PONDURANCE

Testimony to the Defense Subcommittee of the House Appropriations Committee

Niloofar Razi Howe

Fellow, International Security Program, New America

March 23, 2021

Chairwoman McCollum, Ranking Member Calvert, and distinguished members of the Subcommittee, thank you for inviting me to testify today on future challenges in cybersecurity. I am a Fellow in the International Security Program at New America, a D.C.-based non-partisan think tank, and I also serve on a number of corporate and government advisory boards. I have spent close to three decades in the technology sector, with the last 15 years focused on innovation in the national security and cybersecurity sectors. I have been a venture capitalist, an entrepreneur, and a corporate executive in the cybersecurity industry. I have examined cybersecurity issues through a variety of lenses and across multiple disciplines. I hope to put those experiences to use to help develop new approaches and durable solutions to an evolving and complex threat landscape. In this testimony, I hope to lay out the most critical areas of concern and propose options to create resilience to these issues.

Introduction

2021 will go down as one of the most consequential years in cybersecurity and its only March.

The theft of defense secrets, personally identifiable information, and intellectual property, especially by China and Russia, is a key feature of strategic competition in cyberspace today. The SolarWinds supply chain operation by Russia and exploitation of Microsoft Exchange Servers by China are just the latest examples of how sophisticated these adversaries have become, purposefully using U.S. infrastructure to launch devastating attacks against tens of thousands of organizations in a short period of time. They have proved themselves extraordinary opponents who are able to adjust, evolve, and move with a sophistication and rapidity that evades our best defenses and exploits our technical, human, legal, and regulatory vulnerabilities. Efforts to expose Chinese and Russian malicious cyber operations have done little to diminish the pace or scope of these operations. Cybercrime has also become a profitable industry filled with criminal gangs that operate with impunity in jurisdictions that openly harbor them. Ransomware attacks are rising exponentially, as are the accompanying extortion demands. No organization is too big or too small to be targeted and the incident costs are rising at an accelerating pace.

As we adopt new disruptive technologies at an unprecedented rate, we layer complexity into our interconnected digital landscape, which only increases our vulnerabilities. For example, a McKinsey report describes today's modern car as a data center on wheels with more than 100 million lines of software code, (four times that of a fighter jet), reflecting the increasing complexity of systems in connected and autonomous cars.

Complexity is the enemy of safety and security.

We live in a software-based world and the best militaries will soon be defined by the best and most agile software developers. Over time, almost everything that we have experienced in the physical world—prosperity, democracy, corruption and warfare—will happen digitally, but with a speed and severity that we are just starting to comprehend. At the same time, cyber capabilities that enable attacks are becoming increasingly commercialized, offered as a service by groups that specialize in specific aspects of the chain, creating a fundamentally asymmetric dynamic where defending against these attacks is increasingly difficult.

While there are no silver bullets, without a concerted effort to both restore deterrence and impose cost on our adversaries while building resilience through improved cyber defenses, this trend will only worsen over time.

I appreciate the opportunity to explore this complex topic and will conclude by proposing a series of actions focused on the twin pillars of restoring deterrence and building resilience in cyberspace.

Let's start with our challenges in cyberspace.

Background: The Russian and Chinese Intrusions

Over the past few months, cybersecurity experts have uncovered Russian and Chinese cyber attacks against a broad set of government and private sector targets. While the full extent of these attacks is not yet known, the scope and scale are massive, with tens of thousands of global victim organizations, ranging from police and fire departments to the federal government, cybersecurity vendors, and even allies like the Norwegian Parliament and the European Banking authority. The initial goal of these attacks was to access sensitive data such as U.S. defense production data, weapons systems designs, trade secrets useful to national and economic security, and, in China's case, any information related to potential political enemies. The ultimate goal remains to be seen. These attacks are just the tip of the iceberg. Undoubtedly there are other cyberattacks taking place right now by these and other adversaries that we are completely unaware of.

The Russian operation, called SolarWinds or Holiday Bear, and the Chinese intrusion targeting Microsoft Exchange servers, show that malicious cyber actors have been able to adjust their tradecraft, tools and techniques, and procedures. They are adapting in order to take advantage of vulnerabilities that exist in our systems and at the entanglements caused by these systems, and are shielded by an ossified regulatory and legal structure that cannot keep pace with the reality of cyberspace and the agility and creativity of those who wish us harm.

Russia, which has historically been a "noisy" player in the cyber arena, seems to have learned from past cyber operations, including Operation Fancy Bear and Cozy Bear (GRU) targeting the DNC, the RNC, Clinton Presidential Campaign, as well as the World Anti-Doping Agency, the U.S. Anti-Doping Agency, a U.S. nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), as well as the Spiez Swiss Chemicals Laboratory. Russia has adapted its cyber strategy to more closely mirror its human espionage strategy, adopting a more patient, disciplined, restrained approach that is focused on gaining maximum access and advantage. The highly effective SolarWinds campaign should shake loose any vestiges of complacency in appreciating the difficulty in making our organizations resilient to committed adversaries.

China's multi-stage intrusion into Microsoft Exchange servers, which was first detected in January, is now fueling a spate of ransomware attacks against companies unable to keep pace with patching their systems in real-time. This attack seems to indicate that China has no fear of attribution or retribution and is uncharacteristic of its typically controlled posture in cyberspace. Like SolarWinds, China's Microsoft hack takes advantage of widely distributed technology infrastructure, in this case Microsoft Exchange email service. This intrusion enabled unauthorized access to entire email systems of tens of thousands of organizations and follow-on access to connected databases that store sensitive information, intellectual property and trade secrets, as well as personally identifiable information. China's operation first started on January 3, 2021 according to cybersecurity firm Veloxity, which discovered and disclosed the attack on March 2, 2021. While Russia, once discovered, hit the kill switch and has seemingly disabled their access to compromised systems, China has chosen a radically different approach. Rather than disabling its access, China quickly installed backdoors (known as "web shells") on at least 30,000 systems. These backdoors exponentially increase the scale of harm that can be inflicted and can be exploited for second stage attacks, such as ransomware, by all manner of malicious adversaries who have mobilized almost overnight using automation to identify and attack targets that have not yet patched their systems (often despite best efforts). Due to the proliferation of threat actors and the ubiquitous availability of offensive tools that exploit undisclosed vulnerabilities or "0-days", nation-states as well as cybercriminal gangs can mobilize quickly to take advantage of even a rumor of a new vulnerability, as they did in this case.

These intrusions underscore the fact that no matter how sophisticated our defenses, no matter how vigilant we are in training and educating, human error from conventional software development processes, coding vulnerabilities, and not properly maintaining and updating our systems will always leave a door open for committed adversaries, a door we need Congress' help to close. Everything we do is increasingly IP-enabled and the security of our systems and our networks is inversely proportional to the number of nodes, the number of users, and the number of applications it supports. Marc Andreessen, the inventor of the first web browser, famously wrote, "software is eating the world." He may not have appreciated that software is also eating our security.

According to a Microsoft report, as of March 12, approximately 80,000 of Microsoft's 400,000 customers had yet to update their servers, a drop from approximately 100,000 unpatched systems on March 9. During that same time, one cybersecurity firm observed that the number of attempted attacks grew ten-fold from about 700 to over 7,000.

Even when we do move fast, our adversaries move faster.

Our adversaries are bold and perhaps more importantly, they are able to evolve. They study and understand our technical and operational weaknesses and our blind spots and will continue to take advantage where they can to the detriment of our political, economic, and national security. No matter what new defenses we put in place, so long as we remain connected to the Internet, our adversaries will adapt, adjust, and find new ways to exploit our systems. And they will do it with a rapidity that is breathtaking.

As we examine the evolution of malicious cyber operations over time, from Destover (the 2014 attack against Sony Entertainment) and Crash Override (the 2016 attack against Ukraine's power grid) to NotPetya and SolarWinds, we can see the speed with which our adversaries adjust their tactics, find and exploit weaknesses, and extract valuable information. Soon enough, they will disrupt and destroy infrastructure as they have done to other countries. The damage they can inflict in a short period of time is massive. For example, NotPetya, the 2017 cyber attack that was also attributed to Russia, combined ransomware and wiper software that destroyed data. It invaded corporate networks through a corrupted software update from a small firm in Ukraine and was able to infect thousands of computers globally in just minutes; it ultimately cost businesses $10 billion in damages. We must respond with equal agility and speed if we are to have a chance to defend our systems, our country, and our people.

Three specific issues that exacerbated issues related to both SolarWinds and Microsoft Exchange are worth deeper examination: (1) the use of U.S. infrastructure by nation-state adversaries, (2) ubiquitous supply chain risk, and (3) lack of information sharing mandate.

The Use of U.S. Infrastructure by Adversaries

One especially troubling aspect of the recent Russian and Chinese operations is the use of U.S. infrastructure (i.e., from U.S.-based servers) as the launching pad for malicious activity. Both the SolarWinds and Microsoft Exchange attacks took full advantage of an intelligence blind spot created by a legal framework that prohibits U.S. intelligence agencies, such as the NSA, from conducting operations inside the United States and legal processes that move too slowly for the FBI to disrupt operations. This is not a new issue. Time and again, our adversaries in cyberspace are able to operate undetected on U.S. infrastructure and the current approach, which relies heavily on voluntary information sharing and incident reporting, is not working.

Both the SolarWinds and the Microsoft attacks show that we have created an unintended "lawless zone" inside the U.S. We should expect our adversaries to take full advantage of this blind spot, which includes disposable infrastructure such as Virtual Private Servers, for their attacks against our government and our companies. We can expect that with full awareness of the legal standards restricting U.S. government access to domestic information and infrastructure, especially for surveillance and law enforcement purposes, our adversaries will continue to launch their operations using our technology infrastructure against us.

Supply Chain Risk

The security of our digital ecosystem is directly correlated to the least secure supplier, customer, vendor in that ecosystem. Russia's SolarWinds attack also reveals that long-term campaigns focused on supply chain vulnerabilities can be very difficult to detect and, by extension, incredibly productive for the attacker, regardless of whether the goal is network attack or espionage. Russia lay dormant for months, perhaps longer, after successfully introducing back doors and stolen keys into various technology infrastructure companies, testing their code, testing their stealth. The attack was inadvertently discovered by one of the victim companies, cybersecurity firm FireEye, but only after running forensics on thousands of machines and tens of thousands of files. Very few organizations could have dedicated the resources necessary for uncovering the root cause and scope of the compromise in a timely manner. FireEye was able to do it in days.

Lack of Information Sharing

FireEye was under no legal obligation to disclose discovery of the SolarWinds breach, bringing to light another shortcoming of our regulatory framework, which is primarily focused on data privacy and breaches affecting personal information. Voluntary disclosure is a rare thing and often brings with it serious legal liability that most organizations will legitimately shy away from. In this case, without FireEye's voluntary disclosure of the breach and the technical details necessary to defend against it, Russia would likely still be collecting information from this operation.

The Broader Cyber Threat Landscape

Unfortunately, SolarWinds is not a unique campaign. We must assume that quiescent malware resides throughout our infrastructure, throughout the long tail of vendors to our most critical agencies, waiting to be stealthily called into action at the right time. Even if discovered, once activated there is no mandatory disclosure requirement that could serve as an early warning system for other potentially vulnerable organizations.

Securing cyberspace, and by extension, everything that connects to it, is incredibly hard. Underpinning all of our struggles is the fact that the Internet was constructed in an environment of trust, and that assumption has turned out to be an increasingly damaging flaw. When the internet was originally conceived in the mid 20th Century and operationalized in the 1990s, the vision was utopian—universal connectivity and universal interoperability based on the premise of openness. The Internet was also anti- establishment in that it was not subject to national sovereignty nor to nation-state governance—instead it was to be governed by a multi-stakeholder, transnational, stateless, nationless, borderless body based on universal shared principles, standards, norms, and values. Sadly, though not surprisingly, none of these principles, standards, norms, and values are shared by our adversaries.

As the Internet has matured and we have operationalized every aspect of our lives in this domain, we have become personally, economically, politically, and militarily dependent on cyberspace and the threat this dependence represents has grown in kind and in effect. We are witnessing that, from ransomware, Intellectual Property theft, to cybercrime, espionage, and cyber conflict/cyber war, influence campaigns, the rise of misinformation/disinformation, cyberviolence, cyberbullying, and exploitation. The malfeasance that takes place in this domain seems endless.

Global events only add fuel to the fire of cyber attacks. The COVID-19 pandemic caused a dramatic acceleration in digital transformation for all organizations as we pivoted overnight to a work-from-home model. As a result of this pivot, the Internet became the new corporate network and our attack surface expanded as pandemic related malfeasance took hold in cyberspace, from pandemic related phishing lures and ransomware campaigns to COVID-19 disinformation and vaccine-related IP theft.

While the threat landscape is endless, a few trends are worth focusing on.

Key Trends

The world is changing dramatically with a speed, scope, and scale that we have never experienced, partially fueled by a pandemic that forced every organization to accelerate its digital transformation projects. As we digitize business, economic, defense and social infrastructures, embrace cloud and edge computing, autonomous vehicles, 5G and microsensors, Artificial Intelligence, small low orbit satellites with advanced sensor platforms, the Internet of Things (IoT), drones, distributed ledger technology, augmented and virtual reality, autonomous weapons, quantum computing, and synthetic biology, to name a few, we must reimagine how we organize to defend against the threats each new technology brings with it.

One of the most pervasive and harmful cyber threats to organizations are ransomware attacks, both in terms of the disruption caused and monetary loss inflicted. The cost of these attacks is estimated to be between $40 billion and $170 billion globally. By encrypting files and demanding payment, hackers have quickly figured out how to monetize illegal access into networks, increasing the pace and sophistication of their techniques while demanding higher and higher ransoms over time, testing what price the market will bear, all with little fear of retribution or prosecution. Ransomware attacks are particularly pernicious and can fundamentally disrupt a government's ability to deliver critical services to its citizens for prolonged periods of time, as we experienced with attacks against a series of municipalities such as

Atlanta, Baltimore, New Orleans, Greenville, and St. Lucie to name a few.

Another threat is the almost nonexistent security features in IoT devices. IoT, powered by 5G networks, is being embraced by businesses to take advantage of the $11 trillion of economic gain waiting to be realized across the full spectrum of economic activity. Many of these devices are inexpensive and rely on slim profit margins and, with little to no regulation or liability, they generally lack even the most basic security features we have come to expect in our connected devices as manufacturers prioritize time to market and efficiency over security. The result is that most IoT devices have known vulnerabilities and have already become a key component of adversary attack tactics, such as botnets. From real world attacks on Industrial IoT such as the cyberattack on Israel’s water system, to a White Hat hackers successful hack of the Tesla Model S, to the novel Burn-In: A Novel of the Real Robotic Revolution by Peter Singer and August Cole, which examines 10 real-world IoT hacks that can bring Washington DC to a standstill, the lack of security in IoT devices presents an ever-growing threat to our resilience. As IoT devices proliferate in every corner of society from business-to-business applications in manufacturing, agriculture, healthcare, smart cities, ports, power grids and transportation to consumer applications such as home automation, their vulnerabilities will also proliferate into every aspect of our corporate and personal lives.

The growing market in low earth orbit satellites threatens to form the most ubiquitous surveillance platform ever built with no meaningful regulation to control what they are used for or by whom. Iran, for example, used ***commercial*** satellite images to monitor Ain al-Asad Air Base in Iraq as it prepared to launch more than a dozen ballistic missiles at U.S. and coalition forces on January 7, 2020. These platforms can now be easily tasked by government, corporations and individuals at low cost with few regulatory or technical limits. We are fusing the power of increasingly powerful sensors such as satellites, drones, and even robotic dogs and the breathtaking increases in the amount of signal (data) that is being generated by the explosion of IoT devices, together with improvements in artificial intelligence and machine learning. Fueled by the power of edge computing, this extraordinary combination of sensor, signal and intelligence leads us quickly to a world where every square meter of planet earth is under constant surveillance that can be accessed by any government, any corporation, and any individual for any purpose at any time. Space is commercializing. Space is democratizing. Space, powered by AI, is the next cyber battleground.

As more money pours into Artificial Intelligence from governments and technology firms, the ramifications are poised to be immense and by definition beyond what the human brain can comprehend. Like IoT, AI is being rapidly adopted across industry, from finance, manufacturing, pharma and healthcare to applications such as cybersecurity. AI modeling is highly dependent on the integrity of data used in training its systems and protecting that data from compromise, manipulation and poisoning will be critical. We are at the very early stages of developing approaches to detecting and remediating data manipulation and need to invest the resources necessary to ensure we are developing the right resilience and response capabilities for the AI sector. We have time but should not be complacent.

An emerging threat is the digitization of fragile societies without thought to security ramifications. This trend poses a credible security risk both to those societies and possibly to the broader interconnected world. While 60% of the world's population is already online, many of the people who are now being brought online live in some of the world's most chaotic geographies. While access to the Internet will enable them to access the benefits of the digital economy such as digital finance, virtual education and exchanges, virtual healthcare, as they get connected via the Internet, with few norms to truly govern behavior or those who seek to destabilize and manipulate them, we must be prepared for new forms of malfeasance and exploitation. This is especially true if we are operating without a commitment to global digital literacy. As one example, the rollout of Chinese digital currency is actually the rollout of a new form of ubiquitous economic surveillance.

The threat of influence operations leveraging social media platforms continues unabated. Foreign intelligence services and proxies continue to embrace U.S. social media platforms to spread misinformation and disinformation in ways that undermine U.S. society and interests, including our need for a well-functioning democracy. The growth and reliance on social media in the United States has enabled our adversaries, especially Russia and China, to engage in State-on-Individual activities (manipulation) to exploit vulnerabilities in our society, amplify polarization, radicalize our youth, endanger communities, weaken institutions and undermine any sense of objective truth in society. These activities undermine the Root of Trust necessary for a well-functioning democracy. On Facebook, websites promoting coronavirus conspiracy theories have more than ten times the engagement as public health organizations. An Oxford University study of COVID-related disinformation documented 225 distinct conspiracy theory campaigns, 88% of which used social media as their hub. As recently as last week, WSJ reported that three online publications directed by Russia's intelligence services are spreading disinformation to undermine confidence in Pfizer and Moderna's COVID-19 vaccines. By definition, polarized societies are ineffective at governance as there is no common ground to build consensus to enact bipartisan policies, laws, and regulations that benefit all of society. As our ability to govern erodes, so does people's faith in the government leaders and their political system. The 2021 Edelman Trust Barometer puts numbers against the "raging infodemic that feeds mistrust" finding that businesses, not government, emerge as the only trusted institution that is viewed as being both competent and ethical. The cost of doing nothing to stop disinformation and misinformation campaigns now outweigh the risk of doing something.

Underpinning all of these issues is the fact that human beings have obsolete mental models and cognitive biases that perhaps were useful when we lived in caves, surviving attacks from the wild, but do little to help us in the age of technology acceleration or protect us against our increasingly vulnerable digital existence. A human being sits at the intersection of our networks and devices and continues to be the weak link in our security programs and architecture. For example, 91% of all cyber attacks start with a phishing email, which still drives a better response rate than most marketing programs. This human, with flawed mental models, is also responsible for developing the policies, laws, and regulations to protect our people and our businesses from harm. The pace at which we have historically developed societal and government solutions, adapted to new technologies, and built consensus with respect to our most pressing problems is too slow for the age of technology acceleration. It is time to change our perspective and mental model with respect to the timelines we must operate on, the agility with which we take action, and the collaborative model we employ. Our adversaries have.

There are no easy answers, no silver bullets.

While eliminating the threat is almost impossible, at least in the near term, there are actions we can take over time that can restore deterrence and lead to greater resilience—resilience of our systems, resilience of our agencies and organizations, and resilience of our society. Focusing on deterrence and resilience is critical as new waves of technology innovation are adopted at a blindingly fast pace. As the scope, scale and pace of technology innovation increases so does the complexity of our systems and, by extension, the opportunity for malfeasance. We cannot ignore the tremendous economic gains that accrue to early adopters who will not wait for security to launch pilot programs and test new and disruptive technologies but we must develop solutions that enable us to respond rapidly to new threat vectors and new techniques, creating resilience to the vulnerabilities they create.

To do this well and on a timeline that is relevant we must rethink our approach to cybersecurity and cyber defense with a clear understanding and appreciation for the unique role the U.S. government must play in leveling the playing field. The harsh reality is that the issue is not when we suffer attacks but how quickly we can react and recover from these attacks.

A Framework for Solutions

To defend our strategic position in cyberspace requires a willingness to both impose cost on malicious actors by restoring deterrence as well as improving our defensive capabilities by building resilience.

1. Restoring Deterrence

Deterrence is the unique purview of government. Government must do what only the government can do—deter malfeasance in cyberspace, especially by nation-state adversaries, by using our tools of national power against those who are harming us. The private sector cannot defend itself alone against nation- state adversaries and criminals who are agile, persistent, and creative and who operate with no fear of reprisal. Even the strongest walls will eventually succumb to a capable, well-funded adversary if there is no deterrence. In 2018, Peter Singer, a Senior Fellow at New America, wrote about the collapse of cyber- deterrence: “Less generously, these trends have created the opposite of deterrence: incentives. The failure to clearly respond has taught not just Russia and China, but any other would-be attacker, that such operations are relatively no pain on the cost side, and all gain on the benefits side. Until this calculus is altered, the United States should expect to see not just Russia continue to target its citizens and institutions but also other nations and non-state groups looking for similar gains.” His observation is even more true now in the wake of current events. Strong deterrence is the cornerstone of any security framework and the U.S. government must take up this challenge in a decisive and consistent way.

- **Reduce the threat of ransomware by imposing cost on Russia and those harboring these groups.** The only way to have a meaningful impact on the ransomware industry is to impose significant costs on the nations harboring these criminals and enabling them to commit their crimes with impunity and with no fear of reprisal or prosecution. In a recent interview, a representative from the audacious Russian ransomware-as-a-service hacking group REvil (aka Sodinokibi), bragged, ”For me personally, there is no ceiling amount. I just love doing it and making a profit from it. There is never too much money—but there’s always the risk of not enough money.” Asked why he was willing to give the public interview, he replied, “Unusual ideas, new methods, and brand reputation all give good results.” Ransomware has become a plague infecting organizations globally with devastating effect. It has also become an incredibly profitable business model for the criminal gangs, mostly Russian, who carry them out. These gangs are comfortable bragging about their techniques, building brand reputation, and pulling in millions (or perhaps hundreds of millions) of dollars in profits each year. If the SolarWinds campaigns does not expand beyond its current apparent aim of espionage, imposing cost on Russia for this attack may make little doctrinal sense. Imposing cost on Russia, especially with economic tools of national power and policy (sanctions, embargoes, tariffs), for creating a safe harbor for these criminals is, however, justified and in line with global norms. Without a fundamentally different approach to the problem, we can expect to see the number, cost and extortion demands of ransomware attacks continue increasing with no ceiling in sight. Stopping ransomware attacks serves the dual purpose of both reducing the cybersecurity threat landscape, especially for resource-constrained entities like hospitals, schools, and state and local governments, which are often the target of these attacks, but more importantly, allowing our incident responders and security professionals, who are overwhelmed responding to ransomware attacks, to focus on detecting and responding to more sophisticated attacks like the SolarWinds and Microsoft.

- **Develop an offensive strategy aimed at inspiring fear and respect in our adversaries.** Almost a decade ago, Crowdstrike co-founder Dmitri Alperovich said, “We do not have a cyber problem, we have a China, Russia, Iran, North Korea problem.” The most consequential cyber intrusions of the past few years have been executed by nation-states and developing a coherent framework for deterring and responding to malicious activity by nation states (as well as their proxies) in cyberspace that we apply on a relentlessly consistent basis is critical. We must adjust our legal framework to empower U.S. government agencies to collect the necessary intelligence to detect, attribute and defend against these activities, and do it in a way that does not abrogate civil rights. We must create friction and impose cost on countries that attack us—our people, our companies, our government, our democracy—and do it in a way that is consistent with the U.S. Constitution and the values of our democracy. The standup of USCYBERCOM and the implementation of its defend forward and persistent engagement strategies under General Nakasone is an important and impactful evolution of our strategy, and it should be integrated into a broader framework that includes all tools of national power-- economic, military, diplomatic, and cyber. This framework should also include a national cybersecurity strategy that builds up our defensive capabilities with respect to critical infrastructure sectors likely to be on the receiving end of these attacks against the U.S. The creation at the NSC of a strategic cyber position is a critical move toward creating such a strategy.

- **Deter adversarial activity on U.S. infrastructure.** Our adversaries are taking advantage of our laws, regulations, and authorities, including our blind spot on U.S. infrastructure, in designing their cyber operations for competitive strategic advantage in cyberspace. There are a number of actions we can take to address this threat. We can grant new authorities to intelligence agencies and law enforcement agencies so that they can effectively and efficiently carry out their mission against malicious actors operating on U.S. networks with the rapidity that is required to be responsive. Additionally, Congress can support “Know Your Customer” (KYC) requirements similar to the Anti Money-Laundering scheme used by the Financial Services industry including requiring network providers to report suspicious activity to DHS or the FBI. A KYC scheme would raise the bar on adversarial activity removing the shield of anonymity in these operations, especially with respect to the use of disposable infrastructure such as Virtual Private Servers, which can be spun up and spun down faster than law enforcement can keep pace today.

- **Continue Building Public-Private Partnership.** If our ultimate goal is defending our nation by defeating our adversaries in cyberspace rather than accommodating them, then, in addition to establishing acceptable norms of behavior, developing and committing to a consistent policy of engagement, escalation and deterrence, we must have a working model for successful public-private collaboration and engagement empowered to move with the agility and rapidity of our adversaries. Defeating our adversaries presupposes our ability to harness the vast technical expertise and resources as well as the unique authorities of the federal government, the vast technical expertise and agility of the private sector, a collaborative intelligence gathering and sharing framework, and coordinated response planning. There have been great examples of effective partnership over the past few years, especially at DoD, including the collaborative efforts by NSA, USCYBERCOM, FBI, CISA and the private sector to protect the 2018 midterm and 2020 Presidential election from foreign interference, the collaborative effort in 2020 by NSA, USCYBERCOM, HHS and private sector to protect vaccine developers from cyber intrusions, DoD's CIO delegation of authority to NSA in 2020 to share cyber threat information and cybersecurity guidance directly with the Defense Industrial Base companies and their cybersecurity providers, the standup of NSA's Cybersecurity Directorate in 2019 and its continuous engagement and information exchange with other federal agencies as well as the DIB and private sector on advisories and other guidance regarding adversary activity, threats, and techniques, and CYBERCOM's DREAMPORT initiative in 2018 to enable cyber innovation between the Command and private sector. We have experience showing the meaningful outcomes that these partnerships can drive and must continue building them, reducing barriers (legal, policy, or provincial) to cooperation and operational collaboration. One recently proposed solution is the creation of a National Cyber Response Network (NCRN). Building on the great work done by Cyberspace Solarium Commission Report, the 2021 National Defense Authorization Act (NDAA), and the Aspen Cybersecurity Group, the NY Cyber Task Force recently published a report emphasizing that the creation of an NCRN can build upon existing public-private partnerships if empowered in advance with appropriate authorities to orchestrate specific response actions for cyber defense during severe cyberattacks.

- **Reclaim our leadership-setting technology standards.** For decades, our nation has played a critical global leadership role, providing vision, diplomacy and stability to further our interests and our allies' interests, and this role is core to the trust and partnership required for a stable society and effective governance at home and around the world. We must do this in the digital world as well. To move us to a world of resilient systems and a resilient society, we must reclaim our technology innovation edge and set the standards for our digital infrastructure, which increasingly underpins every aspect of our existence. We cannot allow our adversaries, especially Russia and China, to set the norms and standards globally for technology, including cyber, at International Government Organizations. The United States must counter with a democratic alternative, working with allies, together producing a deterrent effect with standards that deter malicious activity, reduce the attack surface and promote resilience. We effectively surrendered global leadership of 5G standards to China because we were driven by outmoded assumptions and a misguided unilateral position. We cannot repeat this mistake with future technologies such as AI.

2. Building Resilience

While eliminating the threat is not possible, by continuing to raise defensive capabilities, we can make it harder for our adversaries to run sustained intrusion campaigns and create resilience for our organizations even when they are successful.

- **Reduce our vulnerability to digital supply chain risk and the long tail of suppliers and contractors to our most critical organizations.** Asking every organization to determine for itself whether or not a supplier poses acceptable or unacceptable risk is a recipe for failure. We should institute a program where software vendors relied upon by our most critical organizations and in our most critical sectors are subject to risk assessments (including audits of their software code and development practices) and a certification process that creates a "trusted list" of acceptable vendors. The Cyberspace Solarium Commission recommended the creation of a National Cybersecurity Certification and Labeling Authority and the European Union recently promulgated regulation requiring Member States to establish, publish, and maintain trusted lists. Given the global nature of technology and supply chains, coordinating a trusted list program with our allies as well as the private sector partners, is foundational to building resilience.

- **Next generation encryption is table stakes.** Sophisticated adversaries are both trying to exploit U.S. encryption while actively pursuing the development of a quantum computer, which can perform calculations exponentially faster than today's computers, potentially enabling them to destroy the encryption algorithms that currently protect our data and, by extension, our systems. Congress should make funding research to develop and deploy next-generation encryption a national priority.

- **Create a mechanism to compel mandatory disclosure and information sharing.** Government agencies, and especially the DoD, can make real time breach notification a condition of contracts with their contractor base, with penalties for noncompliance. Both SolarWinds and Microsoft intrusions underscored the importance of real time breach notification and information sharing by both public and private sector organizations. To this day, we neither know the scope nor scale of these intrusions as some victims have not publicly acknowledged the intrusions and others have disclosed very little. Public-private information sharing and cooperation remains a serious issue with legal liability concerns serving as the biggest deterrent to disclosures and without legislative mandate it is unlikely to become a reality. Understanding that the U.S. government's broad shift to commercial cloud services only introduces new avenues of cyber exploitation and therefore new risk, we must turn into this issue in real time. We must create a mechanism to compel confidential information sharing, including technical details, both by victim organizations as well as the first responders who investigate and restore the systems, and a liability safe harbor for such disclosures.

- **Set minimum Security Standards for IoT.** Congress should enact basic regulation with respect to IoT. The U.S. government can help protect the ecosystem of billions of connected devices by setting basic security standards, requiring features such as auto update, and importantly providing the right incentives, including tax incentives for vendors to implement these standards and corporations (including critical infrastructure) to deploy secure products and the financial headroom and reason to make changes.

- **Create Resilience by Establishing a Cybersecurity Civilian Corps.** While there have been a few enormous ransomware payments over the past few years by large corporations, by and large, the target of ransomware attacks are small and medium sized businesses and government entities that hold valuable information but are under-resourced when it comes to IT and cybersecurity. These organizations often do not have the budget to build specialized security teams, and even if they do, have difficulty recruiting and retaining top talent. As a result of their limited resources, they have limited ability to respond to ransomware attacks in real time. Over two years ago, as a solution to this problem, Natasha Cohen and Peter Singer of New America proposed the creation of a Cybersecurity Civilian Corps modeled after Civil Air Patrol or Volunteer Firefighters. Rather than competing with the private sector, this model would allow a public service organization that leverages private sector talent in a voluntary capacity, and provides the opportunity to serve the nation against a real national security threat. Much like volunteer firefighters, these volunteers could receive tax credits and training in return for their service, saving state and local governments hundreds of millions of dollars in expense. Such a program could draw on and be a training partner for local educational institutions, addressing the adjacent challenge of recruiting more people into the cybersecurity industry, with outreach programs such as clinics and competitions at local junior high and high schools, supplementing any existing programs. The Homeland Security Act of 2002 envisioned but did not follow through with the creation of a National Emergency Tech Guard program, a corps of volunteers whose training is funded by the government and who can be deployed during periods of crisis to restore critical systems and services to their communities. This idea may not be new, but the timing is right for Congress to support this type of program.

- **Future forecasting for resilience.** There is no unifying governmental organization tasked with looking "over the ridgeline" to assess future cyber vulnerabilities and their relative risk. There are many governmental and commercial organizations that perform aspects of this vital role, but they are disconnected from each other and overwhelmed with current priorities. For relatively low cost and little organizational friction, the U.S. government could task a single organization, perhaps a qualified University operating as an FFRDC, with the responsibility of focusing on future vulnerabilities in order to enable more forward leaning and effective planning for resilience. The CERT Coordination Center, which focuses on current attacks and vulnerabilities, is an FFRDC partnership between the U.S. government and Carnegie Mellon University. CERT is an ideal model to mirror for a clearinghouse organization, with no operational responsibilities, that can consolidate a global view of future threats that we have yet to completely imagine or defend against.

- **Leverage Private Sector Expertise.** The private sector has developed deep technical expertise in certain domains and the U.S. government must leverage the private sector better and not duplicate effort in areas where private sector capabilities now surpass government capabilities. In the threat intelligence market, while U.S. intelligence agencies can bring the full power of their capabilities to bear on a selected basis producing unique insights into foreign adversaries, the private sector has advanced capabilities across a broad group of actors (foreign and domestic), including insight into attacker behavior, tactics techniques and procedures (TTPs), and campaigns. Coordinating intelligence between the private and public sector to understand adversary behavior and create a coordinated response to defend and defeat the adversary is critical. As we build and invest in government capabilities, we must be careful not to duplicate or compete with private sector capabilities.

- **Empower Digital Citizenship.** "Misinformation is a long-term problem that demands long-term, sustainable solutions as well as short-term interventions," write Kristin Lord and Katya Vogt in Stanford Social Innovation Review. We live in a polarized, hyperconnected world of impatient digital citizens who are being continuously and creatively targeted with misinformation and disinformation. This human-centered problem requires human-centered solutions. Developing and funding media literacy programs that teach individuals how to discern the difference between fact, opinion, misdirection and lies, is critical to a well-functioning society and should be a national priority. IREX, a global development and education nonprofit organization[1], developed a Learn to Discern education program for the Ukrainian Ministry of Education to combat Russian disinformation campaigns. Their program integrated information consumption skills into existing secondary school curricula and teacher training programs at pre- and in-service teacher training institutes. Working with the non-profit community as well as the private sector, the U.S. government should fund the development of similar programs and curricula in the U.S. for our elementary, middle and high school students as well as for teacher training. With a broad digital literacy campaign, we can build resilience to state-sponsored disinformation campaigns, help individuals recognize divisive narratives, and improve our youth's ability to navigate increasingly polluted online spaces in a safe and responsible way. As we do this, we must pay close attention to misinformation innovations such as deep fakes, which present a unique challenge, and fund research aimed at identifying and mitigating the threat they pose to the very concept of objective truth. Support of research that can create an antivirus approach to deepfakes by focusing on their rapid debunking and attribution, coupled with requiring platform companies to require watermark on any known deepfakes are two potential strategies for reducing the possibility that deepfakes can be weaponized.

- **Organize USG to succeed.** From an organizational perspective, the U.S. government continues to be misaligned with today's cyber threat environment. There is a massive authority/capability mismatch with respect to the agencies most relevant to cybersecurity: DHS/CISA, NSA, FBI as well as Sector Specific Agencies, such as Treasury and Energy, which have deep expertise in their respective domains. We do not have time for provincialism or for aspirational thinking. As we define clear swimlanes for each of these agencies, we must remain realistic and clear-eyed about the capabilities that exist today, the leadership, timeline, and talent it would take to transform/upskill those capabilities, and, in the meantime, develop a plan to leverage talent as necessary from the agencies that have the qualified professionals to defend our nation in cyberspace. Make no mistake, enemies are currently exploiting this deficit to our increasing detriment. The move to agile has created tremendous benefits in software development by enabling a culture of rapid continuous delivery of software, responsive to changing circumstances and customer needs. A similar mindset shift in how the U.S. government operates and organizes in cyberspace in order to react, adapt and respond to real-time issues is a critical strategic imperative.

- **Cybersecurity and STEM Education.** Our fundamental challenges in cybersecurity will only increase over time if we cannot fill the talent to build the capabilities and design the policies we need to compete. All of society must focus on developing education programs to skill, reskill, and upskill individuals from all backgrounds into our industry regardless of their education level. In addition, to solve our most technical problems, including next generation encryption and quantum computing, we must inspire the next generation of students to embrace STEM careers. NSA's partnership with the National Science Foundation and ODNI provides a great model for an effective K-12 cyber outreach program. This program, known as GenCyber, which promotes cybersecurity education through summer camps for both students and teachers, with an emphasis on recruiting and retaining underrepresented groups in cybersecurity, started with eight camps in six states and has grown to 122 camps in 34 states reaching 5,000 students annually, 45% of whom are minorities. The National Centers of Academic Excellence in Cybersecurity program, also run by NSA in partnership with CISA and the FBI, supports 330 institutions and produces over 20,000 diverse graduates per year. The prototypes already exist for increasing STEM engagement at all stages of education with diversity and inclusion goals. With Congress' support, model programs like these can be rolled out more broadly across the country.

Conclusion

The growing challenges faced by the U.S. in cyberspace are at their core national security challenges that require a fundamentally different, more agile, more collaborative approach. Time is not on our side nor are we fully rising to the challenge. The recommendations outlined above are intended to support empowering a democratic society that is resilient enough to respond to the unintended consequences of technology innovation and the inevitable exploitation and use of those technologies by adversaries. These recommendations, and the many like them made over the decades by my colleagues, experts, working alone or as a part of commissions, task forces and working groups, can be the starting point of what will be a long and difficult journey toward cyber resilience.

Our adversaries are fast, creative, persistent, and unconstrained by law or regulation. Unless we change our approach, they will continue to identify vulnerabilities in software used across varied networks for maximum impact with little to no fear of retaliation. They will continue to advance intrusion tools and tradecraft faster than gaps in cyber defenses can be closed. They will continue to use common anonymization platforms, open source capabilities, generalized toolkits, and leverage inherent functionality built into operating systems to obfuscate their activity and make attribution difficult. They will continue to leverage our laws and regulations to enable their operations for maximum effect.

These first few months of 2021 should serve as a wakeup call to take the actions we know we must take, make the changes we know we must make, no matter how difficult the path, and do it with the agility, rapidity, and boldness of our adversaries. The clock is ticking. We are running out of time.

[1] *Niloo serves on the Board of Directors of IREX.*