NSA, DOJ's FBI, and ODNI, it very quickly becomes clear that coordination is critical if the government is to achieve unity of effort.

And in fact, in the past three Presidential administrations, George W. Bush, Barack H. Obama, and Donald J. Trump, something approaching a position with coordination authority has existed, at least until fairly recently (and some might argue even now, albeit significantly cut down and without the level of influence and authority that most experts would agree is necessary to succeed). Indeed, under Presidents George W. Bush and Obama this position had significant influence and coordination power.

For example, under President Bush, Neill Sciarrone, working with Melissa Hathaway in the Office of the Director of National Intelligence, was able successfully steer the then-single largest executive branch effort on cybersecurity—HSPD-23/NSPD-54 – President's Comprehensive National Cybersecurity Initiative—successfully through the interagency process to completion. Likewise, in the Obama Administration, successive inhabitants of the office including Ms. Hathaway, Howard Schmidt, and Michael Daniel has significant influence and strong coordination roles as did various Assistants to the President for Homeland Security and Counterterrorism like John Brennan and Lisa Monaco. Indeed, even in the early part of the Trump Administration, there is general agreement that Rob Joyce had significant influence and coordination authority in the cyber arena as did Assistant to the President for Homeland Security and Counterterrorism Tom Bossert.

---

[44] *See* Cyberspace Solarium Commission, *Commission Report*, *supra* n. 32 at 37.

[45] *Id*. at 38.

Given the general agreement that such coordination is advisable, and indeed, necessary, one needs wonder why the Commission's approach might be controversial.

The first and most obvious issue that would likely trouble any White House—regardless of political party and relationship with Congress—is the idea of having yet another Senate-confirmed appointee in the White House Office. As it stands today, there are four prominent Senate-confirmed officials in the White House Office, the Director of the Office of Management and Budget, the United States Trade Representative, Director of the Office of Science and Technology Policy, and the Director of the Office of National Drug Control Policy.

Of these positions, two relate directly to matters that are textually committed to Congress, namely Congress's power of the purse (e.g., the ability to tax and spend)[46] in the case of OMB, and the Congress's authority to lay duties, imposts, and excises and to regulate commerce with foreign nations[47] in the case of USTR. As such, both of these positions are core to the relationship between the White House and Congress. The other two positions relate to areas, at least in the White House that are not particularly core to that executive-legislative relationship. And, as a result, even though successive Presidents appointed individuals to all four positions, there is little question that the Directors of ONDCP and OSTP wield drastically less influence in the White House than the Director of OMB and the USTR.

The challenge, of course, with a National Cyber Director, particularly as it relates to a position in the White House Office and as described in H.R. 7331, is that this individual would have responsibilities that are generally understood by Presidents to be squarely in their control, namely matters related to the execution of the President's textual Commander-in-Chief responsibilities. And while Congress may certainly argue that it has a number of textual commitments in this area also, like the declaration of war authority and the provisioning of the armed forces, the reality is that Presidents have long taken the view that matters of national security decisionmaking, particularly in the White House, are firmly committed to their discretion. Thus, it is likely that any President, regardless of party or relationship with Congress, would be strongly opposed to Senate-confirmation of such an individual and, if such confirmation was ultimately required, it may actually undermine rather than buttress the individual position's influence and role within the White House.

Moreover, making such a position Senate-confirmed essentially seeks to elevate it to an Assistant to the President role, namely a principal officer inside the White House Office. The challenge with doing so, of course, is that the vast majority of issues such an individual would deal with likely also fall squarely within the ambit of the existing responsibilities of the Assistant to the President for National Security (i.e., the National Security Advisor). As a result, if such a position were to be created, it would likely create core conflict within the White House Office: either an NCD whose national security-related decisions and advice would go directly to the President without the views of the National Security Advisor or you'd have filtering of the views of a Senate-confirmed individual in the White House Office through the National Security Advisor who is, of course, not Senate-confirmed. The legislation clearly envisions the former

[46] U.S. Const. Art. I, Sect. 7, cl. 1 & Art. I, Sect. 8, cl. 1 & Art. I, Sect. 9, cl. 7.

[47] U.S. Const. Art. I. Sect. 8, cl. 1 & Art. 1, Sect. 8, cl. 3.

approach—that is, direct advice to the President—which could very well create its own set of coordination and integration challenges within the White House and with the interagency.

This challenge is enhanced, in particular, when it comes to areas of clear overlap between existing White House officials like the National Security Advisor (e.g., in the case of offensive and defensive cyber operations), as well as the Director of OMB (e.g., in the case of budgetary authority).[48] Where the situation becomes even more problematic, however, is where the NCD's assigned authorities appear to directly conflict with the authorities of another cabinet-level official. So, for example, when it comes to H.R. 7331's authorization to the NCD to "direct" the federal government's response to cyberattacks and cyber campaigns of significant consequence, including developing operational priorities, requirements and tasks, and ensuring deconfliction and execution of operational activities, one might not be surprised if such a proposal encounters extremely stiff resistance from the President, on behalf of the Department of Defense and the Commander of U.S. Cyber Command. After all, while it is not unusual to have the National Security Advisor play a coordinating function across a wide range of national security matters, it is rarely the case that the National Security Advisor is called upon to direct responsive military activities. A similar problem could also arise with the Secretary of State if, as the Commission envisions, the NCD would be the primary representative of the United States to foreign governments and international bodies on cyber matters.[49]

Finally, the size of the office likewise presents its own challenges. While it is true that the USTR has an office of over 200 individuals and OMB has nearly 500,[50] even at 75 authorized individuals, when one adds in the authority for other outside experts, consultants, and other government agency personnel in support, this number is likely to be viewed as too high for the mission. This is particularly the case given that such an office would be roughly 1/3 the size of the entire National Security Council staff, which itself is currently seen as fairly bloated (even after the Trump-directed staff reductions in 2019).[51]

VI. Recommendation and Conclusion

With all of these challenges, the question is whether having a Senate-confirmed individual is critical to the effort and, if so, whether placing that person outside the White House Office may be a more successful approach. At the end of the day, a more subtle approach working within the White House may be most advisable. Such an approach could involve Congress working collaboratively with the President to determine how best to ensure the long-term existence of a position focused on cybersecurity coordination with elevated rank (i.e., Deputy Assistant to the President) and to ensure the appointment of individuals with sufficient expertise and cachet to

---

[48] *See, e.g.*, Mieke Eoyang & Anisha Hindocha, *Reexamining the Solarium Commission's Proposal for a National Cyber Director*, Lawfare (May 21, 2020), *available online at* <https://www.lawfareblog.com/reexamining-solarium-commissions-proposal-national-cyber-director>.

[49] *Id.*

[50] *Id.*

[51] *See* Kathryn Dunn Tenpas, *Crippling the Capacity of the National Security Council*, Brookings Inst. (Jan. 21, 2020), *available online at* <https://www.brookings.edu/blog/fixgov/2020/01/21/crippling-the-capacity-of-the-national-security-council/>.

move the office forward, as well as small, elite leadership team of 5-10 individuals, made up of significant footprint of cyber-experienced political appointees and additional detailees to support.

One approach to solving this problem may be to adopt the method used by Congress to create the NSC Executive Secretary as well as to require the assignment a coordinator for malign foreign influence campaigns.[52] The one challenge this approach raise is the question whether such an individual, required to be appointed by statute, could also be required to be a commissioned officer. Assuming not, Congress may wish to use the same approach it took with respect to Special Adviser to the President on International Religious Freedom (e.g., a sense of Congress provision)[53] and could also consider adding specific, directive cyber coordination language to the National Security Council functions, as was done with respect to malign foreign influence campaigns.[54] Likewise, Congress could put in statute a requirement that the cyber coordinator must brief Congress regularly as was done with the malign foreign influence campaign coordinator.[55] These approaches, done right, could achieve many of the goals sought by the Commission, without creating the key problems described herein.

Thank you again for the opportunity to present my views to the Committee. I look forward to discussing your questions and ideas.

[52] *See* 50 U.S.C. § 3021(e)(1) & 50 U.S.C. § 3021(g)(1).

[53] *See* 50 U.S.C. § 3021(f).

[54] *See* 50 U.S.C. § 3021(b)(4).

[55] *See* 50 U.S.C. § 3021(g)(2).