Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

# CYBERSECURITY:

## CHANGING THE MODEL

Franklin D. Kramer
Robert J. Butler

# CYBERSECURITY:

## CHANGING THE MODEL

Franklin D. Kramer
Robert J. Butler

ISBN-13: 978-1-61977-587-9



April 2019

# CONTENTS

# 1. INTRODUCTION AND SUMMARY

There is a cybersecurity gap. Despite all efforts, adversarial cyberattacks are outrunning defender security improvements in technology, processes and education. Accordingly, this report recommends a change to new models of cybersecurity that will deliver significantly better results for the key arenas of: critical infrastructures; states, cities, and localities; the federal government; and the international sphere. Crucially, the federal government would enhance its active involvement, expanding support for "coordinated partnerships" in those key arenas, and Congress would provide additional resources and authorities requisite to the task. The private sector would likewise play a key role engaging and supporting coordinated partnerships, including in the development of advanced technologies and the use of critical capabilities such as cloud technologies, automation, and artificial intelligence. The important outcomes would result from coordinated actions, sustained and focused funding, and development and implementation of advanced technologies.

- For the key critical infrastructures of energy, finance, transportation, telecommunications, and water treatment, this report recommends the establishment of an enhanced public-private model, with the federal government and key enterprises organizing coordinated, advanced protection and resilience, intelligence sharing, and active defense. The government should provide annual budgetary support and financing for costs incurred, and should utilize its capabilities to "defend forward… to stop threats before they reach their targets."

- For states, cities, and localities, this report recommends moving from a largely decentralized and under-resourced approach to a full-fledged, state-centric cybersecurity expert center, to coordinate state-level cyber efforts including: law enforcement and the National Guard; provision of cybersecurity by the state as a service to cities and localities; and establishment of structures and procedures for the federal government to provide states with annual cybersecurity budgetary resources to increase education, training, and exercises, and to undertake "attack protection" through active defense and a "defend forward" approach.

- For the federal government, this report recommends the establishment of a National Cybersecurity Fusion Center featuring: intelligence and operational capabilities; increased support to critical infrastructures and state, city, and locality entities, including establishment of a federal cybersecurity budget for these enterprises; expanded use of active defense and "defend forward"; an increased focus on the Department of Defense (DoD) overcoming vulnerabilities and enhancing cybersecurity resilience, including providing a standard "resilience architecture" for contractors and subcontractors; and significant additions of cybersecurity personnel and budgetary funding to the Department of Homeland Security (DHS) and the Department of Defense.

- For international activities, this report recommends organizing around likeminded countries and organizations, including through: the establishment of an International Cyber Stability Board; provision of protection and resilience to key cross-border critical infrastructures, including finance and transportation; undertaking a multinational campaign response to malignant cyber actions by significant nation-state and criminal threats; and enhancing capabilities to defend against armed attack, including with allies and close partners.

Congress will have a critical role in achieving these objectives. Legislation will be required for

- establishing a National Cybersecurity Fusion Center that will coordinate intelligence and operational actions focused on cybersecurity resilience in the United States, to include timely technology insertion, streamlined processes and continuous learning;

- providing requisite authorities for federal support to cybersecurity for key critical infrastructures, and to states, cities, and localities;

- creating an annual federal budget line to support cybersecurity for states, cities, localities, and key critical infrastructures;

- establishing a federal budget line item to support cybersecurity for the federal government, and increasing the number of cybersecurity personnel at the Department of Homeland Security, pur-

suant to a programmatic plan presented to the Congress;

- increasing the focus on and expanding resources—including the number of cybersecurity personnel—to significantly upgrade the cyber resilience of the Department of Defense, including its contractors and subcontractors, pursuant to a programmatic plan presented to the Congress;

- establishing and regulating "certified active defenders," private-sector entities that will operate in conjunction with, and under the direction and control of, the government to enhance cybersecurity resilience; and

- internationally, authorizing enhanced cybersecurity support to NATO and other treaty allies, as well as the establishment of an International Cyber Stability Board of likeminded allies to undertake resilience of cross-border critical infrastructures and multinational campaigns, with respect to significant cyber adversaries.

In addition to such actions, Congress should

- authorize, and budget for, a substantially enhanced cybersecurity research, development, and deployment effort, utilizing both private and public capabilities; and

- create a commission with governmental and private-sector participation that should evaluate the potential establishment of cybersecurity regulatory requirements for key critical infrastructures, for information technology and cybersecurity providers, and for public or private companies with revenues greater than $100 million.[1]

# 2. CYBERSECURITY: CURRENT DEFICIENCIES

Despite recent cyber-defense improvements, there is still a cybersecurity gap and a need for dramatic change—both architecturally and organizationally—in light of escalating and pervasive threats. The need for cybersecurity enhancement is particularly important, given that, "as we enter into renewed great power competition, the US does not enjoy the same historical military superiority over potential adversaries."[2] The need for significant change is especially demonstrated by the regularity of successful cyberattacks, as well as the persistence of well-known vulnerabilities and related deficiencies.

- In March 2018, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) publicly stated that the critical infrastructures of "energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors" had been targeted by Russian attackers who had "gained remote access into energy sector networks." More recent media reports indicate that North Korea is likewise undertaking cyber operations to access critical infrastructure.[3]

- The cities of Atlanta, Baltimore, Dallas, Denver, Sacramento, San Diego, and San Francisco have recently been attacked. Other cities, as well as states and localities, are similarly vulnerable.[4]

1 This report does not deal with cyber as a component of influence operations and disinformation as part of hybrid/gray-area attacks; rather, it focuses on the operational aspects of cyber and the potential for espionage and disruption. For discussion of hybrid issues, see Franklin D. Kramer and Lauren M. Speranza, *Meeting the Russian Hybrid Challenge, Atlantic Council*, May 2017, https://www.atlanticcouncil.org/images/publications/Meeting_the_Russian_Hybrid_Challenge_web_0530.pdf.

2 Michael D. Griffin, "Defense Science Board 2019 Summer Study on Future of US Military Superiority," Under Secretary of Defense, October 1, 2018, https://www.acq.osd.mil/dsb/TORs/SS19 - Future of US Military Superiority - TOR.pdf.

3 "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," US Department of Homeland Security, CISA, March 15, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A; Troy Stangarone, "North Korea Is Still Trying to Hack US Critical Infrastructure," *Diplomat*, March 14, 2019, https://thediplomat.com/2019/03/north-korea-is-still-trying-to-hack-us-critical-infrastructure/.

4 Julie Spitzer, "3 Cities Recently Suffering Cyberattacks," *Becker's Hospital Review*, March 30, 2018, https://www.beckershospitalreview.com/cybersecurity/3-cities-recently-suffering-cyberattacks.html; Noam Erez, "Cyber Attacks Are Shutting down Countries, Cities and Companies. Here's How to Stop Them," World Economic Forum, June 22, 2018, https://www.weforum.org/agenda/2018/06/how-organizations-should-prepare-for-cyber-attacks-noam-erez/; "Port of San Diego Hit by Ransomware Cyber-attack," *SmartCitiesWorld*, October 4, 2018, https://www.smartcitiesworld.net/news/news/port-of-san-diego-hit-by-ransomware-cyber-attack-3408; and Cesar Cerrudo, "Cities Are Facing A Deluge Of Cyberattacks, And The Worst Is Yet To Come," *Forbes*, April 18, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/04/18/cities-are-facing-a-deluge-of-cyberattacks-and-the-worst-is-yet-to-come/#1ee08cc12559.

- The federal government has not organized effectively to protect itself, as demonstrated by the successful attack on the Office of Personnel Management (OPM) resulting in compromise of the personal information of some twenty-two million people, and the more recent Office of Management and Budget (OMB) memorandum stating "OMB and DHS determined that 71 of 96 [federal] agencies (74 percent) participating in the risk assessment process have cybersecurity programs that are either at risk or high risk."[5]

Particularly concerning in the face of potential high-end attack is the failure of the Department of Defense to provide cybersecurity measures for key weapons systems, as a 2018 report by the General Accountability Office (GAO) demonstrates.[6] Additionally, the assessments of the Department of Defense Office of the Director, Operational Test and Evaluation's 2018 fiscal-year annual report indicate that "DOD missions and operations remain at risk from adversarial cyber operations," including a key capability—the Joint Regional Security Stack—that "is unable to help network defenders protect the network against operationally realistic cyber-attack." The report also states that the "rate of [cyber defense] improvements is not outpacing the growing capabilities of potential adversaries."[7] Moreover, media reports have indicated that DoD contractors and subcontractors have been significantly affected by cyberattacks, and a recent public report for the secretary of the Navy states that the "system has demonstrably failed."[8]

Additionally, international actions have been ineffective as adversary nation-states have been the sources of major cyberattacks. As the 2018 Foreign Economic Espionage in Cyberspace report states, "foreign intelligence services—and threat actors working on their behalf—continue to represent the most persistent and pervasive cyber intelligence threat."[9] The 2019 Worldwide Threat Assessment by the director of national intelligence (DNI) concurs, with several strong statements:[10]

> *"Moscow continues to be a highly capable and effective adversary, integrating cyber espionage, attack, and influence operations to achieve its political and military objectives. Moscow is now staging cyber attack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis… Russian intelligence and security services will continue targeting US information systems, as well as the networks of our NATO and Five Eyes partners…*
>
> *"China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems. China remains the most active strategic competitor responsible for cyber espionage against the US Government (USG), corporations, and allies. It is improving its cyber attack capabilities…*
>
> *"Iran continues to present a cyber espionage and attack threat. Iran uses increasingly sophisticated cyber techniques to conduct espionage; it is also attempting to deploy cyberattack capabilities that would enable attacks against critical infrastructure in the United States and allied countries…*
>
> *"North Korea poses a significant cyber threat to financial institutions, remains a cyber espionage threat, and retains the ability to conduct disruptive cyber attacks."*

There have been several recent, specific state-directed attacks that underscore these findings.

- Russian attacks include the Russian-generated NotPetya attack that infected some two hundred

5 Ellen Nakashima, "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say," *Washington Post*, July 9, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?noredirect=on&utm_term=.8960dc0d8a52; "Federal Cybersecurity Risk Determination Report and Action Plan," Office of Management and Budget, May 2018, https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf.

6 "Weapons System Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities," (Government Accountability Office report to the Committee on Armed Services, US Senate, October 2018), https://www.gao.gov/assets/700/694913.pdf.

7 "FY 2018 Annual Report," Director Operational Test and Evaluation, December 2018, 45, 229, https://www.dote.osd.mil/pub/reports/FY2018/pdf/other/2018DOTEAnnualReport.pdf.

8 Kyle Rempfer, "Report: Navy Is Under 'Cyber Siege,' National Secrets Leaking from the Hull," *Navy Times*, March 13, 2019, https://www.navytimes.com/news/your-military/2019/03/13/report-navy-is-under-cyber-siege-national-secrets-leaking-from-the-hull/; "Cybersecurity Readiness Review," Secretary of the Navy, March 2019, https://www.navy.mil/strategic/CyberSecurityReview.pdf.

9 *Foreign Economic Espionage in Cyberspace, National Counterintelligence and Security Center*, 2018, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

10 Daniel R. Coats, Statement for the Record, *Worldwide Threat Assessment of the US Intelligence Community before the Senate Select Committee on Intelligence, Director of National Intelligence*, January 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

thousand computers and resulted in damages of hundreds of million dollars, the 2016 attack against the Democratic National Committee, and the recent series of attacks against network infrastructure devices.[11]

- China engaged in the OPM attack noted above, as well as attacks against managed service providers, espionage against DoD contractors, and recent indictments for stealing proprietary technology from US-based Micron technology used to make dynamic random-access-memory (RAM) chips.[12]

- North Korea launched the Sony and WannaCry attacks, the latter infecting systems including those of the United Kingdom's National Health Service, Spain's Telefonica, Germany's Deutsche Railroad, France's Renault, and the United States' Boeing.[13]

- Iranian attacks have included the distributed denial-of-service attacks against financial institutions, the Shamoon attack against the Saudi Arabian energy industry, and recent attacks against the Internet Domain Name System.[14]

Criminal attacks are also increasing. As the 2019 Worldwide Threat Assessment states, "Foreign cyber criminals will continue to conduct for-profit, cyber-enabled theft and extortion against US networks…[F]inancially motivated cyber criminals very likely will expand their targets in the United States in the next few years. Their actions could increasingly disrupt US critical infrastructure in the health care, financial, government, and emergency service sectors."[15] The Symantec 2018 report states that the "sheer volume of threats increased, but the threat landscape has become more diverse," including coin-mining, supply-chain, ransomware, and mobile-malware attacks.[16] Businesses are unable to cope with these attacks, as demonstrated by statistics showing that some 61 percent of small and medium enterprises have been subject to attack.[17] Large companies fare no better, as larger companies including Marriott, Facebook, Target, Adobe, Equifax, Yahoo!, eBay, Heartland, Uber, JPMorganChase, Anthem, and Home Depot have suffered attacks.

Finally, threats are likely to increase in the future. As Director of National Intelligence Dan Coats put it in a January 2019 statement, "All our adversaries and strategic competitors will increasingly build and integrate cyber espionage, attack, and influence capabilities."[18] Also, the structures of planned 5G networks will be key, including concerns over China's role in their deployment, and the concomitant potential for cyber espionage and disruption.[19]

11 Alfred Ng, "US: Russia's NotPetya the Most Destructive Cyberattack Ever," CNet, February 15, 2018, https://www.cnet.com/news/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/; "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," US Department of Homeland Security.

12 "Advanced Persistent Threat Activity Exploiting Managed Service Providers," US Department of Homeland Security, CISA, October 3, 2018, https://www.us-cert.gov/ncas/alerts/TA18-276B; Catherine Stupp, "Nation-State Hackers Target Managed Service Providers to Access Large Companies," *Wall Street Journal*, October 31, 2018, https://www.wsj.com/articles/nation-state-hackers-target-managed-service-providers-to-access-large-companies-1541013256; Ellen Nakashima and Paul Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare," *Washington Post*, June 8, 2018, https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?noredirect=on&utm_term=.dddc6fb044b3; "PRC State-Owned Company, Taiwan Company, and Three Individuals Charged With Economic Espionage," Department of Justice, Office of External Affairs, press release, November 1, 2018, https://www.justice.gov/opa/pr/prc-state-owned-company-taiwan-company-and-three-individuals-charged-economic-espionage.

13 Danny Palmer, "WannaCry Ransomware Crisis, One Year On: Are We Ready for the Next Global Cyber Attack?" ZDNet, May 11, 2018, https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/.

14 Muks Hirani, Sarah Jones, and Ben Read, "Global DNS Hijacking Campaign: DNS Record Manipulation at Scale," FireEye, January 9, 2019, https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html; Eric Chabrow, "7 Iranians Indicted for DDoS Attacks Against US Banks," *BankInfo Security*, March 24, 2016, https://www.bankinfosecurity.com/7-iranians-indicted-for-ddos-attacks-against-us-banks-a-8989; Nicole Perlroth and Clifford Krauss, "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try," New York Times, March 15, 2018, https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.

15 Coats, Statement for the Record, *Worldwide Threat Assessment of the US Intelligence Community before the Senate Select Committee on Intelligence* , 6.

16 *Executive Summary 2018: Internet Security Threat Report*, Symantec 23, March 2018, 1-2, https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf.

17 "2017 Ponemon Institute Study Finds SMBs Are a Huge Target for Hackers," Keeper Security, press release, September 19, 2017, https://www.prnewswire.com/news-releases/2017-ponemon-institute-study-finds-smbs-are-a-huge-target-for-hackers-300521423.html.

18 Coats, *Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community before the Senate Select Committee on Intelligence*, 5.

19 James A. Lewis, *How Will 5G Shape Innovation and Security: A Primer, Center for Strategic and International Studies*, December 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181206_Lewis_5GPrimer_WEB.pdf.

# 3. A ROADMAP TO BETTER CYBERSECURITY

The objective of this report is to outline realistic changes to the cybersecurity environment that would result in better cybersecurity for users. Achieving 'better" cybersecurity—perfect security is not an option—will require three fundamental conceptual and operational changes.

First, change will require greater use of effective coordinated partnerships, to provide critical expert capabilities to users. Cybersecurity is complex, and it requires expert engagement. As an analogy, in the financial arena, users rely on banks and other financial institutions to be responsible for key aspects of their monetary transactions, including payments, lending, and savings—though, of course, users have their own responsibilities as part of that system. Critical elements of effective coordinated partnerships include the development of advanced technology and the use of effective operational approaches, including cloud technologies, automation, and artificial intelligence.

Second, new partnerships and other changes will require the federal government to be more significantly involved in the provision of cybersecurity. That will include the provision of budgetary resources, the enhancement of resilience through coordinated partnerships, and the undertaking of significant responses to cyberattackers. To create effective partnerships, the nation's best resources will need to move to support the most critical assets and sectors.

Third, the technical architecture and underpinnings for defending against cyberattacks must change. The attack surface is too broad to address with conventional solution approaches, and is increasing by an order of magnitude with the convergence of information technology systems (data), and operational technology platforms (SCADA, sensors). Gaps in private and public cloud-based services are outpacing certification and accreditation. New IoT devices provide countless entry points into private networks, and sophisticated botnets are growing and becoming automated for advanced distributed-denial-of-service (DDoS) attacks. Trusted platforms have been found to have backdoor access, and mobility continually challenges the definition of securing to "the edge".[20]

Despite these evident and growing risks, organizations susceptible to attack often fail to fix the problem in a timely manner. Perhaps the problem is seen as too overwhelming or unsolvable (which is partially true as there is no end-state in cyber readiness). But we must improve this situation soon and in a sustainable way. Recommended changes include: a rapid migration to a zero-trust architecture for enterprises and extended enterprises; rationalization and consolidation of disparate systems and networks; development of a secure hardware capability; machine-learning/artificial-intelligence-augmented cyber defenses; expanded use of the cloud to provide expert-level capabilities; and active defenses built upon an ever-increasing, intelligent zero-trust architecture.

These general approaches, explained in detail below, are necessary for three reasons. First, effective cybersecurity resilience is beyond the capability of most entities; coordinated partnerships can provide the requisite additional resources. Second, current cybersecurity does not include effective responses against attackers, and the "bad guys"—nation states and criminals— have not been significantly deterred. As General Paul Nakasone, commander of US Cyber Command (USCYBERCOM), recently stated, "Thus far, our responses against adversaries who have penetrated our networks…have not worked."[21] Third, there are far too few resources devoted to cybersecurity. While it is something of an overstatement, current cybersecurity actions are all too often akin to the Pentagon aphorism of "providing all assistance short of actual help." Or, to use a sports analogy, it is as if one football team had eleven players on the field, while the other initially had six and sometimes increased that number to nine—better, but not enough to win. The foregoing suggests the general approach; what follows are the specifics.

20 FireEye Threat Intelligence, "China-based Cyber Threat Group Uses Dropbox for Malware Communications and Targets Hong Kong Media Outlets," FireEye, December 1, 2015, https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html.; Savia Lobo, "Security researcher exposes malicious GitHub repositories that host more than 300 backdoored apps," Security Boulevard, March 5, 2019, https://securityboulevard.com/2019/03/security-researcher-exposes-malicious-github-repositories-that-host-more-than-300-backdoored-apps/."

21 William T. Eliason, "An Interview with Paul M. Nakasone," *Joint Force Quarterly* 92, January 17, 2019, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1734461/an-interview-with-paul-m-nakasone/.

## A. CHANGING THE CYBERSECURITY MODEL FOR KEY CRITICAL INFRASTRUCTURES: ENERGY, FINANCE, TELECOMMUNICATIONS, TRANSPORTATION, WATER TREATMENT

A logical place to start and prioritize the analysis is with the critical infrastructure and key resources (CIKR) that support the foundation of society and how we live, work, and survive. These include: energy, especially the electric grid, and oil and gas pipelines; finance; telecommunications; transportation, particularly air, rail, and maritime; and water and wastewater treatment. Disruption of any of these could have significant cascading effects on the economy.[22] However, even within these sectors, it will be worthwhile to focus, at least initially, on the most critical entities—an approach along the lines of the one the finance industry has already utilized in the establishment of the Financial Services Analysis and Research Center (FSARC), comprising the eight largest US financial institutions.[23] Likewise, prioritizing and beginning with a limited number of key entities for other sectors will allow for a more efficient and innovative process.

The relevant threats to the central CIKR should be recognized as high-end, nation-states threats—as reflected, for example, in the Russian penetrations of critical infrastructures noted above and the Iranian attacks on financial institutions and energy infrastructure. Within each infrastructure, it will be important to undertake prioritization—i.e., to determine which entities are most critical to a national effort if a high-end attack occurred—and to plan and resource to meet those requirements with a goal of effective resilience. The DHS National Risk Management Center (NRMC) is undertaking a significant risk-evaluation effort, and part of that effort can be working with sector-specific agencies to determine key sectoral critical infrastructures.[24]

Achieving effective resilience will require important systemic changes, and the development of effective coordinated partnerships. Importantly, adversary nation-state cyber capabilities are well beyond the defensive capacities of most critical infrastructures. Even the telecommunications industry, which has a very good internal capacity to provide protection and resilience for its networks, has recognized the need for governmental assistance against high-end attacks.[25] Additionally, the development of expert private-sector capabilities—including secured cloud-based technology, automation, and artificial intelligence—adds to the capacities that should be included in a coordinated partnership.

Changing the cybersecurity model for key CIKR would differ somewhat among critical infrastructures. What would be most effective for grid companies will likely differ from what would be most effective for air transportation, telecommunications, finance, or water treatment. It is important to understand that enhancing cybersecurity for key CIKR is not a simple process that will be achieved quickly. Rather, it will be important to set up tailored, multiyear programs to support the energy, finance, telecommunication, transportation, and water-treatment sectors in deploying and operating available technology, and in developing new or modified capabilities to meet sector-specific needs.

A goal might be the development of a Common Reference Architecture that could be expanded to other members of the sector. Such an approach would need to be highly programmatic and operational, taking into account the different aspects of the different sectors. For each sector, the federal government and key CIKR enterprises would organize a coordinated cybersecurity effort. On the federal-government side, this would mean that the lead sector-specific agency—the Department of Energy (grid and pipelines), the Department of the Treasury (finance), the Environmental Protection Agency (water), and the Department of Homeland Security (telecommunications and transportation)—should have regular interaction with the recommended FSARC-like entities,

22 "National Risk Management," US Department of Homeland Security, accessed March 28, 2019, https://www.dhs.gov/cisa/national-risk-management-center.

23 The FSARC was established in October 2016, with initial membership of eight large financial institutions: Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street, and Wells Fargo. "FS-ISAC Announces the Formation of the Financial Systemic Analysis & Resilience Center (FSARC)," Financial Services Information Sharing and Analysis Center, press release, October 24, 2016, https://www.fsisac.com/sites/default/files/news/FS-ISAC Announces the Formation of the Financial Systemic Analysis (FSARC).pdf.

24 "National Risk Management Center," US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, November 15, 2018, https://www.dhs.gov/sites/default/files/publications/NRMC 100 Days Fact Sheet 20181115_CISA v2.pdf. "Protecting National Critical Functions: the NRMC has launched a far-reaching effort across all 16 critical infrastructure sectors to identify and validate a list of National Critical Functions. This allows DHS to assess critical infrastructure interdependencies and identify risk and the impact it would have on our critical functions."

25 "NSTAC Report to the President on Information and Communications Technology Mobilization," National Security Telecommunications Advisory Committee, November 19, 2014, 11–13, https://www.dhs.gov/sites/default/files/publications/NSTAC - Information and Communications Technology Mobilization Report 11-19-2014.pdf.

consisting of a limited number of sector entities with a focus on developing effective cybersecurity architectures, capabilities, and processes. The Department of Homeland Security, where not the lead agency, and the Department of Defense, in all instances, should also be engaged, given their key responsibilities for national cybersecurity. The Department of Homeland Security has established a tri-sector council focusing on telecommunications, financial, and energy industries.[26] This is a worthwhile undertaking, but sector-specific working relationships with a limited number of entities would allow for more effective operationally oriented interactions. Further, as indicated by media reports, the FSARC has important interaction with US Cyber Command, and similar relationships should be developed for other critical-infrastructure sectors.[27] According to General Nakasone, such efforts are being undertaken, and should be expanded: "USCYBERCOM has developed strong partnerships with DHS, the FBI, and sector-specific agencies for select critical infrastructure and key resource sectors. We are doing this purposefully, in partnership with DHS and private-sector leads. It is critical that we develop these partnerships prior to a possible crisis."[28]

Effective resilience will require taking steps in advance of adverse cyber events. One key element will be to provide key CIKR with highly effective available technology and techniques. Those capabilities will come from both the private sector and the government. The use of private-sector cloud technology, automation, and artificial intelligence can be key for the provision of cybersecurity. The DoD's recent Cloud Strategy states

> *"…[E]ach Cloud Service Provider will be integral to combating cyber challenges and securing the cloud. The Cloud Service Providers will automatically scan infrastructure resources and generated logs, which will be used to identify vulnerabilities early and to make intrusion detection and mitigation in near-real time a reality across much of the enterprise…[A] focus must be applied to both software and hardware-which change at an incredible pace. Keeping up with those changes is difficult, but failure to keep pace has created significant security risks and will only increase in the years to come. Here, again, modern commercial providers have addressed this problem. Moving…to the cloud will take advantage of the rapid roll out of software and hardware updates…Hardware with defects or vulnerabilities is constantly swapped out and software patches are applied with vigor in a secure and fault tolerant manner."*[29]

The federal government, likewise, has valuable cybersecurity research and development underway, which should be incorporated to support key CIKR. Review of the Department of Energy's Multiyear Plan for Energy Sector Cybersecurity and Cybersecurity for Energy Delivery Systems (CEDS) Research and Development Program demonstrates the depth of research.[30] Similarly, the Department of Homeland Security Science and Technology Directorate (S&T) "supports the full spectrum of cybersecurity research and development (R&D)…including the finance, energy, and public utility sectors, as well as the first responder community…[and] helps a variety of end-users understand and use emerging cyber-capabilities, such as blockchain and the Internet of Things."[31]

Additionally, appropriately using highly effective available technology from major government security agencies, including the Department of Defense and the intelligence community, may provide significant benefits to key CIKR. In the recent National Defense Authorization Act, Congress required transfer of the Sharkseer capability from the National Security Agency (NSA) to the Defense Information Systems

26 Derek B. Johnson, "Cybersecurity: With Elections Over, CISA Focus Shifts to Risk Management Center," *Federal Computer Week*, November 17, 2018, https://fcw.com/articles/2018/11/17/cisa-dhs-risk-center-launch.aspx.; Tri-Sector Executive Working Group Risk Management Activities: chartered with senior industry representatives from the financial-services sector, communications sector, electricity sub-sector, and senior government representatives from the Departments of Homeland Security, Treasury, and Energy. Efforts have been launched to help direct intelligence-collection requirements, build cross-sector risk-management playbooks, and better understand systemic risk: "National Risk Management Center," US Department of Homeland Security.

27 Chris Bing, "Inside 'Project Indigo,' the Quiet Info-sharing Program between Banks and US Cyber Command," *CyberScoop*, May 21, 2018, https://www.cyberscoop.com/project-indigo-fs-isac-cyber-command-information-sharing-dhs/. "In an emailed statement, a Cyber Command spokesperson acknowledged Project Indigo's existence."

28 Eliason, "An Interview with Paul M. Nakasone."

29 "DOD Cloud Strategy," Department of Defense, December 2018, 4, https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF.

30 "Multi-Year Program Plan for Energy Sector Cybersecurity," US Department of Energy, March 2018, https://www.energy.gov/sites/prod/files/2018/05/f51/DOE Multiyear Plan for Energy Sector Cybersecurity _0.pdf; "From Innovation to Practice: Re-Designing Energy Delivery Systems to Survive Cyber Attacks," Cybersecurity for Energy Delivery Systems (CEDS) R&D Program, July 2018, https://www.energy.gov/sites/prod/files/2018/09/f55/CEDS From Innovation to Practice FINAL_0.pdf.

31 A listing of projects can be found at "Cybersecurity," US Department of Homeland Security, accessed March 28, 2019, https://www.dhs.gov/science-and-technology/cybersecurity.

Agency, thereby enhancing its usability and practical effectiveness.[32] While this transfer was certainly not an exact precedent, if the key CIKR are to have effective cybersecurity against highly capable adversaries, use of governmental high-end capabilities on their behalf will be warranted.[33] The Defense Department and the intelligence community will need to establish an operational model that provides cybersecurity for key CIKR, while maintaining operational security of classified capabilities. It may well be that the best approach will be for even the fact of particular usages to be nondisclosed, but their usage can be highly valuable.

A second key element to establishing the changed cybersecurity model will be the creation of structures and procedures to effectuate smooth interaction between the federal government and the relevant critical infrastructure. On the governmental side, it would be easy to become bogged down in bureaucracy, so it will be critical for Congress to pass legislation that authorizes the requisite capacity. The proposed federal National Cybersecurity Fusion Center, discussed below, would be the appropriate place to organize multiagency programmatic and operational aspects of support to the key critical infrastructures. On the private-sector side, as noted, one important step will be for each sector to have in place an FSARC equivalent to facilitate interaction with the federal government.

The third key element will be for the USG to effectively use active defense and "defend forward" capabilities on behalf of key CIKR. The DoD cyber strategy states, "We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[34] More specifically, with respect to critical infrastructure, the strategy states:

"Second, the Department seeks to preempt, defeat, or deter malicious cyber activity targeting US critical infrastructure that could cause a significant cyber incident regardless of whether that incident would impact DoD's warfighting readiness or capability. Our primary role in this homeland defense mission is to defend forward by leveraging our focus outward to stop threats before they reach their targets. The Department also provides public and private sector partners with indications and warning (I&W) of malicious cyber activity, in coordination with other Federal departments and agencies."[35]

The US cyber strategy has thus determined the importance of "attack support" for key CIKR; they function as public goods critical not only for national security, but also for governance and the economy. While Defense Department capabilities are thereby intended to be engaged in generating effective resilience for the key critical infrastructures, the nationwide implementation of such a mandate could require substantial efforts beyond the current capacity of USCYBERCOM. However, while the National Guard is already engaged in cyber activities, one potentially useful approach to enhancing active defense would be to utilize capabilities available from the private sector. Government entities could be supported by "certified active defenders," i.e., private-sector entities with high cyber capabilities who will work under government direction and control, in accordance with a legislative mandate that will need to be established. Without trying to overdo the analogy, the Constitution provides for private support to defense efforts in its authorization of "letters of marque," and certified active defenders under governmental direction and control would be a modern version. However, such certified active defenders should focus on defense and resilience and, unlike with letters of marque, should be under government direction and control.

The fourth key element will be congressional legislation to help implement the proposed cooperative-partnership model between the federal government and the key critical infrastructures, one aspect of which will be financial arrangements to make such efforts successful. There is a clear need for increased resources—the failure of cybersecurity for key infrastructures shows current resources are not enough. Because it is mainly "externalities" affecting national security (and other public goods) that are of concern, resources need to come mainly from public funds, and not from companies. While the decision is ultimately for Congress, financing could be provided via a number of mechanisms, including grants

32 H.R. Res. 5515, 115 Cong. (2018) (enacted). According to media reports, "Sharkseer uses artificial intelligence to monitor traffic across DoD networks and sift through emails and documents that could pose network security risks." Peter Graham, "Report: NSA to Transfer 'Sharkseer' Cybersecurity Program to DISA," *ExecutiveGov*, July 30, 2018, https://www.executivegov.com/2018/07/report-nsa-to-transfer-sharkseer-cybersecurity-program-to-disa/.

33 The Department of Defense and the intelligence community have the ability to utilize a combination of governmental R&D capabilities such as the Defense Advanced Research Projects Agency, "skunk works" at entities like federally funded R&D centers, faster acquisition authorities as can be utilized under so-called "other transactional authority," and other fast-tracking actions, such as the Defense Innovation Unit or In-Q-Tel to help support requirements for key CIKR.

34 "Summary: Department of Defense Cyber Strategy 2018," US Department of Defense, September 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

35 Ibid., 2.

and subsidies, contracts, tax relief, and federally authorized rate increases. A budget for certified active defenders will also be required. Given the national security requirement for such actions, the rationale for legislation is clear enough.

With respect to establishing an effective cooperative-partnership system, just as has been required in the safety, health, and environmental arenas, the federal government will need additional authorities to provide the effective cybersecurity resilience required by the nation. As discussed above, each of the critical infrastructures will require an appropriately tailored model. While cybersecurity will be a regularly changing arena for the foreseeable future, certain capabilities and techniques should be put in place, and the federal government should have the directive authority to require those, so long as it is also paying for them. In using directive authority, officials will need to consider the differences between sectors, and have sufficient flexibility that industry can meet the directive requirements while maintaining reliable operations. The directive authority will also be needed to authorize the combined operational activities required to effectuate proper use of best available technology and techniques for active defense. Authorizing such directive authority is obviously a non-trivial point, as changes in certain systems can affect the systems' reliability. Congress has already taken a step in this direction with the passage of the FAST Act, which provides the secretary of energy with emergency directive authority in the event of a cyber emergency.[36] It will be important for the government to have directive authority for all key CIKR, including authority to require action prior to an incident. The rationale for undertaking such action is the nation's ever-increasing dependence on cyber and information technologies, and the failure of existing cybersecurity measures to provide adequate protection and resilience. In the Information Age, with critical technologies dependent on secure cyber systems, failure to change can result in unacceptable national vulnerabilities.

## B. CHANGING THE CYBERSECURITY MODEL FOR STATES, CITIES, AND LOCALITIES

States, cities, and localities provide essential governance and services ranging from police, fire, and emergency medical services to education to elections to traffic control. However, as the discussion of attacks above underscores, all those entities are subject to significant cyber intrusions. As one study, undertaken in conjunction with the National Association of State Chief Information Officers, noted, "one state estimates that two years ago there were 150 million attacks a day, while today [2018] there is an average of 300 million attacks per day."[37]

In response, states have begun to enhance cybersecurity efforts: "every state has an enterprise-level [Chief Information Security Officer (CISO)] role…All 50 states have established the CISO's authority via the legislature, secretary, or [Chief Information Officer]. In addition, most states now have a formally approved cybersecurity strategy and governance process that articulates and oversees the state's cybersecurity vision and guidelines and provides consistency across the enterprise."[38]

As the analysis indicates, however, these steps have not been sufficient in developing and/or executing a cyber strategy. "[S]trides in governance and in establishing the CISO role's legitimacy have not resulted in significant progress in overcoming the top challenges US states face in implementing effective cybersecurity programs. CISOs continue to face perennial challenges in acquiring an adequate budget and workforce to carry out their responsibilities."[39]

The resource challenge is clear: "In most states, the CISO's only source of cybersecurity funding is derived from the state's IT budget, and is not designated as a separate line item. And the percentage of state enterprise IT budgets allocated to enterprise cybersecurity is still 1–2 percent, and annual budget increases have

36 "The FAST Act also gave the Secretary of Energy new authority, upon declaration of a Grid Security Emergency by the President, to issue emergency orders to protect or restore critical electric infrastructure or defense critical electric infrastructure. This authority allows DOE to support energy sector preparations for and responses to natural, physical and logistical events." Karen Evans, *Testimony of Assistant Secretary Karen Evans, Office of Cybersecurity, Energy Security, and Emergency Response, Before the Committee on Energy and Commerce, United States House of Representatives, 115th Congress*, September 27, 2018, https://www.energy.gov/sites/prod/files/2019/01/f58/9-27-18 Karen Evans-FT-HEC.pdf.

37 Srini Subramanian and Doug Robinson, "The 2018 Deloitte-NASCIO Cybersecurity Study," Deloitte Insights, October 22, 2018, 1, https://www2.deloitte.com/insights/us/en/industry/public-sector/nascio-survey-government-cybersecurity-strategies.html.

38 Ibid., 5.

39 Ibid., 3.

not kept pace with the needs of today's security landscape and tomorrow's evolving challenges."[40]

By contrast, "private US industries spent an average of 28 percent of their IT budget on security technologies."[41] Similarly, on average, at the state level, there are six to fifteen full-time-equivalent cyber professionals. This contrasts with one hundred full-time-equivalent cyber professionals in financial institutions similar in size to an average state.[42] The cybersecurity challenges states face will only increase with the continued development and importance of digital technology, yet "emerging technology initiatives in areas such as IoT (Internet of Things), artificial intelligence, smart enterprises (smart cities), and blockchain technology rank at the bottom of the CISO initiative list, indicating that they may not yet be a priority for CISOs."[43]

As indicated above, the amounts states have actually spent on cybersecurity are relatively small. The National Governors Association analyzed state cybersecurity spending in fiscal years 2015–2017, reviewing twenty-three states and the District of Columbia.[44] While the information is not easy to correlate, in the category of "information security and assessments," the study found that fifteen states had spent a total of $86 million over the three-year period, the amounts and usages varying widely. A simple average would put the annual state spending on these categories at somewhat less than $2 million—though the study noted annual expenditures ranging from $140,000 to $8 million. Similarly, in the category of "homeland security and emergency management," the study reviewed expenditures by seven states totaling $32 million over the three-year period, or an annual average of $1.4 million per state, with specific expenditures ranging from $100,000 to $13 million. The key point to take from the study is that cybersecurity spending at the state level is relatively low. It would be reasonable to infer that expenditures by localities are even lower.

The discussion below sets forth recommendations regarding personnel, technology, organization, and resources, in order to achieve an adequate level of cybersecurity for states, cities, and localities.[45]

First, as a good starting point, there is a critical need to have a higher degree of available expertise and training. In building such capabilities, states are obviously not starting from scratch, as numerous capabilities already exist. In addition to the state CISO office, states may have some degree of cyber capability in their law-enforcement entities, homeland security agencies, information-technology offices, public universities, and state National Guards—and can also engage with multiple private-sector and academic entities, both for-profit and nonprofit. If not already accomplished, states should undertake an inventory and assessment of such capabilities. The value of such an effort has not escaped the notice of governors and other state officials, and recent analysis for the National Governors Association noted twenty-two states have established government bodies to identify and mitigate cyber threats.[46]

Two areas deserve particular focus. First, National Guard units are a potential source of important capability. While the National Guard can be called under federal control, for the most part, it operates as a state entity. The National Guard has undertaken significant enhancement of cyber capabilities. The National Guard Bureau has stated: "The Army National Guard is establishing a Cyber Brigade with 5 Cyber Battalions, 10 [Cyber Protection Teams] (one in each [Federal Emergency Management Agency] region), 5 Cyber Support Companies, and 5 Cyber Warfare Companies under State authority (Title 32) between FY16 –FY22."[47]

A related news article elaborated that, in 2017, the Army activated a cyber brigade that oversees cyber units in thirty states. "Each of the cyber protection battalions will have a cyber security company, a cyber warfare company and two cyber protection teams. The headquarters will have about 25 personnel, with each company consisting of about 35-40 people. They will conduct vulnerability assessments, cyber

40 Ibid., 7.
41 Ibid., 9.
42 Ibid., 7.
43 Ibid., 11.
44 "Meet the Threat: States Confront the Cyber Challenge, Memo on State Cybersecurity Budgets," National Governors Association, https://ci.nga.org/files/live/sites/ci/files/1617/docs/1705StateCyberBudgets.pdf.
45 The recommendations that follow would also generally apply to territorial and tribal governments, but would need to be adapted to particular contexts.
46 Ibid., 44.
47 "NG Cyber Defense Team," US National Guard, December 2017, https://www.nationalguard.mil/Portals/31/Resources/Fact%20Sheets/NG%20Cyber%20Defense%20Team%20Fact%20Sheet%20(Dec.%202017).pdf.

analysis and defensive cyberspace operations on military networks, among other duties."[48]

Similarly, as of December 2017, the Air National Guard had established "12 Cyberspace Operations Squadrons," including "7 Network Warfare Squadrons, 2 Information Operations Squadrons, 1 Information Aggressor Squadron as well as other cyber-capable units."[49]

A more recent article, which included interviews with senior National Guard officers, stated, "The National Guard currently has 3,880 cyber service members in 59 cyber units in 38 states, but that number is scheduled to grow."[50] In short, the National Guard is a current, and growing, cybersecurity resource.

While the National Guard looks to both its national defense and state roles, the latter is an important element. The National Guard can provide vulnerability assessments, monitoring, and other capabilities as agreed between it and state organizations. For example, one National Guard officer, Colonel Jori Robinson, vice commander of the 175th wing of the Maryland Air National Guard, said her unit spent some of its time protecting police cyber grids. "It was reactive. The Maryland State Police kind of felt like something was going on in their networks," Robinson said. "We worked with the state police to do a vulnerability assessment. We wrote up a report for them and told them, 'This is what you can do; this is what we're seeing; this is how you fix X, Y and Z.'"[51]

In Texas in 2018, the Army Cyber Institute and other key partners conducted the second Jack Voltaic cyber experiment/exercise, focused on testing civil-military response to physical cyber events in Houston. The exercise highlighted key actions that the National Guard and state departments should take to better support states and communities. State and National Guard organizations need to develop cyber-response handbooks that can be shared across states, so military knowledge can scale to better support local governments. The Army Cyber Institute-led research further recommended that the DoD maintain an inventory of existing and emerging critical National Guard and Army Reserve cyber capabilities, which could be leveraged by state, and better enable national-level coordination for states support.[52]

Second, the nonprofit and private sectors can be important elements of state cybersecurity strategy. The Jack Voltaic experiment/exercise and other state-based assessment reports highlighted the importance of statewide incident-response campaigns and statewide Information Sharing Analysis Organizations (ISAO) for improving a state's overall cyber posture. Both the campaign and ISAO need to be driven by strong public-private partnerships that include academic centers of excellence.[53] As another report recommended, "CISOs can establish a network among state and local agencies, academia, and corporations to share threat information, capabilities, and contracts to strengthen state cyber defenses."[54] The study found: "CISOs have increased their use of outsourcing by two- to three-fold for certain functions, including cybersecurity risk assessments, audit log analysis, and threat management and monitoring. However, more than half of US states still do not outsource these functions. Doing so can be a significant opportunity as states continue to struggle with hiring and retaining qualified security staff. State CISOs should work to understand and define the cybersecurity functions that can be delivered by their state workforce, and then forge long-term partnerships with the private sector for their remaining cybersecurity functions and competencies, with continual improvement and service level expectations."[55]

One useful way for a state to engage is through arrangements with universities and other academia—some of whom may be state-funded, so resources may be available outside the state cybersecurity budget. Good examples include the NSA/DHS Centers of Academic Excellence in Cybersecurity Defense Education and the NSA

48 Charlsy Panzino, "Army National Guard Activates its First Cyber Brigade," *Army Times*, September 28, 2017, https://www.armytimes.com/news/2017/09/28/army-national-guard-activates-its-first-cyber-brigade/.

49 "NG Cyber Defense Team," US National Guard.

50 Scott Maucione, "National Guard Cyber Units Protect Country's Interests, Still Face Training Issues," *Federal News Network*, January 18, 2019, https://federalnewsnetwork.com/defense-main/2019/01/national-guard-cyber-units-protect-countrys-interests-still-face-training-issues/.

51 Ibid.

52 "Jack Voltaic 2.0: Threats to Critical Infrastructure," Army Cyber Institute at West Point, 2018, https://www.afcea.org/event/sites/default/files/files/JackVoltaic_ExecSummary_R12%20(Final).pdf.

53 Ibid.

54 Subramanian and Robinson, "The 2018 Deloitte-NASCIO Cybersecurity Study," 12.

55 Ibid., 11.

Centers of Academic Excellence in Cyber Operations.[56] Another example is the multi-university National Cybersecurity Preparedness Consortium, which includes the University of Texas at San Antonio, Texas A&M Engineering Extension Services, University of Memphis Center for Information Assurance, Norwich University Applied Research Institutes, and the University of Arkansas Criminal Justice Institute.[57]

Third, and most importantly, an organized coordination mechanism for policy and operations needs to be established. There are existing structures to build upon, but they vary from state to state. Some states maintain state cybersecurity centers: "Based on their current roles and responsibilities, these centers can be divided into three categories: (1) integration centers that focus on information sharing and incident response; (2) centers with a workforce and education focus; and (3) centers with policy making authority."[58]

Some states have information-technology offices with a security mandate. One media report noted that between 10 and 15 states have built "security operations centers."[59] A number of states operate "fusion centers" with multifunctional focus, including crime, counterterrorism, and critical infrastructure, but also, increasingly, cybersecurity.[60] All these are valuable, but the key issues to resolve are whether there is adequate directive authority by the state cybersecurity entities to ensure that state agencies undertake necessary cybersecurity-resilience measures, and whether there is a coordinated-response mechanism in the event of a cyberattack.

In sum, for effective cybersecurity coordination, a key task will be for the state itself to establish an expanded central repository of expertise—in effect, a cybersecurity agency—though the precise mechanisms can differ from state to state. As discussed further below, the value of a central, coordinated mechanism expands beyond the state level, as it also provides a platform for effective interaction upstream to the federal government, and downstream to cities and localities.

One of the most challenging aspects of cybersecurity within a state arises at the city and locality level. As with the state level, the key issues are resources and personnel, but the problem is magnified. Broadly speaking, cities and localities cannot provide adequate cybersecurity on their own. Many cities and localities have very few information-technology personnel, and they often have multiple job duties, of which cybersecurity will only be a part. Aside from very large cities such as New York and Los Angeles (which have excellent cybersecurity approaches), most cities and localities need a different model. An effective model for cities and localities would have two key elements: obtaining cybersecurity as a service from the state, and integrating the significant use of cloud services, automation, and artificial intelligence as elements of cybersecurity. Also, given the expanded reach of cyber attacks to potentially impacting multiple localities simultaneously, pooling of resources and funding to achieve cybersecurity capabilities and personnel could be an effective approach.

Cybersecurity as a service generally means that an authorized outside party is contracted to provide some, or all, of a client's cybersecurity requirements. At the state level, one well-known and useful example is the Michigan CISO as a service, which was undertaken as a pilot program in 2018. The Michigan program operated as follows.

> *"To meet these requirements, Michigan launched a pilot program to establish a Chief Information Security Officer (CISO) as a Service…*
>
> *"'The goal was to provide resources to each county and to serve as a trusted broker,' Michigan Deputy Chief Security Officer Chris DeRusha said. And to do so with awareness that*

56 "National Centers of Academic Excellence," US National Security Agency, accessed March 28, 2019, https://www.nsa.gov/resources/students-educators/centers-academic-excellence/; "Centers of Academic Excellence in Cyber Operations," US National Security Agency, accessed March 28, 2019, https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-centers/.

57 "The National Cybersecurity Preparedness Consortium," National Cybersecurity Preparedness Consortium, accessed March 28, 2019, http://nationalcpc.org/about.html.

58 "Meet the Threat: States Confront the Cyber Challenge, Memo on State Cybersecurity Centers," National Governors Association.

59 Colin Wood, "Alabama Gov. Kay Ivey Announces State's First Security Operations Center," *StateScoop*, October 1, 2018, https://statescoop.com/alabama-gov-kay-ivey-announces-states-first-security-operations-center/.

60 "Thirty-nine fusion centers (51%) selected cybersecurity as a top five priority in 2017, an increase of 11% from the previous year. Fusion centers also identified which cyber-related activities they contribute to and/or conduct. These activities include strategic cyber analysis, tactical cyber analysis, technical cyber analysis, or none. Of the 39 fusion centers that reported cybersecurity as a top five priority, 59% indicated they have capability in all three of the cyber analysis activities (Figure 17)." "2017 National Network of Fusion Centers Final Report," US Department of Homeland Security, National Network of Fusion Centers, October 2018, https://www.hsdl.org/?view&did=817528, 17.

*funding is often in short supply, particularly at the local level.*

*"The Michigan Department of Technology, Management and Budget (DTMB) saw common governance as a key to establishing a baseline. DTMB asked the questions, where do we start, and what are the priorities? It then deployed a knowledgeable CISO to provide a baseline assessment of the cybersecurity posture of participating counties. That CISO employed a free IT security assessment tool called CySAFE (Cyber Security Assessment for Everyone), which was created by the state and counties to assess, understand and prioritize their basic cybersecurity requirements."*[61]

The Michigan pilot effort is highly valuable for demonstrating how a "state as a CISO" might work when city and locality resources are limited. A more effective model could be developed using cloud technology, automation, and artificial intelligence—both for the state itself, and to be provided to cities and localities.

A model could be developed that would combine the capabilities of state authorities along with those of private-sector entities, and with resources in support from the Department of Homeland Security and the Department of Defense (including the proposed National Cybersecurity Fusion Center, if established). There is little sense to a cyber strategy, as set forth by the DoD, that undertakes to "defend forward" if inadequate resilience has been established for the entities being defended. But, state, city, and local entities are currently key critical infrastructures that, for the most part, lack necessary cybersecurity resilience.

There is, of course, no doubt that such an effort would require both additional resources and some significant focus on IT capabilities at the state/city/locality level, as many state and local IT capabilities are significantly outdated. However, a planned program over a five-year period could make a significant difference. Resources obviously cannot come out of the air, but, per the discussion below, this would be a good use of federal monies, and in accord with the precedent of providing federal funding in connection with enhancing cybersecurity for the 2018 elections.

The third element of effective cybersecurity at the state/city/locality level is enhanced support from the federal government. DHS does support the Multi-State Information Sharing and Analysis Center (MS-ISAC), which provides information on best practices, tools, and threats—all of which are valuable and necessary, but as the discussion above indicates, insufficient to provide adequate resilience in the face of multiple and increasing cyber threats.[62] An enhanced federal role would have two key elements: resources and operational support. First, as discussed above, states and their subdivisions lack the resources required for adequate cybersecurity, even though it has become a critical requirement of governance, including in the provision of services. The federal support to states' election security for the 2018 midterm elections is a model of what should become a broader, regular cybersecurity line item in the federal budget. The budget for the election support was $380 million, and states were required to match 5 percent within two years.[63]

A useful way to approach future monetary requirements would be for the Department of Homeland Security, with support from the Department of Defense (operating jointly through the National Cybersecurity Fusion Center, if established), to work with the private sector to define key elements of a state/city/locality cybersecurity model, and for the states to present five-year plans incorporating those elements, along with the concomitant budgetary requirements. Defining the key elements for such a model would be important to ensure that the funds are well-spent, but would also allow for necessary flexibility, since states differ in significant ways.[64] Accordingly, the precise nature of the model adopted will differ from one state to another, and the amounts of resources required will, of course, also differ. By way of example, Texas likely would be organized differently from, and need more resources than, Rhode Island. However, such differential implementation and resource requirements are characteristics of many federally supported programs that are implemented

61 Mickey McCarter, "NASCIO Midyear 2018: Michigan Embraces CISO as a Service," *StateTech*, April 23, 2018, https://statetechmagazine.com/article/2018/04/NASCIO-Midyear-2018-Michigan-Embraces-CISO-as-a-Service.

62 "MS-ISAC," Center for Internet Security, accessed March 28, 2019, https://www.cisecurity.org/ms-isac/.

63 "US Election Assistance Commission Announces All Eligible States And Territories Have Requested Hava Funds," US Election Assistance Commission, accessed March 28, 2019, https://www.eac.gov/news/2018/07/16/us-election-assistance-commission-announces-all-eligible-states-and-territories-have-requested-hava-funds/.

64 Interestingly enough, a good portion of the 2018 funding was not spent prior to the election, though the money is multiyear and can be spent later. Matthew Weil and Joshua Ferrer, "States are Waiting to Spend New Federal Election Money—And That's a Good Thing," Bipartisan Policy Center, November 2, 2018, https://bipartisanpolicy.org/blog/states-are-waiting-to-spend-new-federal-election-money-and-thats-a-good-thing/.

at the state level, and the creation of such a federal program to support state and city/locality cybersecurity would mean much better cybersecurity for the nation as a whole.

The second element of an effective federal cybersecurity program for the state/city/locality level would be the federal government providing support to entities under cyberattack, in accord with the DoD cyber strategy to support critical infrastructures. This can be done through a combination of utilizing existing resources—such as the national protection teams of Cyber Command, the hunt and incident-response teams at DHS, and the National Guard—and creating some new types of resources, including private-sector "certified active defenders."[65] Additionally, it would be valuable to expand training programs for state cybersecurity entities and personnel, and to develop operational exercise programs that mirror the continuously adapting threats. Federal support is further discussed in the section on the federal government below.

## C. CHANGING THE USG CYBERSECURITY MODEL

The federal government's cybersecurity model needs significant enhancement to create effective resilience for the federal government itself, and to provide support to key critical infrastructures and states, cities, and localities as discussed above. As the recent report by OMB and DHS states, "The recent government-wide cybersecurity risk assessment process conducted by OMB, in coordination with the DHS, confirms the need to take bold approaches to improve Federal cybersecurity."[66]

In determining such steps, it is useful to consider actions that the federal government has taken. These include the establishment of the DHS National Cybersecurity Communications and Information Center (NCCIC) and the NRMC, the DNI Cyber Threat Intelligence Integration Center, the DoD Cyber Command, and the FBI Cyber Division, and a recent memorandum of understanding between the DHS and the DoD. However, in the words of the DHS director of the NRMC, "We are facing an urgent, evolving crisis in cyberspace. Our adversaries' capabilities online are outpacing our stove-piped defenses."[67]

The first step toward "bold approaches" that resolve "stove-piped defenses" would be creation of a National Cybersecurity Fusion Center. Most importantly, the proposed center would have an operational role to organize the provision of capabilities prior to, and in response to, cyberattacks, similar to the operational activities of "joint interagency task forces" (JIATF) used in other arenas (though such activities would not necessarily be headed by the Defense Department). The national protection teams from USCYBERCOM, including the National Guard when federalized, and the hunt and incident-response teams from DHS, would generally operate under the direction of the National Cybersecurity Fusion Center. Legislation would be needed to determine such issues as the chain of command and funding, with the existing frameworks for interactions between the Federal Emergency Management Agency and the Department of Defense providing a sensible starting point. To make its operational role effective, the center would have an intelligence and information-sharing function, integrating relevant information and analysis from the National Cyber Threat Intelligence Center, the cyber elements of the NRMC, and the NCCIC. The center would work with the federal departments, agencies, key critical infrastructures, and states to support their cybersecurity efforts, as discussed above.

The proposed National Cybersecurity Fusion Center's core efforts would be supported by designated personnel from the Department of Homeland Security, the Department of Defense, the Intelligence Community, the Federal Bureau of Investigation, the Department of Energy, the Department of Treasury and the Department of State. Other entities that have important cyber roles, such as the Federal Reserve

65 "NCCIC ICS," US Department of Homeland Security, National Cybersecurity and Communications Integration Center, https://ics-cert.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_NCCIC%20ICS_S508C.pdf. "NCCIC's Hunt and Incident Response Team (HIRT) provides onsite incident response, free of charge, to organizations that require immediate investigation and resolution of cyber attacks. In 2016, the incident response capabilities of US-CERT and ICS-CERT were combined to create HIRT, which operates under NCCIC and provides DHS's front line response for cyber incidents and proactively hunting for malicious cyber activity. Upon notification of a cyber incident, HIRT will perform a preliminary diagnosis to determine the extent of the compromise. At the customer's request, HIRT can deploy a team to meet with the affected organization to review network topology, identify infected systems, image drives for analysis, and collect other data as needed to perform thorough follow on analysis. HIRT is able to provide mitigation strategies and assist asset owners/ operators in restoring service and provide recommendations for improving overall network and control systems security.

66 "Federal Cybersecurity Risk Determination Report and Action Plan," Office of Management and Budget, 3.

67 Robert Kolasky, *Statement for the Record, Robert Kolasky, Director National Risk Management Center, National Protection and Programs Directorate, US Department of Homeland Security, For a Hearing on "Cyber Threats to Our Nation's Critical Infrastructure" before Senate Committee on Judiciary, Subcommittee On Crime And Terrorism, 115th Congress*, August 21, 2018, http://mepoforum.sk/wp-content/uploads/2018/08/08-21-18-Kolasky-Testimony.pdf.

and the Federal Communications Commission, would provide personnel focused on their respective areas of expertise. If established, private-sector "certified active defenders" would operate under the direction and control of the National Cybersecurity Fusion Center. Overall, the center's functions would include greater cybersecurity effectiveness for federal governmental functions, and support to key CIKR and states, as previously discussed.

Undergirding this national fusion center is the need for a continuous net-assessment process, which can inform USG decision-makers and partners when they will enjoy relative advantage with cyber-enabled actions, or when there is increased adversary risk for a specific US national interest. This new, dynamic process must continuously incorporate, and correlate USG technical and human, as well as business and open-source, intelligence to enable increased automation in cyber defense, as well as more agile decision-making across the USG as the government measures its strengths and vulnerabilities vis-à-vis adversaries and strategic competitors.

With respect to the federal government, the National Cybersecurity Fusion Center concept would include utilizing the Department of Defense's cyber "defend forward" strategy as part of establishing cyber deterrence and resilience. Federal systems should not be attacked with impunity by adversaries, whether nation-states or criminals. Equally importantly would be a more focused effort to require mandatory use of highly effective cyber technology and techniques to resolve the deficiencies that led OMB and DHS to determine that multiple federal agencies have "cybersecurity programs that are either at risk or high risk."

DHS currently has the authority to issue emergency directives and binding operational directives, which require action on the part of federal agencies in the civilian executive branch.[68] However, the system is obviously deficient, as exemplified by the OMB/DHS report noted above. In part, this is because the system allows the affected agency to create its own mitigation plan. That is not a strategy designed to bring the most cutting-edge cybersecurity capabilities to bear. That problem is exacerbated by the absence of any central funding to resolve agency cybersecurity issues. Congress needs to provide, as part of its cybersecurity efforts, a budget that DHS and/or the National Cybersecurity Fusion Center could apply to remediating federal agencies' cybersecurity deficiencies.

Additionally, the DHS would be able to accomplish its tasks much more efficiently if the number of personnel focused on cybersecurity were significantly increased. In addition to its responsibility for the cybersecurity of most of the federal government, the DHS is the sector lead for multiple critical infrastructures. It would be fair to say that it has done as well as can be expected, but is nonetheless unable to perform all required tasks with the current number of personnel. While Congress should evaluate the numbers, it would be reasonable to have, as an initial goal, an increase in size over several years comparable to the more than six thousand that the DoD has in USCYBERCOM (a number that, as discussed below, should itself be increased). However, in order to generate an effective result, Congress should require DHS to provide a programmatic plan for such an increase, and its probable effects. It should also be recognized that the current budgetary caps would significantly affect the ability to accomplish such an increase. The very significant cybersecurity vulnerabilities that face the nation call for those caps to be modified in such a way that DHS can accomplish its cybersecurity tasks.

The second element of an enhanced cybersecurity effort by the federal government would be congressional action with respect to key CIKR, and the states providing budgetary support and creating appropriate standards. Most importantly, just as it needs to create a central funding mechanism to enhance federal-agency cybersecurity, Congress should establish an annual budget line item to support cybersecurity for key critical infrastructures and the states. The budgetary support provided by the Congress in conjunction with the 2018 elections provides the basic model for such an effort. However, the funding would go to supporting cybersecurity for the broader range of state (and through the states, city and locality) governance functions, such as police, fire, education, and other regular state and city/local governance activities. Further, and as proposed above, the federal budget—or alternative mechanisms such as tax relief—should be utilized to ensure that key critical infrastructures have sufficient funding to meet cybersecurity requirements.

As discussed above, the federal government should have greater directive authority for key critical infrastructures and should work to establish standards for cybersecurity that states and key critical

68 "Cybersecurity Directives," US Department of Homeland Security, accessed March 28, 2019, https://cyber.dhs.gov/directives/.

infrastructures would meet. Significant legislative change would be required, but with current approaches being inadequate the need for change is apparent. Legislation would have to allow for sufficient flexibility needed to establish tailored requirements appropriate to different sectors and to the states. In the case of the states, the decision to comply would be voluntary as required by the American federal system. By contrast, for the key CIKR, all of which are in interstate commerce, directives would be mandatory, and meeting the standards would be required to receive funding.

The third key federal cybersecurity activity would be a more substantial international effort. Short of responding to an armed attack, this would consist of a greater set of activities in connection with so-called "gray area" or "hybrid" attacks against the United States, and also, as appropriate, against allies and partners. Congress has been highly supportive of taking such actions. The John S. McCain National Defense Authorization Act for Fiscal Year 2019 specifically authorized active defense against Russia, China, North Korea, and Iran.[69] Under the international-law doctrines of countermeasures and necessity, there are actions nations can take, both offensive and defensive in nature, against the perpetrator of a cyberattack, provided certain conditions are met.[70] These measures would otherwise not be lawful, but are justified due to a prior wrongful act against the state (for countermeasures) or circumstances that place a state's essential interests in "grave and imminent peril" (for pleas of necessity).[71] There are several requirements and restrictions on these actions. For instance, countermeasures require attribution of the initial act to a state actor, while both countermeasures and actions of necessity must follow the customary principles of necessity and proportionality. Still, nations have significant options in this realm.[72] This body of law also supports the use of collective countermeasures, a concept particularly relevant for NATO (and other US alliances, including with Australia, Japan, and the Republic of Korea), which enables multiple nations—even those not directly harmed by the hybrid act—to act together to amplify a response under certain circumstances. Under the accumulation-of-events doctrine, individual incidents or successive attacks, which alone may not rise to a sufficient level of force to justify the use of countermeasures, can be assessed under the law as connected incidents.[73] Taken together, these may reach a threshold that would justify more severe countermeasures.

The fundamental objective for the United States in this arena is to develop the doctrine and capabilities to effectively deter—or, as necessary, through the approach of persistent engagement and defend forward, respond to—adversary gray-area cyberattacks. There are media reports that the Department of Defense has taken actions in this arena, including, as one example, against the Russian Internet Research Agency, to protect the integrity of the 2018 midterm elections.[74]

Finally, in an era of great-power competition, in which the United States is expending significant resources on developing military capabilities to deter or respond to armed attack, it is important to have requisite, comparable cyber capabilities, both for resilience and for operational use. Given the findings of both the recent GAO and the Department of Defense's Office of the Director, Operational Test and Evaluation reports regarding significant weapon-system vulnerabilities and other deficiencies in DoD cyber resilience, Congress should significantly increase the number of personnel and resources available to the DoD for cybersecurity. A good way to determine the appropriate number would be to require the Defense Department to provide a report to Congress with a remediation plan and the requisite resources, both financial and personnel, required to implement it. The Defense Department also needs to significantly improve the cyber resilience of its contractors and subcontractors,

69 H.R. Res. 5515, 115th Cong. (2018) (enacted).

70 Catherine Lotrionte, "Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law," *Cyber Defense Review* 3, 2, Summer 2018, 73–114, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/CDR_V3N2_ ReconsideringConsequences_LOTRIONTE.pdf?ver=2018-09-05-084840-807.

71 While there no universally accepted definition for a state's "essential interests," they are generally considered to include issues related to a state's security, or preservation of its natural environment, economy, public health, safety, and food supply. See *United Nations, Draft Articles on Responsibility of State for Intentionally Wrongful Acts, With Commentaries* (New York: United Nations, 2001), Article 25, http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

72 For a full discussion, see Lotrionte, "Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law."

73 Ibid.; see also, United Nations, *Draft Articles on Responsibility of State for Internationally Wrongful Acts, With Commentaries*; Colonel Gary Corn and Eric Jensen, "The Technicolor Zone of Cyberspace—Part I and Part 2," Just Security, May 30, 2018, https://www.justsecurity.org/57217/technicolor-zone-cyberspace-part/.

74 Ellen Nakashima, "US Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?utm_term=.5076da2cf2fc.

in light of reports that there have been significant penetrations of high consequence. The current system of requiring adherence to Defense Federal Acquisition Regulation Supplement (DFARS) regulations has not proved adequate. The DoD should instead create a required "resilience architecture," which contractors and subcontractors will have to implement. This should not be a checklist, but rather, a requirement for integrated capabilities that could meet desired parameters. Contractors and subcontractors should be regularly subject to no-notice penetration and other testing, to ensure that they meet the desired standards. As noted above in the discussion of critical infrastructures, establishing an effective resilience architecture likely will include governmental provision of key technologies, requirements for greater use of the secured-and-compliant cloud to maximize expert capabilities, and ongoing development of enhanced resilience capabilities. Since there will be costs required for implementation, the Defense Department will need to evaluate how to integrate such requirements into bid proposals, to ensure that desired cyber resilience is obtained. Congress should require the DoD to include elements of a resilience architecture for contractors and subcontractors in the remediation plan noted above.

The requirements for responding in the context of armed attack are discussed further below, in the international section.

## D. CHANGING THE INTERNATIONAL CYBERSECURITY MODEL

Cyber is inherently international, and, to be effective, cybersecurity needs to be implemented at the international, as well as national, level. The United States has several important types of international arrangements affecting cybersecurity, including through the intelligence community-led "Five Eyes," national security treaty arrangements—including NATO and with, among others, Australia, Japan, and the Republic of Korea—and law enforcement under the Budapest Convention. However, creating effective resilience will require doing more than is currently the case.

At the international level, the first step to cybersecurity effectiveness is to increase the coordinated activities of "likeminded" nations and entities. Two actions would be most useful. The first would be the creation of an International Cyber Stability Board, consisting initially of a small number of likeminded countries—for example, the United States, Australia, Canada, France, Germany, Japan, Republic of Korea, and the United Kingdom—or, alternatively, those NATO countries that have offered to provide offensive cyber capabilities to the Alliance. The board would be a voluntary organization along the lines of the Financial Stability Board (FSB) or the Proliferation Security Initiative (PSI).[75] However precisely established, the member countries would work together to develop protection and resilience for cross-border CIKR such as finance and maritime, undertake campaign responses to cyber-criminal and terrorist actions, as well as develop a counter-hybrid approach to the cyber threats presented by Russia, China, North Korea and Iran.[76] [77]The authors have previously described the proposed board.

"Operationally, the proposed board would act much as the fusion and joint operations centers developed in several countries to meet terrorism threats have done, except on an international basis. To be effective, it will be important to go beyond purely defensive measures and to raise the costs to cyber attackers.

"To be sure, part of the board's program would be to generate deterrence by denial and resilience at a truly international level, as the standards discussed above would seek to limit the consequences of any attack. Defense through strictly denial and resilience

75 "The FSB is not a treaty-based organisation. Policies agreed by the FSB are not legally binding, nor are they intended to replace the normal national and regional regulatory processes. Instead, the FSB acts as a coordinating body, to drive forward the policy agenda of its members to strengthen financial stability. It sets internationally agreed policies and minimum standards that its members commit to implement at national level." "Coordination of Financial Sector Policies," Financial Stability Board, accessed March 28, 2019, http://www.fsb.org/work-of-the-fsb/; "It is a voluntary initiative geared toward enhancing individual and collective partner nations' capabilities to take timely and appropriate action to deal with a fast-changing proliferation threat environment. The PSI provides a platform for networking among states and coordination of their activities to counter proliferation." "Who We Are," Proliferation Security Initiative, accessed March 28, 2019, https://www.psi-online.info/.

76 Symantec tracks about one hundred and forty criminal groups, a number that could be affected by a significant campaign approach. "Internet Security Threat Report (interactive infographic)," Symantec, 2018, https://interactive.symantec.com/ISTR?CID=70138000001MD17AAG.

77 "Army cyber forces have also supported the Joint force as an integral part of Joint Task Force ARES (JTF-ARES), a JTF that I'm privileged to lead that has been countering ISIS' use of cyberspace as a domain to spread messages and coordinate combat activity. The work of JTF-ARES has been an important part of the coordinated multi-domain military campaign that helped defeat ISIS on the ground in Iraq and Syria." Paul M. Nakasone, *Statement by Lieutenant General Paul M. Nakasone, Commander, United States Army Cyber Command Before the Subcommittee on Cybersecurity, Committee on Armed Services, 115th Congress*, March 13, 2018, https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-13-18.pdf.

is not sufficient for effective cybersecurity in the face of more aggressive and harmful behavior by nation states engaged in cyber exploitation and attack activities. Attackers need to suffer costs for their activities. A multinational set of actions would be key to creating such costs. The key common operational effort would be an ongoing campaign among the nations of the board to deter and defeat significant cyber attackers.

"An effective cybersecurity campaign would utilize the full spectrum of national and multinational resources. It would necessarily include intelligence and information sharing as well as law enforcement, and work across jurisdictions enhancing ongoing efforts. But it will also be critical to find means of both active defense and offense that would be consequential against cyber attackers."[78]

The second step to international cybersecurity effectiveness is increased activities in connection with national security efforts, such as NATO, or, in the Indo-Pacific, with Australia, Japan, and the Republic of Korea. The Department of Defense is already working closely with countries in each of these arenas, but several additional steps would be of high value, focused on the reduction of vulnerabilities, establishment of greater resilience, and the use of offensive capabilities. In the NATO arena, such actions have been described.

"First, for the frontline states, NATO should establish 'cyber collective defense, where the framework nations (the United Kingdom, Canada, Germany, United States) leading the eFP [enhanced forward presence battalions] in the Baltics and Poland assist those nations in establishing enhanced cyber resilience for their telecommunications, electric grids, and reception facilities that are critical to warfighting and thus a key requirement for deterrence.' Those framework nations would work with each of the frontline states to develop the operational procedures to respond to an attack and put in place advanced capabilities that would limit the consequences of such an attack, through enhanced resilience and the ability to recover...

"This could include offensive cyber operations as a means of deterrence...[C]reating such a combined joint task force (CJTF) for cyber—under the auspices of the new Combined Operations Center at [Supreme Headquarters Allied Powers Europe]—would be a good first step, given the need to incorporate multiple national capabilities and to connect offensive and defensive capabilities and actions...[S]uch a CJTF could have a three-part mandate: capabilities coordination; operational-concept development, including interaction with non-cyber capabilities; and establishment of a doctrine to include legal requirements."[79]

In sum, greater resilience and the tailored use of cyber offensive capabilities are important steps for achieving an asymmetrical advantage. Such efforts are applicable equally to close allies in the Indo-Pacific, and to key partners in the Middle East.

## E. CONGRESS AND CYBERSECURITY

Congress will be a highly important actor in changing the model for more effective cybersecurity. Establishing such cybersecurity will require additional resources, in terms of both money and personnel, as well as new methods and organizational efforts.

As the discussion above highlighted, legislation will be required in seven areas.

- establishing a National Cybersecurity Fusion Center that will coordinate policy, budgetary and operational actions focused on cybersecurity resilience in the United States;
- providing requisite regulatory authorities for federal support to, and oversight of, cybersecurity for key critical infrastructures;
- creating an annual federal budget line to support cybersecurity for states, cities, localities, and key critical infrastructures;
- establishing a federal budget line item to support cybersecurity for the federal government, and increasing the number of cybersecurity personnel at the Department of Homeland Security, pursuant to a programmatic plan presented to Congress;
- increasing focus and expanding resources, including the number of cybersecurity personnel, to upgrade the cyber resilience of the Department of Defense, including contractors and subcontrac-

78 Franklin Kramer, Robert Butler, and Catherine Lotrionte, "Raising the Drawbridge with an International Cyber Stability Board," *Cipher Brief*, October 27, 2017, https://www.thecipherbrief.com/article/exclusive/tech/raising-drawbridge-international-cyber-stability-board.

79 Franklin Kramer, Hans Binnendijk, and Lauren Speranza, *NATO Priorities: After the Brussels Summit, Atlantic Council*, November 2018, 10, https://www.atlanticcouncil.org/images/publications/NATO-Priorities-After-the-Brussels-Summit.pdf.

tors, pursuant to a programmatic plan presented to the Congress;

- establishing and regulating certified active defenders—i.e., private-sector entities that will operate in conjunction with, and under the direction and control of, the government to enhance cybersecurity resilience; and

- internationally, authorizing enhanced cybersecurity support to NATO and other treaty allies, and for the establishment of an International Cyber Stability Board of likeminded allies to undertake resilience of cross-border critical infrastructures and multinational campaigns, with respect to significant cyber adversaries.

Congress should additionally authorize and budget for a cybersecurity advanced research, development, and deployment effort, utilizing both private and public capabilities, and should create a commission with governmental and private-sector participation that should evaluate the potential establishment of cybersecurity regulatory requirements for key critical infrastructures, information-technology and cybersecurity providers, public companies, and private companies with revenues greater than $100 million.

Congress' role is extremely important in connection with budgetary support, inasmuch as the requisite funding is simply not available otherwise for key critical infrastructures, states, cities, or localities. Equally important would be funding to expand advanced-technology research-and-development efforts, by both the federal government and the private sector. To be sure, there are useful R&D activities ongoing, including those noted at DOD, DOE, and DHS, as well as in the private sector. But, given the ever-increasing importance of information technology and the significant deficiencies in cybersecurity, a concentrated and expanded effort—both for supporting the development of new technologies and ensuring they can be brought to market for deployment—would be highly worthwhile.

Given the scope of the problem, it would be valuable to increase the amount of direct cybersecurity funding, and to also include a focus on cyber architectures and other methods of coordinated capabilities, such as the use of cloud architecture, automation, artificial intelligence, and managed services, which would lead to a more-secure future cyber framework. Multiple R&D approaches could be undertaken, in the near, medium, and long terms. For example, the top-ten types of cyberattacks are well known, and an R&D effort that generated more significant protection against them, through automation, artificial intelligence, or cloud technology, would be highly valuable.[80] [81] Perhaps more important would be an automated ability to hunt for, and rapidly disable, successful intrusions, or to develop so-called "zero-trust" architectures capable of limiting intruder effectiveness, including through both software and secure hardware approaches. Similarly, reduction of the botnet problem, which has increased substantially in recent years, would be extremely worthwhile.[82] So too could be developing an integrated approach for use in the provision of managed services, including the use of software-defined networks.[83] The recent report of the so-called "Cybersecurity Moonshot" commission stated that "there are broad categories of technologies that are fundamental to the realization of a safe cybersecurity," specifically noting

- "5G communications network (wireless and wired) designed with enhanced security, interconnectivity, privacy, and availability;

80 There are many lists. See Jeff Melnick, "Top 10 Most Common Types of Cyber Attacks," *Netwrix Blog*, May 15, 2018, https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

81 Possible relevant areas of R&D could include: changing the nature of the attack surface, through capabilities such as formal coding, hardware-based protection, and automatic vulnerability checking and repair; enhancing protection through advanced capabilities, including artificial intelligence and quantum computing; and reducing the impact of attacks through implementation of "dynamically changing information technology," including processes such as non-persistence and virtualization. See generally Harriet G. Goldman, "Building Secure, Resilient Architectures for Cyber Mission Assurance," Mitre, 2010, https://www.mitre.org/sites/default/files/pdf/10_3301.pdf, which discusses such techniques as diversity, redundancy, integrity, isolation/segmentation/containment, detection/monitoring, least privilege, non-persistence, distributedness and moving-target defense, adaptive management and response, randomness and unpredictability, and deception.

82 "NSTAC Report to the President on Internet and Communications Resilience, 2017," President's National Security Telecommunications Advisory Committee, 2017, https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20DRAFT%20-%20508%20compliant.pdf.

83 Possible areas of R&D relevant to integrated managed services could include: work on taxonomy and metrics to know what makes a difference at the network, enterprise perimeter, OT perimeter, and endpoints; and ways to combine capabilities of network, IT and OT perimeters, and endpoints. One potentially valuable approach would be to consider utilizing the capabilities provided by "software-defined networks" complemented by the use of automation, including through artificial intelligence, so that a state central operations center could provide continuous support to cities and localities. Such a network could be used to provide basic cybersecurity to cities and localities, including continuous monitoring, malware detection and endpoint protection, email checking, and limits on privilege escalation. Additionally, those efforts could be combined with greater use of cloud services by cities and localities. Such services could be contracted at the state level, and made available to cities and localities as part of state-provided cybersecurity as a service. Cloud capabilities are used for more than cybersecurity, of course, but greater usage (as is being undertaken at the federal level) could provide both enhanced services and enhanced cybersecurity.

- "Artificial intelligence…for near autonomous response to cyber threats at machine speed to achieve self-healing computing environments that identify flaws, prevent exploitation of those flaws, and mitigate impacts of failures;

- "Behavior biometrics combined with AI capabilities can reduce the reliance on easily compromised personally identifiable identification, allowing for the creation of identity scores that render passwords obsolete and give greater transparency and confidence in identifying users;

- "Quantum Communications and Quantum Resistant Cryptography [to] [p]rovide a trusted encryption and communications platform, leveraging quantum technologies, that is resistant to quantum general purpose (QGP) computers, tamper-resistant, and available to all services. This needs to be in place before the advent of QGP computers that can decrypt existing sensitive data;

- "Common Resilience [to] [a]ssure access and availability for required functionality of critical services by automating and simplifying the consumption model of threat prevention-oriented cybersecurity tools and capabilities;" and

- "Implementing cryptographically assured microsegments within distributed networks can reduce attack surfaces, limit lateral reconnaissance, and dramatically lessen impacts of malware, to help support both operational resilience and Zero Trust methodologies."[84]

Finally, as discussed above, Congress would need to enact legislation that allowed for tailored directive authority for key critical infrastructures and, separately, for a framework to provide support to states, cities, and localities. A related effort would seek to determine how to ensure cybersecurity more broadly, by more extensive regulation of key CIKR, information technology, cybersecurity providers, and certain larger users. There are multiple factors to take into account in considering such legislation. A good way to provide a usable framework would be to create a commission, with government and private-sector participation, that should evaluate the potential establishment of cybersecurity regulatory requirements for key CIKR, information technology, cybersecurity providers, public companies, and private companies with revenues greater than $100 million. Congress has used commissions effectively in multiple arenas. With an appropriately focused mandate and relevant expertise on the commission, useful recommendations could be generated.

84 The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President on a Cybersecurity Moonshot (Draft)*, https://www.dhs.gov/sites/default/files/publications/DRAFT_NSTAC_ReportToThePresidentOnACybersecurityMoonshot_508c.pdf, 16-17.

# 4. CONCLUSION

Cyberspace is not secure. Cybersecurity has been outrun by cyberattackers. A significant, focused effort to change to new models of cybersecurity, however, can deliver effective cybersecurity for the United States. Technological development, process changes, and appropriate resources will all be required. Coordinated partnerships between the federal government and the private sector will be important. The federal government will need to better organize itself through the establishment of a National Cybersecurity Fusion Center, and increase its support to the private sector. Internationally, the Department of Defense's effective application of its "defend forward" strategy and the organization of likeminded countries, including through the establishment of an International Cyber Stability Board, will be crucial. Congress has a critical role to play through the provision of resources, the creation of new approaches, and effective oversight. The effort will be neither simple nor short—but, with the concentrated application of American knowhow and determination, it can be accomplished.

## AUTHORS:

**Franklin D. Kramer** is a former US assistant secretary of defense for international security affairs, and a distinguished fellow and board member at the Atlantic Council.

**Robert J. Butler** is a former US deputy assistant secretary of defense for cyber policy. He is currently senior vice president for critical infrastructure protection operations at AECOM, and an adjunct fellow at the Center for a New American Security.

# Atlantic Council | Board of Directors

## CHAIRMAN
*John F.W. Rogers

## EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

## CHAIRMAN EMERITUS
Brent Scowcroft

## PRESIDENT AND CEO
*Frederick Kempe

## EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

## VICE CHAIRS
*Robert J. Abernethy
*Richard W. Edelman
*C. Boyden Gray
*Alexander V. Mirtchev
*Virginia A. Mulberger
*W. DeVier Pierson
*John J. Studzinski

## TREASURER
*George Lund

## SECRETARY
*Walter B. Slocombe

## DIRECTORS
Stéphane Abrial
Odeh Aburdene
*Peter Ackerman
Timothy D. Adams
Bertrand-Marc Allen
*Michael Andersson
David D. Aufhauser
Matthew C. Bernstein
*Rafic A. Bizri
Dennis C. Blair
Thomas L. Blair
Philip M. Breedlove
Reuben E. Brigety II
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
Ralph D. Crosby, Jr.
Nelson W. Cunningham
Ivo H. Daalder
*Ankit N. Desai
*Paula J. Dobriansky
Thomas J. Egan, Jr.
*Stuart E. Eizenstat
Thomas R. Eldridge
*Alan H. Fleischmann
Jendayi E. Frazer
Ronald M. Freeman
Courtney Geduldig
Robert S. Gelbard
Gianni Di Giovanni
Thomas H. Glocer
Murathan Günal
John B. Goodman
*Sherri W. Goodman
*Amir A. Handjani
Katie Harbath
John D. Harris, II
Frank Haun
Michael V. Hayden
Brian C. McK.
Henderson Annette
Heuser Amos Hochstein
*Karl V. Hopkins
Robert D. Hormats
*Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Reuben Jeffery, III
Joia M. Johnson
Stephen R. Kappes
*Maria Pica Karp
Andre Kelleners
Sean Kevelighan
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Richard L. Lawson
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Wendy W. Makins
Zaza Mamulaishvili
Mian M. Mansha
Chris Marlin
Gerardo Mato
Timothy McBride
John M. McHugh
H.R. McMaster
Eric D.K. Melby
Franklin C. Miller
*Judith A. Miller
Susan Molinari
Michael J. Morell
Richard Morningstar
Mary Claire Murphy
Edward J. Newberry
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Hilda Ochoa- Brillembourg
Ahmet M. Oren
Sally A. Painter
*Ana I. Palacio
Carlos Pascual
Alan Pellegrini
David H. Petraeus
Thomas R. Pickering
Daniel B. Poneman
Dina H. Powell
Robert Rangel
Thomas J. Ridge
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
Rajiv Shah
Stephen Shapiro
Wendy Sherman
Kris Singh
Christopher Smith
James G. Stavridis
Richard J.A. Steele
Paula Stern
Robert J. Stevens
Mary Streett
Ellen O. Tauscher
Nathan D. Tibbits
Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Geir Westgaard
Maciej Witucki
Neal S. Wolin
Mary C. Yates
Dov S. Zakheim

## HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
George P. Shultz
Horst Teltschik
John W. Warner
William H. Webster

**Executive Committee Members*

*List as of April 1, 2019*

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.



Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org