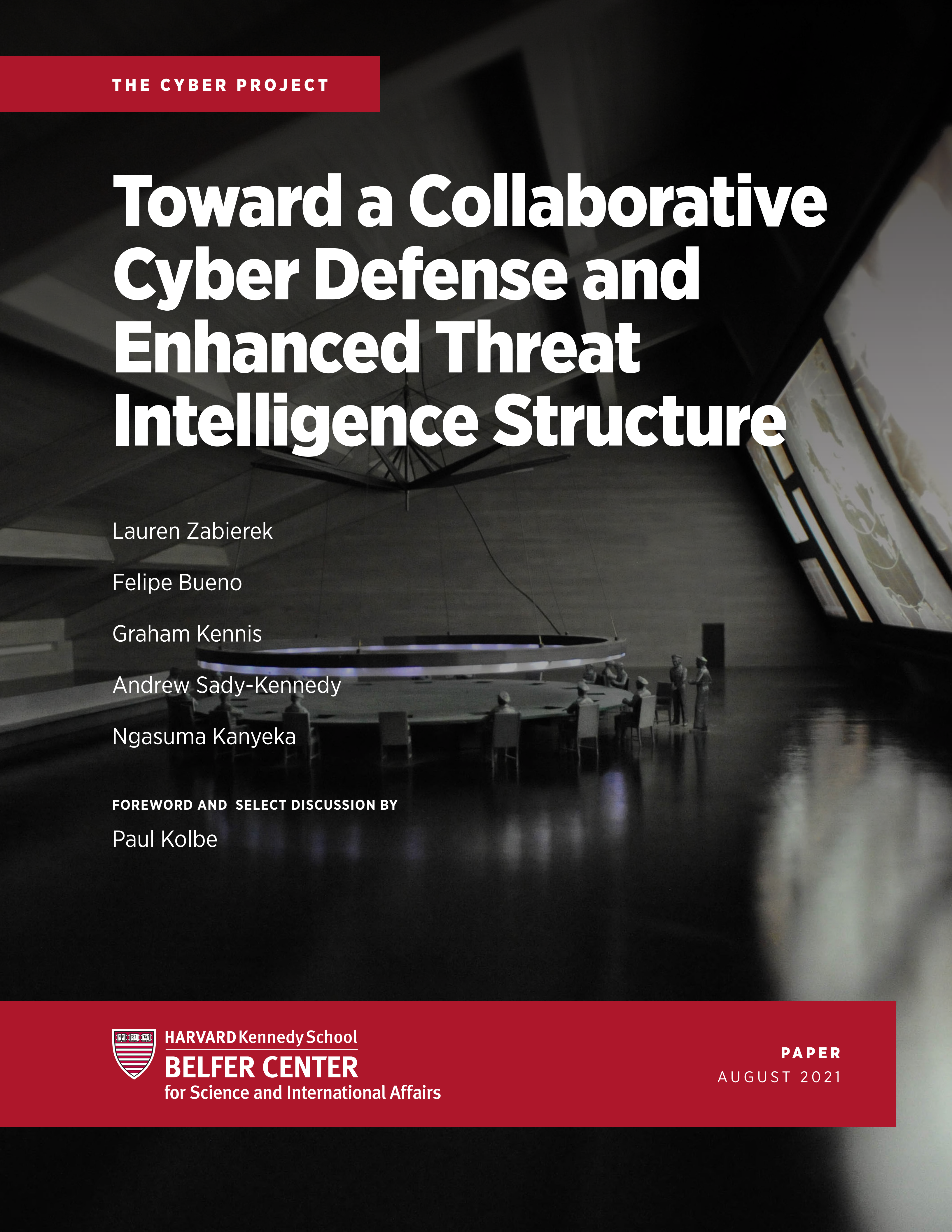

THE CYBER PROJECT

Toward a Collaborative Cyber Defense and Enhanced Threat Intelligence Structure

Lauren Zabierek

Felipe Bueno

Graham Kennis

Andrew Sady-Kennedy

Ngasuma Kanyeka

FOREWORD AND SELECT DISCUSSION BY

Paul Kolbe

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
AUGUST 2021

The Cyber Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/Cyber

Statements and views expressed in this report are solely those of the authors and do not imply endorsement by Harvard University, Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

Design and layout by Andrew Facini

Printed in the United States of America

THE CYBER PROJECT

Toward a Collaborative Cyber Defense and Enhanced Threat Intelligence Structure

Lauren Zabierek

Felipe Bueno

Graham Kennis

Andrew Sady-Kennedy

Ngasuma Kanyeka

FOREWORD AND SELECT DISCUSSION BY

Paul Kolbe

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
AUGUST 2021

Special Thanks

The research team and especially Executive Director Lauren Zabierek would like to thank the following for their time and contributions:

Cyber Experts: Sean Plankey, Tatyana Bolton, Camille Stewart, Bryson Bort, Philip Reitinger, Philip Reiner, John Costello, Brian Nussbaum, Chris Krebs

Intelligence Legends: Former DNI Jim Clapper and Former Principal Deputy DNI, Sue Gordon

Service Year expert: Jesse Colvin

Interviewees at state and major urban area fusion centers who requested to stay anonymous, but who provided vital information for the purposes of this research. Their input helped to shape our analysis and recommendations in this report.

Interviewees at private sector firms who requested to stay anonymous, but who provided vital information for the purposes of this research. Their input helped to shape our analysis and recommendations in this report.

Interviewees at federal agencies who requested to stay anonymous, but who provided vital information for the purposes of this research. Their input helped to shape our analysis and recommendations in this report.

Interviewees at ISACs, ISAOs, and other collaborative organizations who requested to stay anonymous, but who provided vital information for the purposes of this research. Their input helped to shape our analysis and recommendations in this report.

Students and Fellows: Jeff Fields, Sahar Kazranian, Jose Munoz

Foreword

A seemingly unending litany of damaging cyber breaches of American companies, institutions and government agencies makes headlines with tiresome regularity. Many of these attacks are attributed to nation states which seek to steal intellectual property, classified files, personal information, or financial data. Sometimes this is simply espionage carried out at scale, a sustained draining of our secrets, our research, and our wealth. Other times it reflects preparation of the battlefield—reconnaissance behind the digital lines of an adversary and occasional emplacement of the cyber weapons which can be triggered in event of conflict. The fact is, we live in an age of ambient cyber conflict.

In most cases, this contest reflects an unequal match. Companies across the nation can't be expected to defend against cyberattacks from nation state actors any more than they would be able to defend against a conventional military attack. At the same time, sloppy cyber practices, bad system design, and focus on device features and cost at the expense of security can place not only a company at risk, but the entire nation. The SolarWinds supply chain cyber operation amply demonstrated the collective vulnerability, government and private sector, created when weak links in the chain are identified and exploited by an adversary. The damage can be instantaneous, or it can be slow attrition of national strength and capability.

Reducing cyber risk posed by state or non-state adversaries requires a layered defense to understand threat, harden defenses, deter attack, and mitigate damage when an attack occurs.

The focus of this paper is on the first barrier of any effective cyber defense—intelligence.

Effective intelligence is not just a product or a report, but instead is a system which can provide early warning prior to attack, as well as situational awareness during the course of one. Presently, many factors diminish the ability of both government and the private sector to effectively collect, disseminate, and act upon intelligence regarding cyber threats. Silos created by classification, commercial competition, and fear of litigation all get in the way of quick dissemination of threat intelligence.

Companies may have critical insight into attacks on their networks, but may not reveal for fear of damage to reputation or share price. Government agencies may have critical intelligence on threat actors, methods and targets, but choose not to reveal in order to protect classified sources and methods. Commercial cyber threat firms serve their customers, and sometimes the wider public, but lack the scale and incentive to provide universal coverage. While players in the cyber defense industry are very capable—SolarWinds was first reported by one - we cannot base national cyber defense on vendors.

A new paradigm for cyber intelligence is needed, one that weaves together the competitive advantages of government and the private sector into a holistic, resilient, and responsive intelligence structure which underpins our collective cyber defense. The following outlines our vision for what just such a structure might look like.

*—**Paul Kolbe**, Director of the Belfer Center's Intelligence Project*

Table of Contents

A miniature of “The War Room” as depicted in the 1964 classic film *Dr. Strangelove*

Courtesy Eric Chan and the Los Angeles County Museum of Art, CC-BY 2.0

Executive Summary

National security structures envisioned in the 20th century are inadequate for the cyber threats that America faces in the 21st century. These structures, created to address strategic, external threats on one end, and homeland security emergencies on the other, cannot protect us from ambient cyber conflict, because they were designed for different times and threats. Our nation—comprising the federal government, private sector companies, critical infrastructure operators, state and local governments, nonprofits and universities, and even private citizens—are constantly under attack by a myriad of cyber actors with ever-increasing capabilities.

The SolarWinds breach was but one glaring example of the type of cyber operation perpetrated by a nation state against our government and private sector systems, designed to evade our defenses, and using our laws and national security structures against us. The adversary operated in domestic infrastructure, where the military and Intelligence Community cannot. We do not yet know the extent of the actors' access or intent, but in the cyber domain, the line between information-gathering and more damaging or destructive activities is thin—perhaps a few lines of code. The operation proved that a fundamental redesign of our domestic cyber defensive posture is both necessary and urgent to protect against future cyber operations. As such, we believe the time is now to develop an integrated, networked approach to collaborative defense and intelligence analysis and sharing between the federal government, state and local governments, and the private sector. This report seeks to create a roadmap toward this vision, answering how a 21st century threat can be tackled by the tools available in its own time.

The Current State

The team of researchers at the Cyber Project conducted several interviews with stakeholders in both the state and federal governments and the private sector. In the public sector, the team interviewed actors currently in, and recently departed from the federal government (to include Sector Risk Management Agencies (SRMAs), CISA, and ODNI) and state government (fusion centers). Furthermore, academia, critical infrastructure and national laboratory operators, information and sharing organizations and alliances, as well as analysts in the private sector, ranging from large banks to manufacturers to software companies. The team also poured over existing research and literature about fusion centers, sharing organizations, and critical infrastructure resilience—and incorporated lessons from the Cyberspace Solarium Commission report as well as the Team of Teams model. Our findings are expanded in the larger report, but we summarize below.

The common themes were clear and were presented in the following thematic areas.

Structural Challenges

There are cultural, organizational, legal, and technological barriers to collaborative defense and intelligence sharing between the public (federal, state, local government) and private sectors (business, critical infrastructure, nonprofit). The fundamental challenge is that the structures and incentives are lacking, and the relationships that do exist are largely ad hoc and point-to-point. Furthermore, there is no clear operational picture of the entire threat landscape, or a national, strategic approach to address these threats. We lack comprehensive understanding because we aren't collecting, processing, and sharing the data that is out there in a coordinated, sustained manner.

Limited & Limiting Resources

Domestic cybersecurity is hampered by limited resources (talent, data, funding), silos, and an emergency management approach to increasing threats. The federal government similarly suffers from "swim lanes" and budget limitations, paperwork requirements, and of course, classification issues—and not one person has been able to determine the priorities across the federal cyber landscape. Additionally, the Intelligence Community orients itself via the National Intelligence Priority Framework (NIPF), however, there is little institutional ability for the private sector to inform intelligence collection requirements.

Uncoordinated, Ad-hoc Sharing

Sharing between the private and public sector is often point-to-point and incident-based, save for limited, voluntary coordination between Sector Risk Management Agencies and their constituents. Furthermore, contract clauses prevent some information sharing between the public and private sectors; in fact, federal government contractors reportedly had to reach out to their contract holders for information during SolarWinds, considerably slowing the investigation. The structures and policies are simply not in place to facilitate sharing and collaboration.

Growing Threat

To say that the U.S. is not prepared for a cyber 9/11 is an understatement and employs the wrong analogy. This novel threat is different from the threat of acute terror attacks on our homeland, and is particularly pressing and unique as compared to previous challenges faced by the U.S. This country and its people, businesses, and government are already under attack, but are ill prepared to tackle imminent present and future attacks, and have been for much of the last decade.

The Vision

Cybersecurity is national security. Approaching cyber threats as anything less than that misdiagnoses the nature of the challenge we face and misplaces the need to create a system to respond adequately. These cyber activities, whether perpetrated by nation-state actors or criminal groups, are characterized more by a persistent, “network spread” paradigm than that of a more traditional, time-bound homeland security approach. Reactive emergency management responses are inadequate. A sustained, concerted, systemic response is required. In the words of Lt General Stanley McChrystal, “it takes a network to defeat a network.” This section focuses on the structures (organizational and technical) and the policies (cultural and legal) necessary to facilitate public-private collaborative defense and threat information sharing in the cyber domain.

Objectives of the Strategy

1. Create a network of Collaborative Defense and Analysis Centers at CISA Regional Offices
2. Scale Voluntary Data Collection and Processing
3. Create a Culture Shift: Knocking Down Barriers to Effective Collaboration and Sharing
4. Unravel the Interagency
5. Personnel: Increase Pipeline, Training, and Exchanges

In this paper, we propose five strategic objectives to move us toward a strategic collaborative defense and enhanced threat intelligence posture between the federal government, state governments, and the private sector. We also address the four lenses through which we viewed these issues: Cultural, Organizational, Legal, and Technological. We don’t purport to have all the answers, and many of the budgetary and operational decisions must be left to the discretion of leaders and policymakers with first-hand knowledge of the environment. We acknowledge that further analysis of the operationalization of cyber threat information by individual organizations and the challenges of collaboration at the tactical level is needed, given the complexities of the threats and the operating environment.

> "Organizations must be networked, not siloed, in order to succeed...Specifically, we restructured our force from the ground up on principles of extremely transparent information sharing (what we call "shared consciousness") and decentralized decision-making authority ("empowered execution")...We dubbed this goal—this state of emergent, adaptive organizational intelligence—shared consciousness, and it became the cornerstone of our transformation."
> —General Stanley McChrystal

Moving toward a whole-of-nation paradigm requires reimagining the concept of national security. On one hand, the concept must be expanded from a solely-governmental function; on the other hand, we must recognize that looking at domestic cyberattacks solely through a law enforcement lens limits our ability to put these attacks in the context of national security, and relying on the private sector to carry the burden of security for the nation is untenable. This would be a monumental and challenging shift, but one that we believe is necessary. This crisis presents an opportunity to reimagine and redesign a new approach to how we collectively tackle cyber security.

Discussion

This strategy document builds upon and in some cases recommends revisions within Presidential Policy Directive (PPD)- 21 (related to Critical Infrastructure Sectors), released in 2013 and PPD-41 (related to United States Cyber Incident Coordination), released in 2016. Those directives set the stage for collaboration between the federal government and private sector, highlighting the need for coordination, incident response, information sharing, and delegating responsibility to the federal agencies tasked with specific statutory and regulatory authorities. The Cyber Solarium Commission report, from which this report draws recommendations and direction, also developed a number of strong recommendations to improve the resiliency of our nation against cyber threats which we aim to build upon here.

The challenge in the cybersecurity posture in the US, is at its core, is about the policies and the structures. To enable clear policy frameworks is the bedrock of what reimagining the US cybersecurity posture requires. This paper argues that the time for such a decision has arrived, because of the growing danger of ransomware and cyberattacks. Although the technology infrastructure needs were outlined and argued for, the impetus for decision making may not have been in place because the scale of attacks did not make this the priority that it ought to have been. Fundamentally, policies are the building blocks of what and how the system will respond to the needs of a cyber-secure America in 2021 and beyond. The financial implications aside, there are hidden costs to continuing with the policy status quo for U.S. security. The growing sophistication of state and non-state cyber actors who prey on the weaknesses of an uncoordinated policy space, know that the reaction time for US attacks is delayed, because the actors who need to make such decisions are uncoordinated, and are not fully empowered to make timely, measured decisions. This urgency is why we argue for a reimagined policy space and urge decision makers to promptly consider making the necessary policy changes. In addition to making prompt, robust action, such a structure will allow for the U.S to take a more proactive role in detecting, and unveiling cyberattacks, the proposals in this paper provide room for a progressive policy environment, one that will give U.S. cyber defenders a nimble, swift and adaptive decision space to counteract and address attacks when they occur, and sometimes, hopefully, before they occur.

A Brief Analysis of the Current State

Often, public-private sharing is facilitated by personal connections in lieu of formal channels, and interactions are ad hoc or incident-focused, instead of being part of a comprehensive, structured, and clear approach. Even when such informal connections exist, the private sector is reluctant to share information as there are no defined circumstances under which federal agencies can share information with the private sector. Fears of liability, litigation, and additional regulatory action on one end, and the lack of security and safety regulations on the other make up the centerpiece of the current legal challenges that stymie collaborative information sharing and cyber defense efforts. Companies fear the damage that could be caused by exposing internal issues with cyber defense, which poses both reputational concerns and a risk of being liable for information that they have shared with other private and public actors. This combination of reputational damage with liability concerns leads to the additional fear of litigation by the company's own clients, who may impose lawsuits for the information that has been breached or shared without their consent. The resulting system is one that is stove-piped and uncoordinated, leaving cybersecurity analysts and operators overextended, and our nation vulnerable. Every organization is responsible for the protection of its own systems and has little incentive or infrastructure to coordinate analysis or defensive actions and with other organizations in the private sector, with states, and with the federal government. Most importantly, there is little institutional capacity for companies, organizations, and agencies to operate a collective defense, systematically sharing threat data and learning from each other.

This is especially true in the utilities sector, where many utility operators are small organizations, owned and operated by private companies, cooperatives, or state and local municipalities. In fact, the majority of electricity customers in the US are served by privately-owned utility companies.[1] Many private sector companies don't often see the government as a useful partner and decline to work with them if they don't have to.[2] Interviewees cited issues with timeliness and relevance of information from the federal government (i.e. indicators versus threat reporting with context), what to do with the information if classified (if analysts have a clearance), and lack of engagement from a government entity if an organization decided to reach out and provide any information.[3],[4] No matter the size and maturity of the company, organizationally, the majority of private sector companies are hampered by limited resources. What resources companies have must be focused internally on mitigating the threat versus attempting to broker

[1] https://www.eia.gov/todayinenergy/detail.php?id=40913

[2] Interview with head of cybersecurity threat intelligence at major US financial corporation, January 28, 2021

[3] Ibid.

[4] Interview with senior information security leader at major tech company

point-to-point relationships with federal or state government entities that may result in little return on investment.[5] As such, individual companies' efforts do not scale to a clear national threat picture or strategic action.

Even after making contact with federal authorities the private sector struggles to understand who is in charge. In such cases where non-federal entities understand and work with Sector-Specific Agencies (SRMAs), the paperwork required to enter an agreement to share cyber threat information can be prohibitive and time-consuming.[6] Furthermore, intelligence collection is rarely informed by private sector requirements, despite it being among nation state adversaries' main targets. These issues were on full display in the wake of the Colonial Pipeline ransomware cyberattack in May 2021, demonstrating just how urgent the need for change is. The lack of a unified federal response often results in a series of complex, opaque lines of communication. Private sector interviewees said they didn't know who to turn to for information or collaboration. When they attempted to work with federal agencies, many rarely ever heard back from them or received information in return. This can lead to a lack of trust that disincentivizes intelligence sharing. One interviewee noted, "If there is no perceived value to this information and these relationships, I or my company will invest our time and resources elsewhere."

The National Network of Fusion Centers, serving states and major urban areas, serve as the primary focal point for the gathering and dissemination of threat information and even threat mitigation at the state and local levels with the federal government through DHS.[7] Every fusion center is different, operating based upon each state's or major urban area's priorities, resources, and cultures, but generally the cyber missions at each are small.[8] In fact, according to the 2018 National Network of Fusion Centers Final Report, only 56% of fusion centers identified cybersecurity as a top priority.[9] Illustrating this point, the presence at one fusion center we explored was limited to a few analysts and their workstations (not a

[5] Interview with head of cybersecurity threat intelligence at major US financial corporation, January 28, 2021

[6] Interview with Sean Plankey, former Department of Energy Principal Deputy Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response, February 11, 2021.

[7] https://www.dhs.gov/national-network-fusion-centers-fact-sheet

[8] Interview with Brian Nussbaum, July 21, 2020

[9] https://www.dhs.gov/sites/default/files/publications/2018_national_network_of_fusion_centers_final_report.pdf

Security Operations Center or SOC).[10] Because of the way DHS and the fusion centers were established after September 11th 2001 and in light of homeland security and civil liberty laws, (which operationally means that fusion centers do not monitor and instead rely on reporting from the public)[11] these centers are law-enforcement centric and focused on homeland emergencies and criminal activities. Indeed, the National Fusion Center Association states its cause is to "...prevent and reduce the harmful effects of crime and terrorism on victims, individuals, and communities."[12]

As vital as this mission is for state and local homeland security, it does not scale well to cybersecurity from a strategic, national security perspective, nor was it designed to do so. These fusion centers are run by state law enforcement entities and are generally focused on crimes and homeland emergencies within that particular state or major urban area. This does not lend itself to strategic analysis and collaboration to respond to nation state cyber threats, especially when not in constant collaboration with federal and private sector entities.

> "We had to unlearn a great deal of what we thought we knew about how war—and the world—worked. We had to tear down familiar organizational structures and rebuild them along completely different lines, swapping our sturdy architecture for organic fluidity, because it was the only way to confront a rising tide of complex threats."[13]

[10] Interview with former state homeland security official, June 19, 2020

[11] Interviews with State Fusion Center leader Dec 14, 2020 and County Intelligence Analysis Center analyst, February 11 2021

[12] https://nfcausa.org/

[13] McChrystal, Stanley A. *My Share of the Task: A Memoir*. Portfolio, 2013.

Objective 1: Create a network of Collaborative Defense and Analysis Centers at CISA Regional Offices

To create the structure and capacity for sustained, whole-of-nation collaboration and sharing, we believe CISA should transform its Regional Offices from advisory posts to collaborative defensive and analysis centers (CDACs), following the motto, “It takes a network to defeat a network.” Regional offices are key to this vision, as they offer physical breadth for the mission and functional diversity, as well as a field office touchpoint and access for businesses and states operating within that region. Such a structure would ensure a sustained, government-led coordinated presence in all regions of the country to combat the threat on a local level. Further, this structure offers visibility, sustainability, and scale, which are vital attributes for protecting critical infrastructure from cyber attacks.

It Takes a Network to Defeat a Network

To operationalize the mindset that,“it takes a network to defeat a network,” an organizational model that is responsive to domestic cybersecurity operations and that is geared toward increasing our resiliency and defense structure is critical now more than ever. In other words, reimagining and designing a truly collaborative defense architecture in which cyber operations are coordinated in planning and execution, and driven by analysis and rapid sharing of threat intelligence among, and between networked nodes and a common situational awareness across the entire system.

We propose the creation of a unified command structure led by CISA with an interconnected and federated network of collaborative operations centers. A new operational director role should be established within CISA’s forthcoming Joint Cyber Planning Office (JCPO) with accompanying staff.[14] This network of centers should utilize the current CISA Regional

[14] The Joint Cyber Planning Office was recommended by the Cybersecurity Solarium Commission and created through the FY21 NDAA to coordinate cyber planning and readiness across the federal government and between public and private sectors. https://www.king.senate.gov/newsroom/press-releases/ndaa-enacts-25-recommendations-from-the-bipartisan-cyberspace-solarium-commission

Office physical and communications infrastructure; however, they must incorporate cross-functional teams of analysts and operators from the public and private sectors, sitting alongside each other and working in collaboration to defend against myriad cyber operations by nation state and non state actors alike. In some ways, the proposed organization and function will be comparable to the National Cyber Security Centre (NCSC) in the United Kingdom[15]or the National Criminal Forensics Training Alliance (NCFTA)[16] but should be scaled to and modified to fit the requirements and realities of the threats against U.S. national security.

> "The future of CISA is in the field"
> —Chris Krebs

Currently, the 10 CISA Regional Offices house Cyber Security Advisors (CSAs), Physical Security Advisors (PSAs), Emergency Communications Coordinators, and Chemical Security Inspectors, and should be a key part of this connected infrastructure. The CSAs sitting at the Regional Offices "*offer cybersecurity assistance to critical infrastructure owners and operators and SLTT governments. CSAs introduce organizations to various CISA cybersecurity products and services, along with other public and private resources, and act as liaisons to CISA cyber programs. CSAs can provide cyber preparedness, assessments and protective resources, strategic messaging, working group support and leadership, partnership in public-private development, and incident coordination and support in times of cyber threat, disruption, and attack.*"[17] Indeed, PPD-21 states the success of these regional centers, "*including the integration and analysis function, is dependent on the quality and timeliness of the information and intelligence they receive from the SRMAs and other Federal departments and agencies, as well as from critical infrastructure owners and operators and SLTT entities.*"[18]

To create the structure and capacity for sustained, whole-of-nation collaboration and sharing, we believe CISA should transform these Regional Offices from advisory posts to collaborative defensive and

[15] https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

[16] https://www.ncfta.net/

[17] https://www.cisa.gov/cisa-regions

[18] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

analysis centers (CDACs). More importantly, within each CDAC, analysts would sit side by side, analyzing and sharing cyber threat intelligence, providing early warning across the ecosystem, and coordinating defensive actions with stakeholder organizations.

> "Organizations must be networked, not siloed, in order to succeed…Specifically, we restructured our force from the ground up on principles of extremely transparent information sharing and decentralized decision-making authority. We dubbed this goal—this state of emergent, adaptive organizational intelligence—shared consciousness, and it became the cornerstone of our transformation."[19]

Cross-functional teams of analysts and operators must have representatives from myriad stakeholders and organizations. Additionally, each Regional CDAC should be led by a Regional Director who is empowered to make decisions regarding operations and analysis, personnel, and office needs and who is aligned with the open and collaborative ethos mandated by this mission.

There is an ongoing debate about whether to grant participants clearances, or to keep everything at the unclassified level. On the one hand, clearing every person to at least the secret level will build trust between people by ensuring that communication and information flow is maximized, instead of compartmentalized. Some have argued that doing so introduces risk and is unsustainable; however, the concept has been proven with the National Defense Cyber Alliance, a nonprofit partnering with the FBI, which has granted its participants secret-level clearances.[20] If leaders decide against granting everyone clearances, the FBI and CISA must continue to issue time-sensitive and unclassified advisories as coordinated with US CYBERCOM and the Intelligence Community.

[19] McChrystal, General Stanley A., et al. *Team of Teams*. Portfolio Penguin, 2015. p153

[20] https://federalnewsnetwork.com/cybersecurity/2020/09/cisa-fbi-working-with-industry-to-make-it-more-painful-for-hackers-to-function/

The Case for an Unclassified Cyber Intelligence Framework

—Paul Kolbe

A common assumption is that the best cyber intelligence must be based upon sophisticated, classified government collection systems, capabilities, and processes. Certainly, the National Security Agency, Department of Homeland Security, and other members of the IC possess bring powerful tools and insight. Indeed, some have speculated that the SolarWinds attack would have been detected and prevented, had only the NSA sensors and tripwires been facing in the right direction - domestically as well as internationally. Legislation is being considered which would unshackle US spy agencies to monitor US based networks for signs of attack.

But it is worth considering the advantages of fully unclassified national cyber intelligence public-private partnership to play a primary role in the nation's cyber defense. Effective national cyber defense depends upon speed and breadth of threat notification. The more quickly a new threat can be identified, and the more and widely this intelligence can be disseminated and acted upon, the fewer systems which will compromised or remain vulnerable. Knowledge is a powerful anti-viral, but classification of data slows and restricts the flow of critical threat intelligence.

Open-source collection can be a powerful, indeed necessary, complement to sensitive government collection and should provide baseline threat intelligence accessible to all.

Speed, scale, and accessibility of threat intelligence is of paramount importance in staying ahead of the cyber offense. There is obviously a role and need for classified government cyber capabilities and operations. But when it comes to enabling a true national defense, which in practice means defense of our private sector networks, the speed, flexibility, and scale that an unclassified, open-source, private sector driven intelligence can bring to the fight should be our foundational approach.

As a start, we propose the following organizations and sectors have a seat in the CDAC:

- FBI
- DHS/CISA
- A representative from **each state fusion center** within that office's region
- A representative from **each critical infrastructure sector** within that office's region
- A representative from **each Sector Risk Management Agency (SRMA)**
- A representative from the **ISACs and ISAOs**
- Representatives from **major corporations and businesses** operating in that region
- A representative from **each major municipal service area** in the region
- A representative from the **NCFTA** depending upon the region
- **Lawyers** representing the interests of private sector firms and federal government, to serve as referees should legal questions or issues arise

Despite major companies' national footprint, we believe that regional offices are key to this vision, as they offer physical breadth for the mission and functional diversity, as well as a field office touchpoint and access for businesses and states operating within that region. Even though cyberspace has no boundaries, people, companies, utilities, assets, infrastructure all reside somewhere and so we believe it is vitally important to have sustained, coordinated presence in all regions of the country to combat the threat on a local level. As Chris Krebs has noted, *"the future of CISA is in the field,"* demonstrating that the solution to combating cyber adversaries is not solely in Washington, DC, but rather based on information and operations at the local level. Further, this structure offers visibility, sustainability, and scale, which are vital attributes for protecting critical infrastructure from cyber attacks.[21] We urge revamping and revitalization of these centers as regional hubs for cybersecurity information and operations, to include the following:

- Expand the physical footprint of each office to create space, computers/workstations, and seating for at least 50 people during 24/7 operations.
- Increase internet bandwidth for defensive cyber operations and strategic communications.
- Ensure these physical offices are inviting and open.
- Ensure access to a suite of top-of-the-line technology and tools for analysis and communications as well as enterprise licenses to all threat intelligence commercial sources. Also ensure connectivity to the Joint Collaborative Environment , or other enterprise-wide "data lake."

We decided to focus on the CISA Regional Offices instead of the National Network of State Fusion Centers for a number of reasons. First, we believe the fusion centers are vital to states' individual cyber and physical security realities and requirements; they were created to respond to homeland security threats and criminal activities, and have long-established processes for doing so. Second, while many fusion centers have relationships with local businesses and organizations and reach out to them when necessary, we envision organizations being co-located within centers. The scale needed to staff each state fusion center with the recommended personnel would be beyond the capabilities of many organizations. Third, state fusion centers are run by law enforcement entities. This law enforcement network remains a primary source of reporting from the public and local organizations, provides necessary reachback capability to state and local governments, and provides vital access to domestic networks through legal means to disrupt operations and help victims recover from computer network intrusion.[22] Because of the law enforcement focus, however, we believe the necessity to respond to time-bound emergencies and crimes and develop cases eclipses

[21] The Cyber Peace Institute. Playing with Lives: Cyber Attacks on Healthcare are Attacks on People; p.18 https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf

[22] Interview with State Fusion Center leader and County Intelligence Analysis Center analyst, February 11 2021

their ability to be strategic and focused on national security. As such, they should remain critical nodes of the overall national network, with state analysts having seats within the Regional CDACs with reachback capability back to their respective state fusion centers. Similarly, we chose not to utilize the Information Sharing and Analysis Centers and Organizations (ISACs and ISAOs) infrastructure because of their sectoral focus and inward connectivity, while recognizing their importance to the overall mission. Because we advocate for a cross-sectoral, cross-domain, and cross-functional approach to the issue, we want to utilize infrastructure that can be connective across the ecosystem.

As the hub for each region, each representative to the CDAC would have reachback capability to their own corporate/organizational, ISAC, state, or local offices for additional analytic or operational support. They would also have an intrinsic understanding of the entities in the region. Furthermore, regional offices would notionally be better at educational outreach to states, major municipal areas, businesses, and even the general public, if staffed and funded appropriately (and should employ marketing experts). Critical to the success of these networked nodes is their connectivity to each other, not only from a communications architecture standpoint, but also from an organizational and cultural one. Regarding communications, every workstation in every regional office must be on the same email, chat, and telephone system.

> "The hallmark of distributed governance is openness that supports deep and real communications, coordination, and connection...leaving behind the strict rules and tight control of information that retards innovation and collaboration."
> —Stephen Goldsmith[23]

Each day or night, there should be an enterprise-wide "operations and intelligence" briefing that everyone in each CDAC can observe to ensure situational awareness across the nation, including representatives from the Office of the National Cyber Director. Not only should analysts share strategic intelligence, but operators should also debrief incidents or defensive and offensive

[23] Goldsmith, Stephen. A New City O/S: The Power of Open, Collaborative, and Distributed Governance. Brookings Institution Press, 2017

operations, noting any major reflections from those activities. This will be the thread that holds all the nodes in place—it is vital to the concept of national situational awareness of the threat and to coordinating defensive actions.

To ensure true collaboration, policies must complement the organizational structures. Compelling organizations to share and collaborate (in addition to incentives) is vital to this construct, according to Bryson Bort.[24] A federal breach notification law is essential to shape the broader sharing environment and to incentivize private sector entities to collect and share information in real-time. At the state-level, governments have initiated unique measures to improve cybersecurity by increasing public visibility of private sector entities with weak security. California has led this movement enacting both the California Consumer Privacy Act in 2018 and an updated version with the California Privacy Rights Act of 2020, giving the state's consumers greater control and information on how their data is being used in a similar fashion to the European GDPR.[25] States around the country are following in California's legal footsteps, with similar data privacy laws being passed in New York, Massachusetts, and Maryland among others. These regulations incentivize private sector entities to invest in cybersecurity to avoid economic and reputational damage.

Used as a tool to incentivize rather than to compel, enacting a federal data privacy law in addition to a federal breach notification law proves crucial for the advancement of our model. Many experts in the cybersecurity field share these views. For example, Dmitri Alperovitch, Silverado Policy Accelerator, recently delivered Senate Testimony to the U.S. House Committee on Homeland Security reaffirming this lack of a comprehensive federal breach notification law.[26] Additionally, the Cyberspace Solarium Commission Report also recommended federal data privacy and breach notification laws in Pillar 4.7 of its report.[27] These proposals aim to increase companies' investment in cybersecurity and data protection, as well as provide a framework for more honest collaboration that improves cyber defense and avoids naming and shaming companies who are exposed to cyberattacks. The most difficult legal aspect to be considered with the breach notification law, in

[24] Informal discussion with Bryson Bort, July 7 2021 via Zoom

[25] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.185.

[26] https://homeland.house.gov/imo/media/doc/Testimony-Alperovitch.pdf

[27] https://www.solarium.gov/report

particular, would be how a breach would be defined and whether it includes solely one type of breach (such as material or PII breaches) or all breaches.[28] To ensure that such a law would be positive for our model, private sector entities must be reassured that data breach notifications will be met with public assistance and additional liability protections.

Bryson Bort recommends starting with the Critical Infrastructure Sectors.[29] As part of recommended safety and security frameworks that can evolve with changing threats, as well as a regulatory body that can certify and enforce standards for critical infrastructure, it may make sense to tack on information sharing and collaboration requirements, much like the Executive Order on Improving the Nation's Cybersecurity that requires federal IT and OT service providers to share information with federal agencies.[30],[31] Doing so will hopefully lay the technological and institutional groundwork for data collection and sharing across the ecosystem.

[28] Interview with Richard Jacobs FBI Assistant Special Agent in Charge, Cyber Div NYC Field Office, April 23 2021

[29] Informal discussion with Bryson Bort, July 7 2021 via Zoom

[30] https://inkstickmedia.com/why-are-we-so-vulnerable-to-cyber-attacks/

[31] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Objective 2: Scale Voluntary Data Collection and Processing

A human-to-human network should be complemented by a machine-to-machine network. Automated collective defense and data collection is a vital part of a resilient cyber posture for our nation. There have been several treatments on this topic, including the 2011 paper led by then-Deputy Under Secretary for the National Protection and Programs Directorate, Philip Reitinger entitled, "Enabling Distributed Security in Cyberspace" that we believe makes the compelling and important case for an automated machine-led collective defense using Automation, Interoperability, and Authentication as building blocks.[32] Such a machine-led collective defense network would also establish the infrastructure base for a robust data collection and anonymization capability as well as a base to collect metrics for analysis by the Solarium Commission-proposed Bureau of Cyber Statistics and the Cybersecurity Safety Review Board as ordered by the Executive Order on Improving the Nation's Cybersecurity.[33],[34] The new National Cyber Director (NCD), in concert with CISA and the Private Sector should work to make this vision a reality with private sector technical solutions and architecture. Given the ample treatment of this topic, however, we will focus instead on the need for increased data collection and processing in the remainder of this section.

Collecting more threat data, and processing it to detect anomalies and create a common operating picture is vital to the success of our cyber operations, offensive and defensive. We have the information and the technology to do this exists, but we do not have the infrastructure or the policies in place to drive coordinated, sustained sharing to create a holistic understanding of the threat at the strategic, operational, and tactical levels, as data resides siloed in countless networks.

[32] *Enabling Distributed Security in Cyberspace Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action,* March 23 2011 https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf

[33] Interview with Philip Reitinger, June 18, 2021

[34] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Using the SolarWinds example, there were clues–between the classified data points and the unclassified observation of activities on domestic servers and networks–but classification restrictions and inadequate infrastructure for data aggregation and sharing prevented piecing those clues together before it was too late. Two separate discoveries at two different cybersecurity companies three months apart led analysts to believe there was something going on, but at least one of those analysts didn't feel there was sufficient information to report it to the government.[35] But those were important data points that could have been helpful in their unfinished state to build a larger picture. The data is out there, but we are not collecting, indexing, processing, and sharing it with all the stakeholders who can analyze it and architect a rapid and coordinated response. And the adversaries know this—they often operate freely in domestic "blue" spaces because they understand that the NSA and USCYBERCOM cannot operate there.[36]

Critical to the success of a holistic solution are several factors, but chief among them are:

- Wide-scale, voluntary participation,
- The *automated* anonymization of such data (automatically stripping out sensitive, personally and organizationally-identifiable information) with the burden placed on the government-funded solution,
- Access controls based on authorities, and
- The processing and indexing of this data to be shareable instantly and throughout time and to detect and mitigate anomalies, freeing up analysts to actually focus on analyzing complex information.

CISA and the Department of Energy have tried to deploy voluntary data collection with programs like Automated Indicator Sharing (AIS) and the Cybersecurity Risk Information Sharing Program (CRISP). Both programs, as noted by the Cyber Solarium Commission, are foundational to collection of data, and could provide early warning capabilities if upgraded and

[35] https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

[36] Borghard, Erica and Schneider, Jacquelyn, Repercussions of SolarWinds, Defending Forward and Cyber Espionage. AFCEA Alamo Chapter. 19 January 2021. Webinar

increased in scale.[37] Created to facilitate information sharing between the public and private sectors by collecting indicators of compromise from participating organizations' networks, the program has unfortunately not scaled as hoped. According to an Inspector General report released in September 2020 (reviewing the system between 2017 and 2018), there are several institutional reasons the program has not reached its potential. First, AIS is hampered by sparse participation in the program; according to the report, in 2018 only 219 private sector organizations were members, limiting the amount of overall data shared within the confines of the system.[38] Second, and relatedly, participants found the information gained via use of AIS lacked the context required to be usable.[39] Third, upgrades to data sharing standards (Structured Threat Information eXpression (STIX)/ Trusted Automated eXchange of Indicator Information (TAXII)) were delayed, hampering automated sharing across the ecosystem.[40] Fourth, the program was understaffed, limiting outreach to the private sector.[41] Despite these updates to be completed by September 2021, the perceived cultural barrier of the DHS as a regulatory agency remains unchanged.

A similar program, the Department of Energy's Cybersecurity Risk Information Sharing Program (CRISP) also relies on voluntary participation from constituents within the energy sector and passively collects threat data from network perimeters and shares near-real-time network data, which undergoes classified analysis by DOE analysts and non-classified analysis using Pacific Northwest National Laboratory's advanced tools"[42] across every sector and at speed and scale. The Energy ISAC and DOE recently announced a partnership to expand CRISP's capabilities to collect and analyze raw operational technology (OT) data from industrial control systems (ICS) networks.[43]

The technology to collect and process data at scale and speed currently exists. Several cybersecurity threat detection companies deploy

[37] Cyber Solarium Commission Report, March 2020 https://www.solarium.gov/report

[38] https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-74-Sep20.pdf

[39] Ibid.

[40] Ibid.

[41] Ibid.

[42] https://www.energy.gov/sites/prod/files/2018/09/f55/CRISP%20Fact%20Sheet.pdf

[43] https://www.nerc.com/news/Headlines%20DL/CRISP%2030NOV20.pdf

architecture at network edge or internally to automatically collect data and then anonymize, aggregate, and apply analytics to the data to render it shareable, discoverable, and detect anomalies.[44] As such, the U.S. could compete and award a contract to an existing company to employ this technology to incorporate into the proposed Joint Collaborative Environment (JCE) which has provisions to protect this data and ensure that it is processed, indexed, and interoperable for sharing and analysis. The JCE, proposed by the Cyber Solarium Commission, would be a *"cloud-based environment in which the federal government's unclassified and classified cyber threat information, malware forensics, and network data from monitoring programs are made commonly available for query and analysis"* in addition to the data interoperability standards and other data processing requirements therein.[45] The Commission also recommended that all participating private sector entities participating in the JCE be extended the same protections as in the Cybersecurity Information Sharing Act of 2015, which protects entities from liability "for the sharing or receipt of cyber threat indicators or defensive measures" so as long as this information is shared through the real-time processing system at the DHS.[46] This data, however, does not need to be housed by a government solution if concerns over government control of data or surveillance are too great. Another solution might be to employ private sector sensors, instead of government ones, with local automatic anonymization, or even "double-blind" collection and sharing. In the spirit of public-private partnership the government could provide a significant amount of funding for the infrastructure and cloud services, but the technology and servicing of the solution could be accomplished through a third-party vendor, and even managed by a public-private partnership nonprofit.

One major technological challenge is the collection and processing of such data—asking every private sector entity to turn on logging and push out such data to the JCE on their own time and dime seems like a failing proposition; in fact Jamil Jaffer noted in the South Carolina Law Review that, *"nonetheless, imposing a minimization-like requirement, somewhat narrow though it might be, will likely make companies less likely to share in the first instance, at*

[44] One example is https://www.ironnet.com/ and another is https://www.trinitycyber.com/en-us/

[45] Cyber Solarium Commission Final Report https://www.solarium.gov/report

[46] Cybersecurity Information Sharing Act of 2015

least until the market develops CISA-compliant sharing systems or mechanisms that employ a technical capability along the lines authorized by statute."[47] The emplacement of this architecture with Internet Service Providers (ISPs), Cloud Service Providers (CSPs), and at state, local, and private sector networks is equally as important, and incentives for wide-scale voluntary participation should be considered. President Biden's Executive Order to Improve the Nation's Cybersecurity requires federal government service providers to collect and share data with federal agencies, and orders improved event logging requirements, laying the groundwork for this collection infrastructure and sharing norm.[48] For instance, one incentive to attract voluntary participation in such a program could include a legal clause that provides full liability protection to participating entities so long as entities meet a baseline of cybersecurity protections that could be developed with members of both the public and private sector, which might incentivize companies to invest more heavily in their own systems.

Yet another important source of threat intelligence data lies in our own hands. According to Symantec, in Q1 2020, 1 in 4200 emails were phishing attempts.[49] There is, however, no comprehensive solution for individuals to report phishing or other compromises, except to call their local law enforcement officers who may log the details of the attempted or successful compromise, but such a solution does not scale. We must build a voluntary and privacy-protecting method to crowd-source threat intelligence. In this case, individuals could push an email or other indicator of compromise to a system like the JCE that collects, aggregates, indexes, and anonymizes (minimizes) this data.

Legal Considerations

Two key legal barriers in the CISA of 2015 should be amended to facilitate the sharing of private sector information to the federal government. These include the minimization requirement upon private sector entities

[47] https://nationalsecurity.gmu.edu/wp-content/uploads/2017/01/Carrots-and-Sticks-in-Cyberspace.pdf

[48] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[49] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-q1-2020

for anonymizing data in Section 104(d) and the limited liability protection clauses in Section 106(d).[50] As advocated by Jamil Jaffer and others, we recommend that these two counterproductive regulations be removed from the CISA of 2015 to incentivize the voluntary sharing of information by the private sector.[51] Given the importance of data anonymization to enforce data privacy, the amendment to the minimization requirement could instead place the burden on the federal government which already possesses this technical capacity. In fact, the State and Local Government Cybersecurity Act of 2019 authorizes the DHS "to deploy technical or analytic capabilities or services that utilize classified cyber threat indicators or intelligence" on unclassified non-federal systems, which legally allows the federal government to assume the burden of anonymizing information for the private sector and increase the resources available for SLTT governments.[52] Moreover, new legislation should also extend the liability protection clause to yield more extensive protections to private sector entities who share information within any component of the collaborative network we recommend.

The third legislative amendment we recommend consists of the Pen Register Trap and Trace (PRTT) Statute that the Cyberspace Solarium Commission report highlights.[53] This electronic surveillance law restricts access to information on cyber threat indicators to electronic communication providers.[54] Private sector entities are thus unable to employ "active defense" mechanisms to track cyber threats after an attack on its systems. To more effectively collect data on cyberattackers, we agree with the Commission's recommendation that Congress should amend the PRTT Statute (18 U.S. Code § 3121) to include the exemptions that exist under the Wiretap Act (18 U.S. Code § 2511(2)).[55]

[50] In moving from the Cyber Intelligence Sharing and Protection Act of 2014 (CISPA) passed in the House, to the Cybersecurity Information Sharing Act (CISA) of 2015, the Senate removed a major liability protection clause that further limits private sector protection from liability. Legislators removed a clause that issued liability protection for the actions taken on the basis of information shared by the voluntary participation of private sector entities. Thus, while the CISA of 2015 was a step in the right direction, incentives for increased collaborative voluntary information sharing in the private sector are still lacking, in large part due to the lack of liability protection when sharing information.

[51] https://nationalsecurity.gmu.edu/wp-content/uploads/2017/01/Carrots-and-Sticks-in-Cyberspace.pdf

[52] S.1846 - 116th Congress (2019-2020): State and Local Government Cybersecurity Act of 2019

[53] https://www.solarium.gov/report

[54] [USC02] 18 USC Ch. 206: PEN REGISTERS AND TRAP AND TRACE DEVICES

[55] USC Title 18 - CRIMES AND CRIMINAL PROCEDURE

Objective 3: Creating a Culture Shift: Knocking Down Barriers to Effective Collaboration and Sharing

Make Collaboration the Norm

Much like the Task Force in the early 2000s, we must make a major cultural shift in domestic cybersecurity. First, as noted earlier, there is a significant disconnect between the field and Washington, DC. Therefore, we must flip the DC mindset on its head to promote an expeditionary culture in which major defensive operations occur in the field and DC is the reach-back office for the federal government. Joining this mission and gaining operational field experience should be essential to promotions, bonuses, and raises. Second, we must create a culture in which sharing and collaboration are the norm, not the exception. Many private sector entities are reluctant to work with government entities because of an imbalance in expectations. Many interviewees noted that they wouldn't know who to go to—would they go to the FBI, where many fear an investigation, or DHS, whose mission currently is to advise and provide resources to private sector entities? Furthermore, they feared any information provided to the federal government might disappear into a black hole and they would never hear from a particular agency again.

Mission-Focused Task Forces

Even for those private sector entities and state fusion centers who have had positive experiences in sharing information with the federal government, success has largely been based on singular (major) incidents and personal relationships. One person noted, "We do well during a major incident—it's the steady-state that is difficult. What would people do on a day-to-day basis...where there is not a 'compelling enough business case' to work together."[56] Similarly, Chris Krebs stated that, to date, in order to get people to work together, there must be a mission to rally stakeholders around—much like during the elections.[57] Perhaps,

[56] Interview with representative from U.S. major software company, February 25 2021

[57] Interview with Chris Krebs, March 5, 2021

therefore, missions may be aligned around countering the most destructive and disruptive espionage operations, countering destructive malware and ransomware, election security, and supply chain security; indeed the Ransomware Task Force recommends a holistic, sustained and coordinated approach to countering ransomware.[58] Creating the mission and priorities (set by the notional CISA Operational Director), the conditions and infrastructure (workspaces, personnel, funding, policies) for doing so, building the connective tissue between nodes (through culture and communications), and ensuring leaders believe in this mindset and execute in line with the values is critically important to achieving such a vision. Getting people to buy into the networked approach must be underscored. Interviewees stated that open sharing was hampered not only by liability concerns, but also the additional work (paperwork/sharing agreements, collection and anonymization of data, and sending it out) to share intelligence, and unfortunately, bureaucratic hurdles. Trying to work with government agencies can be an uphill battle because the culture and organizational infrastructure doesn't allow for systemic collaboration—the trust has not been built, and information remains currency.

> "In the world of intelligence, information was power, leading people at each stage to ask themselves a set of questions: Should we pass this intelligence, and if so, how much? If we share it, will we lose control over it? Will we get in trouble for sharing this information? Will those we pass it to use it in the way we agreed they would? Those doubts cost us speed and often diluted the intelligence, making it less likely to lead to targets... we widely distributed, without preconditions, intelligence we captured or analysis we'd conducted. The actual information shared was important, but more valuable was the trust built up through voluntarily sharing it with others."[59]

Mindset

Integrating disparate agencies and organizations' equities and cultures into a seamless mission may be a daunting task, but it has been done, not only in the aforementioned Task Force, but also with the National Cyber

[58] https://twitter.com/philreiner/status/1395041936235397121?s=20 referring to https://securityandtechnology.org/ransomwaretaskforce/report/

[59] McChrystal, Stanley A. *My Share of the Task: A Memoir*. Portfolio, 2013.

Investigative Joint Task Force, a unique multi-agency cyber center. When considering how even the FBI (which builds cases and conducts investigations over time) fit into an organization whose ethos was to move quickly and aggressively, the key may have been explicitly stated objectives as part of a crucial mission, much like the FBI's Joint Terrorism Task Force (JTTF). In the years following 9/11 the FBI's construction of the JTTF prioritized two things - saving lives and following the law - as the task force's guiding objective. Now, threat information from any JTTF partner organization spreads across the whole ecosystem in a matter of minutes, giving entities from international allies to local governments timely intelligence about terrorist threats.

Traditionally, where analysts are incentivized to produce a certain number of intelligence reports the focus is not on analytic and operational outcomes, but on metrics. And so, collaboration and information sharing then becomes not the goal, but an inhibitor to the number of reports produced by an organization. But, as one interviewee noted, "the most effective information sharing is done analyst-to-analyst and management does not know about it."[60] Indeed, in Lauren Zabierek's experience where the leadership removed the burden of production (i.e. numbers of reports) from the analysts and instead focused on analytic outcomes (and subsequently operational successes), the personnel became more entrepreneurial and innovative.

Most vital to realizing this vision is personnel. From leadership down to the lowest level, everyone must be welcomed and must buy into the mission. Focusing on people, rather than numbers is essential to this effort. This total cultural shift requires diversity in demographics, background, and experience. Make no mistake, this is not an environment in which one particular personality and demographic will succeed—we must move from stifled and stove piped to what Stephen Goldsmith calls a "potent recipe of data, public and private partners, and a focus on creativity and outcomes"[61] and it will take *everyone* as a matter of national security.

[60] Interview with Cyber Threat Intelligence Expert, via online chat. February 24, 2021

[61] Goldsmith, Stephen. A New City O/S: The Power of Open, Collaborative, and Distributed Governance. Brookings Institution Press, 2017

Objective 4: Unraveling the Interagency

As national cyber incidents perpetrated by nation-state actors increase, we need strategic and holistic understanding for operational decision making (offensive and defensive), and national response.

Ensure NCD Authority

When the Cyber Solarium Commission recommended the establishment of the office of the National Cyber Director (NCD) it wrote, "The NCD will be the President's principal advisor for cybersecurity-related issues, as well as lead national-level coordination of cybersecurity strategy and policy, both within government and with the private sector." When codified into law by the National Defense Authorization Act of 2021, Congress appeared to give the President more ability to shape the role, especially in light of the creation of the deputy national security adviser for cyber and emerging technology.[62] It seems, therefore, that the Deputy National Security Adviser for Cyber and Emerging Technology will handle Title 10 and 50 cyber issues (offense), and the NCD will be responsible for the rest of the interagency and engagement with the private sector (defense) from a strategic standpoint, while in continual coordination with each other.[63] This distinction is important, as the interagency cyber environment is characterized by competing equities and priorities, and not one person has been able to unravel this yarn to determine what the nation's cybersecurity priorities are and who arbitrates among interagency turf (i.e. budget), equity, and classification battles. Indeed, as one former senior CISA official noted, "if you can fix that issue, that would be monumental."[64] As such, we recommend the President imbue the NCD with authority to ensure the Director can determine priorities and hammer out interagency conflicts, in coordination with the Deputy National Security Advisor for Cyber and Emerging Technology.

[62] https://www.lawfareblog.com/how-national-cyber-director-position-going-work-frequently-asked-questions

[63] Ibid.

[64] Interview with Chris Krebs, March 5, 2021

To put this into operational focus, the NCD could delegate some tactical decision-making authorities down to the CISA JCPO Operational Director or may decide to step in and arbitrate informational equities—for instance, facilitate the rapid sharing of information between the FBI and a private sector entity to shut down a cyber espionage campaign, versus a long-term investigation. This direction is, in fact, where the Department of Justice seems to be heading and the NCD and NSC would do well to coordinate across the interagency and domestic landscape.[65] One of the biggest complaints we identified when it comes to the interagency environment is what is often referred to as "turf wars" with agencies (or even offices) competing over mission and information in order to stay relevant (and maintain budget) in the eyes of Congress. One current commercial (and former federal) threat intelligence expert we talked to said, "They all fight it out, swim lanes get divided, and all that really happens is that the "cyber budget" gets spread even thinner around the various alphabet agencies and now we're all less effective because we have less money."[66]

Make CISA its own free-standing Agency

While CISA serves as the de facto federal organization for domestic cyber security, its relative infancy and small budget ($1.6bn on operations and support in 2020) hamstring the agency from being able to respond to breaches rapidly while spreading information to other potentially affected entities.[67] Furthermore, while it does maintain a regional infrastructure, it carries a historically strong DC focus. One interviewee noted, "The problem I have with CISA by itself, or any DHS component by itself, is that they don't really exist outside of DC."[68] CISA's ten regional offices cover vast swathes of physical space with minimal staffing dedicated to cybersecurity. While the regional offices garner working relationships with private corporations and fusion centers, the lack of staffing and institutional focus creates difficulty in trying to offer customers consistent, high-quality information across the board. One fusion center employee noted that their regional CISA representative

[65] https://www.washingtonpost.com/politics/2021/07/01/cybersecurity-202-dojs-future-is-disrupting-hackers-not-just-indicting-them/

[66] Interview with Cyber Threat Intelligence Expert, via online chat. February 24, 2021

[67] CISA 2020 Budget. Link

[68] Interview with analyst from Oil and Gas ISAC, December 1, 2020

was very responsive, but that technical questions had to be routed back to DC and took much longer to receive answers.[69]

CISA's status as part of DHS is also an issue—some have noted concerns about its proximity to DHS law enforcement components (potentially limiting the pool of applicants and the desirability to work closely with them) and recently the confirmation of the CISA Director nominee Jen Easterly was held up for unrelated political reasons, hampering the agency's effectiveness in the midst of worsening ransomware attacks.[70] As such, many are beginning to call for CISA's independence from DHS.[71] While we acknowledge this will be a massive undertaking, we support such a bid for independence, as we believe it would give greater authority, bigger budget, and more operational flexibility to an agency that desperately needs it. Moreover, it would provide greater flexibility in hiring practices as it looks to scale up and out (as we've informally heard frustrations over hiring rules), and would assuage concerns over its political baggage. We also believe that it would allow for reform of the Sector Risk Management Agency construct as described below.

Sector Risk Management Agencies

One step down, we must address the Sector Risk Management Agency (SRMA) approach to securing critical infrastructure as laid out in Presidential Policy Directive-21. As Sean Plankey, former Principal Deputy Assistant Secretary at the Department of Energy noted, PPD-21 was written before the creation of CISA,[72] and DHS is tasked with serving as the federal liaison to ten of sixteen critical sectors, ranging from chemicals to dams and information technology, roughly 85% of which is privately owned.[73] Although well-meaning and comprehensive for the time in which this Directive was introduced, the result is disjointed, uncoordinated, and imbalanced investment by federal agencies with varying budgets and personnel to attempt to reach out to their critical infrastructure partners, collaborate, and

[69] Interview with State Fusion Center leader and County Intelligence Analysis Center analyst, February 11 2021

[70] https://www.cyberscoop.com/cisa-senate-jen-easterly-confirmation/

[71] https://thehill.com/opinion/cybersecurity/560920-america-deserves-a-cabinet-level-department-of-cybersecurity?rnd=1625069385&rl=1

[72] Interview with Sean Plankey, former Department of Energy Principal Deputy Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response, February 11, 2021

[73] FEMA Evaluation of critical infrastructure. Link

share intelligence. For example, the Transportation Security Administration within DHS is the lead on pipeline security, but has little cybersecurity capability, and the Environmental Protection Agency is the lead for securing water and wastewater, yet they have a handful of people responsible for security and collaboration with the thousands of water and wastewater treatment utilities in the country, and none with cyber expertise.[74] As the Cyberspace Solarium Commission noted in their 2020 report, SRMAs are underfunded and overmatched in their role as the main touchpoints between the federal government and critical infrastructure.

PPD-21 should be revised to enhance collaboration and sharing across all sectors and entities, transforming the focus from a sectoral approach, to a cross-sectoral, mission-focused, collaborative one. Further, the cybersecurity missions and requirements to collaborate and share information with private sector partners levied upon each Sector Risk Management Agency should be transferred instead to the wholesale mission within CISA, and led operationally at Headquarters and at the CDACs. Much like the FBI has functional divisions at its headquarters with connectivity to its field offices, CISA could also create divisions and interagency task forces with the SRMAs to ensure coverage of the nation's critical infrastructure. The current SRMAs, however, should maintain awareness, oversight of regulatory and statutory requirements, and institutional knowledge and expertise on the physical side. Of note, the Departments of Energy and Treasury are known to have highly capable cyber offices and so decisions to transfer capabilities out would have to be weighed carefully and done thoughtfully.

Intelligence Requirements

According to Intelligence Community Directive-204, the Director of National Intelligence is responsible for promulgating a National Intelligence Priorities Framework (NIPF) document to the intelligence community (IC) and updating it every six months.[75] This document contains a matrix of national intelligence priorities from which all 18 members of the IC draw their mission. The priorities are reviewed and approved by both the President and NSC; consequently strategic competitors and their

[74] https://abcnews.go.com/Politics/critics-tsa-understaffed-ill-equipped-pipeline-security-mission/story?id=77696947

[75] https://www.dni.gov/files/documents/ICD/ICD_204.pdf

capabilities occupy large parts of the framework. Given that the IC's main assets are statutorily prohibited from engaging in steady-state operations on domestic soil the NIPF focuses primarily on external threats to national security. Therefore, cyber threat intelligence itself is but one of a number of priorities and domestic cyber threat intelligence holds a much lower priority. While ODNI has a private sector programs group, it is not specific to cyber threats and focuses its efforts on engaging with state and local government entities.[76]

PPD-21 directs "the efficient exchange of information, including intelligence, between all levels of governments and critical infrastructure owners and operators," however, there is a massive intelligence disconnect between the SRMAs interfacing with their private sector partners and the organizations within these agencies that conduct intelligence collection and analysis that are part of the Intelligence Community. The NIPF serves to outline external collection priorities to inform national decision makers and down-range operators alike. SRMAs have little ability to inform collection priorities from their private sector partners because the NIPF has little room for such collection requirements, yet successful nation-state cyber operations targeting the United States often do so from within "blue space" or domestic, private sector infrastructure. This disconnect has devastating consequences on our security and creates difficulties for primarily domestic-focused federal agencies like the Department of Energy (DoE), which serves as the SRMA for America's energy sector. As the SRMA for energy, the limitations of the NIPF leave little funding and focus on the threat intelligence requirements from DoE's customers, namely critical energy and utilities companies. The DoE, in short, is stuck between two end customers with different requirements. The misalignment of priorities yields inequities in authority, funding, and staffing which impede the effectiveness of the domestic cyber threat intelligence atmosphere when demand for such capabilities is on the rise.

ODNI's Cyber Threat Intelligence Integration Center or CTIIC, is "the federal lead for intelligence support in response to significant cyber incidents, working on behalf of the IC to integrate analysis of threat trends and events, build situational awareness, and support interagency efforts

[76] Interview with ODNI senior official, April 7, 2021

to develop options for degrading or mitigating adversary threat capabilities." The CTIIC and the National Intelligence Manager for Cyber were consolidated under the ODNI's Cyber Executive Office under the Trump administration, with concerns from Congress. In doing so, the office eliminated the National Security Partnerships office, which engaged with state and local government and the private sector.[77] The goals of such a move ostensibly gave ODNI a single focal point for the cyber mission; however, issues remain. As Sean Plankey noted, "the Director of CTIIC has always been a JDA (joint duty assignment)"[78] which, as any federal civilian employee understands, lacks institutional experience and authority needed to compel other offices to cooperate.

Our recommendations are two-fold. First in line with Tatyana Bolton and Bryson Bort's recommendation that CISA become a standalone agency, we recommend that CISA establish an internal intelligence arm, becoming the newest member of the Intelligence Community. That way, this office can work with the CDACs to inform the NIPF process and drive collection requirements and integrate analysis priorities for cyber threats focused on the homeland. Second, we recommend the CTIIC director role be transitioned from a JDA to a permanent Senior Executive Service position to put more weight and authority behind the role, coordinating across the entire IC and continuing to work closely with the NCD and the NSC during evolving or ongoing threats and incidents.

[77] Interview with ODNI senior official, April 7, 2021

[78] Interview with Sean Plankey, former Department of Energy Principal Deputy Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response, February 11, 2021

Objective 5: Personnel: Pipeline, Training, and Exchanges

Service Year

We often read about the gap between the number of open jobs in cybersecurity and the number of "qualified" personnel. According to CyberSeek, there are over 500,000 open cybersecurity jobs and the US lacks the qualified personnel to fill them.[79] Further, of those entering into the career field, estimates say that one in four have the requisite experience for these roles.[80] While the "pipeline" will continue to be a perennial issue, there are early-or mid-career professionals who are working toward employment in the cybersecurity field but for a variety of reasons (lack of experience, systemic racism and sexism, and lack of certifications and training) find difficulties making the jump from training to employment. To bridge that gap, we propose a "service year" in which a person interested in cybersecurity can receive training and support for certification in exchange for a year of service at one or more of the CISA Regional CDACs. Service Year Alliance, a nonprofit nonprofit working to make a year of service a common expectation and opportunity for all young Americans, believes that,

> *"A service year before, during, or after college—or as a way to find your path—gives young people the chance to transform their lives, make an impact in their community, and become the active citizens and leaders our nation needs. Expanding service years has the power to revitalize cities, uplift and educate children at risk, and empower communities struggling with poverty. It can unite the most diverse nation in history, binding people of different backgrounds through common cause."*

President Biden recently signed into law the American Rescue Plan which includes $1 billion for national service, which is a great opportunity

[79] https://www.cyberseek.org/heatmap.html

[80] https://www.fifthdomain.com/home/2017/02/13/isaca-cybersecurity-skills-gap-leaves-orgs-exposed-for-6-months-or-longer/

for the cybersecurity workforce. We recommend that the White House establish an interagency service corps in partnership between DHS (for now, eventually to CISA as a standalone agency) and the Corporation for National and Community Service to create opportunities for young people who want to serve in critical cybersecurity roles in the Regional CDACs. Funding should support training, clearance, administrative overhead, and salary costs for personnel to serve with public sector or non-profit entities that require additional personnel to support the mission. Indeed, such an arrangement would be a win-win: the nation gets more personnel into the cybersecurity field, these professionals receive an invaluable year of operational experience and free training in addition to a salary, and it could fuel civic renewal. The program resembles military service in some ways, but differs, importantly, in that such professionals do not have to wear a uniform, do physical training, or owe more than a year. As former CISA cyber policy lead in the Office of Strategy, Policy and Plans and Cyber Solarium Commission senior director, Tatyana Bolton stated, "national service is a highly underutilized and underfunded priority. Not only should we prioritize it, but it is a no-brainer that we should include cybersecurity as a key facet of national service."[81]

[81] Interview with Tatyana Bolton, former CISA and Cyber Solarium Commission official, January 22, 2021

Training and Exchanges

On the other end of the spectrum, to raise the level of analytic capabilities across the federal entities in cybersecurity, we propose creating opportunities for analytic exchange between CISA, FBI, and NSA. Not only would such an arrangement continue to build connective tissue between the interagency elements, but would provide vital experience and training to federal analysts. Using the Joint Duty Assignment administrative framework, these agencies can set the number of billets to be exchanged between agencies per year and advertise the program with their employees. Furthermore, those analysts on exchange would be qualified to 'deploy' to the regional offices under different authorities, gaining critical experience and operation lessons in the field that they can take back with them to their home offices, staying in-mind when conducting offensive cyber operations or case-based investigations. This is an area the NCD must designate as a priority and seek any additional funding as well as billets (or somehow create a system that doesn't require movement of billets, opting instead for a seamless and easy transition between agencies).

Community Outreach

Finally, the Regional CDACs should be empowered to conduct community outreach as well, and should be visible beacons of security and diversity to get people interested in cyber and offer pathways into the industry. As a former Sean Plankey noted, the government assumes that people will want to work with them but has found that is not often the case for a variety of reasons[82]—as we've discovered in our research, a lot of that reticence is based on a lack of awareness and ease of working with government partners; therefore we believe marketing to the public and to private sector entities is extraordinarily important to the success of the mission.

[82] Interview with Sean Plankey, former Department of Energy Principal Deputy Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response, February 11, 2021

Conclusion

These recommendations are designed to build upon PPD-21 and 41 and the recent Cyber Solarium Commission report. We recognize that when these Directives were written, they envisioned a system in which collaboration and information sharing between the federal government, state and local government, and the private sector were the norm. Unfortunately, that vision has yet to be realized, but we believe with some improvements, we can greatly invigorate these efforts.

At the heart of the domestic cyber threat information sharing and operational collaboration issue is the lack of structures (organizational and technological) and policies (cultural and legal) to facilitate holistic, coordinated, and sustained activities. We believe that the similarities between counterterrorism and cybersecurity—in how the adversary operates by blending into a larger "population" and utilizes the sprawling infrastructure of the internet to perpetuate network spread—beget similarities in how we organize to combat the rising tide of threats using asymmetric capabilities. Therefore there are relevant organizational and cultural lessons learned from special operations that we could apply to domestic cybersecurity. Where there are areas of overlap and conflict, we can start the work to unravel. We can harness the power of current technology to collect and process data, making it easier for private sector entities to participate. And we must focus on the policies that complement the structures to facilitate collaboration, namely insufficient information sharing provisions and burdensome paperwork that make it difficult, time-consuming, and expensive for entities.

Echoing our piece in the Cipher Brief, "the bottom line is that the faster and more widely threat information can be analyzed, disseminated, and actioned in a coordinated manner, the less success attackers will have. Such coordinated actions must be conducted domestically at the tactical level, and externally at the operational and strategic level by the federal government. This is key to a "whole-of-nation" approach that will increase the United States' resilience against cyberattacks."[83] Such a monumental and challenging shift is necessary to improve our safety and well-being as well as our national security writ large.

[83] https://www.thecipherbrief.com/column/cyber-advisor/reimagining-our-domestic-cyber-defense-posture

The Cyber Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/Cyber

Printed in the United States of America