A National Cybersecurity Agenda for Resilient Digital Infrastructure

Aspen Cybersecurity Group

ASPEN DIGITAL
THE ASPEN INSTITUTE

December 2020

Table of Contents

Foreword

In 1858, a public health crisis gripped the city of London. Successive cholera outbreaks spread by contaminated water were killing thousands. The river Thames was so polluted that Parliament refused to meet. As London's population exploded, no one had invested in the basic wastewater infrastructure necessary to manage the consequences of cramming millions of people into one of the world's first metropolises. After years of failing to safeguard access to clean water, the government finally embarked on an unprecedented civil works project to retrofit the entire city with its first sewer system.

Cyberspace today resembles London in 1858. Just as water provides the foundation for human health, the Internet has become the delivery platform and interface for nearly every aspect of our economy and daily life. And like the cholera that thrived in the polluted waterways of London, malicious actors are exploiting our society's stubborn reluctance to invest in the security and resilience of our technology. We built our digital society on a shaky foundation, entrusting our most critical data and activities to systems and tools that were not originally designed with security as a core objective. The revolutionary openness of the Internet was world-altering, but today that very same openness increasingly is used as the vector to undermine its success. And we have yet to invest in the infrastructure, practices, and institutions necessary to protect digital technology.

We consistently underestimate how bad actors might weaponize our technology against us and cause real harm. During the COVID-19 pandemic, we have seen nation-states target the intellectual property of drug developers and criminal groups disrupt already-hospitals with ransomware. All manner of actors are spreading mis- and disinformation about the sources of coronavirus, dangerous and unconfirmed treatments, stay-at-home orders, the efficacy of vaccines, and more.

Yet despite more than a decade of studies, warnings, and high-profile incidents—including those that have already cost companies like Merck, Maersk, and FedEx hundreds of millions of dollars—the government's investment in cybersecurity prevention and response remains woefully inadequate. After the 9/11 attacks, there was no mistaking that the U.S. government was wholly and totally committed to confronting terrorist organizations. It created a new cabinet department (the Department of Homeland Security), and new federal leadership (the Office of Director of National Intelligence and National Counterterrorism Center). It designated billions of dollars of funding toward state and local preparedness. The entire federal apparatus mounted a herculean effort to reorient budgets, processes and priorities.

We see no similar mobilization toward securing the Internet and our digital lives. Warnings of a "Cyber 9/11" have not supplied the trigger. Neither have the untold billions of dollars in damages already caused by cybercrime, ransomware, intellectual property theft, and espionage.

The cybersecurity community's tendency to treat cybersecurity as a problem to be solved has not been effective. Instead, we need to convey cybersecurity as an inextricable element of the digital infrastructure on which all society's priorities depend. Cybersecurity is modern life, and we cannot use cyberspace without it. It is critical to the way we work, the way we bank, the way we shop, the way we drive. The unprecedented events of 2020 have underscored that technology and security are now also central to the way we vote, the way we deliver health care—even the way we spend time with our loved ones amid a pandemic. With half of the American workforce operating from home, billion-dollar corporations are running on Zoom and Slack. Digital technology should be treated like water --the most essential resource—and cybersecurity as the foundation for making it work for every stakeholder community. As our digital dependencies intensify, our way of life will not be possible without better cybersecurity risk management. Digital resilience must become central to everything we do.

This document outlines achievable action steps that we believe will allow federal policymakers to make rapid progress toward a much stronger cybersecurity foundation for our digital infrastructure. Some can be accomplished in weeks or months; others will probably take years. Fortunately, the federal government is not alone. Cyberspace is ultimately the domain of civil society and private enterprise, sectors teeming with experts who can guide the White House and Congress as they grapple with the difficult tradeoffs inherent to any cybersecurity policy decision. In crafting this national cybersecurity agenda, the Aspen Cybersecurity Group sought input from a diverse network of partners in academia and industry. Together, we stand ready and willing to assist policymakers in cultivating a secure, reliable, and resilient cyberspace.

Aspen Cybersecurity Group

The Aspen Cybersecurity Group provides a standing, public-private forum to bridge the gap between policymakers, industry executives, security professionals, and civil society leaders. It aims to operationalize consensus solutions to the hardest cybersecurity problems by cultivating honest dialogue and forging lasting partnerships between government agencies, companies, nonprofits, and individuals.

Current Members

Kate Adams, General Counsel, Apple

Gen. Keith Alexander, Co-CEO, IronNet Cybersecurity

Sara Andrews, CISO, PepsiCo

Monika Bickert, Head of Global Policy Management, Facebook

John Carlin, Chair, Cyber & Technology Program, Aspen Institute

Vint Cerf, Chief Internet Evangelist, Google

Lucy Fato, General Counsel, AIG

Sue Gordon, Founder, GordonVentures LLC

Dr. Lorrie Faith Cranor, Director, CyLab Security & Privacy Institute, Carnegie Mellon University

Michael Daniel, President and CEO, Cyber Threat Alliance

Jim Dempsey, Executive Director, Center for Law & Technology, UC-Berkeley

Don Dixon, Co-Founder & Managing Director, ForgePoint Capital

Lynn Good, CEO, Duke Energy

Aspen Cybersecurity Group – Current Members

Alex Gorsky, CEO, Johnson & Johnson

Yasmin Green, Director of Research, Jigsaw

Gen. Michael Hayden, Principal, The Chertoff Group

Susan Hennessey, Executive Editor, Lawfare

Rep. Will Hurd, Ranking Member,
Subcommittee on Intelligence Modernization and Readiness,
House Permanent Select Committee on Intelligence

Chris Inglis, Managing Director, Paladin Capital Group

Sean Joyce, Partner, PwC

Rep. James R. Langevin, Chairman,
Intelligence and Emerging Threats and Capabilities Subcommittee,
House Committee on Homeland Security

Herb Lin, Senior Research Scholar, Stanford University

Brad Maiorino, Chief Strategy Officer, FireEye

Jeanette Manfra, Director, Government Security and Compliance,
Google

Chandra McMahon, CISO, CVS Health

Lisa Monaco,
Former White House Homeland Security Advisor and Partner,
O'Melveny & Myers

Craig Newmark, Founder,
craigslist and Craig Newmark Philanthropies

Mary O'Brien, General Manager, IBM Security

Dr. Greg Rattray, Adjunct Professor, Columbia University

Former Rep. Mike Rogers, Former Chair,
House Intelligence Committee

David Sanger, National Security Correspondent, New York Times

Dr. Phyllis Schneck, CISO, Northrop Grumman

▶ Aspen Cybersecurity Group – Current Members

Bruce Schneier, Fellow and Lecturer,
Harvard Berkman-Klein Center

Alex Stamos, Director, Stanford Internet Observatory

Kathy Warden, Chairman, President, and CEO,
Northrop Grumman

Michelle Zatlyn, Co-Founder and Chief Operating Officer,
Cloudflare

Jonathan Zittrain, Director, Harvard Berkman-Klein Center

Jane Harman (ex-officio)

Michael Chertoff (ex-officio)

Acknowledgments

The Aspen Cybersecurity Group is a forum for a diverse range of voices, and this report draws on the advice and expertise of a variety of outside partners and colleagues and across industry, government, and civil society. As with any attempt to distill the collective wisdom of an entire community, our efforts have relied on the counsel of too many individuals to acknowledge here. But we would like to give special thanks to people and organizations who graciously volunteered their time to reflect on the challenges ahead of us and help craft a path toward progress.

This report was compiled, managed, and written by David Forscey, with assistance from the entire team at Aspen Digital, including Savilla Pitt, Garrett Graff, Beth Semel, Carner Derron, and Vivian Schiller. Special thanks to Betsy Cooper, Meha Ahluwalia, Mai Sistla, Dominique Harrison, and Kristine Gloria for their contributions on some of the report's most important sections.

Individuals

Marene Allison
John Bansemer
Laura Bate
Kristin Berdan
Sharon Bradford Franklin
David Clark
Larry Clinton
Gary Corn
Jennifer Daskal
Mieke Eoyang
Gregory Falco
Alan Friedman
Michael Garcia
Harley Geiger
Tracie Grella
Jay Healey
Trey Herr
Yurie Ito
Ryan Kalember
Elena Kvochko
Nick Leiserson
Tim Maurer
Marian Merritt
Erin Miller
Mark Montgomery
Travis Moore
Sarah Morris

Acknowledgements

Ben Moskowitz
David Mussington
David O’Brien
Allison Peters
Michael Prebil

Philip Reiner
Diane Rinaldo
Paul Rosenzweig
Ross Schulman

Ari Schwartz
Steven Trush
Sam Visner
Beau Woods

Organizations

Atlantic Council
American University
Berkman Klein Center for Internet and Society
Columbia University
Consumer Reports
Carnegie Endowment for International Peace
Cybersecurity Coalition
CyberGreen
Global Cyber Alliance
Institute for Cyber Law, Policy, and Security
Internet Security Alliance

MITRE
National Initiative for Cybersecurity Education
National Institute for Standards and Technology
Open Technology Institute
Proofpoint
R Street Institute
Space ISAC
Technology for Global Security
Third Way
University of California Berkeley
U.S. Cyberspace Solarium Commission for Standards and Technology

Special Acknowledgments

This report is made possible thanks to the generosity and support of the William and Flora Hewlett Foundation and Craig Newmark Philanthropies.

Purpose and Scope

This agenda is designed to assist federal policymakers in prioritizing, planning, and executing actionable cybersecurity initiatives whose goals are achievable in the next four years. Its intended audience is political appointees and career officials across the executive branch, federal lawmakers and their staff teams, and professional staff on congressional committees.

Note that this is not a framework for a national cybersecurity strategy, although most of its content should figure into one. A comprehensive strategic framework would need to describe clear roles for the private sector and civil society in addition to government—and operate at a global scale.

The next administration and Congress cannot simultaneously address the wide array of cybersecurity risks confronting modern society. Policymakers in the White House, federal agencies, and Congress should zero in on the most important and solvable problems.

To that end, this report covers five priority areas where we believe cybersecurity policymakers should focus their attention and resources as they contend with a presidential transition, a new Congress, and massive staff turnover across our nation's capital:

- Education and Workforce Development
- Public Core Resilience
- Supply Chain Security
- Measuring Cybersecurity
- Promoting Operational Collaboration

Purpose and Scope

Each section defines the problem, makes the case for prioritizing it, establishes measurable outcomes, outlines past obstacles that have stymied past efforts, and details tangible action steps to overcome those obstacles.

This report is designed to be modular, with each section and its subsidiary recommendations able to stand on their own. We hope this will allow champions of specific focus areas to pick and choose based on changing political and business realities.

In selecting these five categories, the Aspen Cybersecurity Group sought to highlight initiatives that:

(a) Create leverage by offering "the greatest advantage to the defender over attackers at the least cost and greatest scale";

(b) Benefit from an established technical or organizational foundation that can facilitate rapid progress; and

(c) Are relevant to the industry stakeholders, researchers, and security thought leaders whose buy-in is essential.

While technically out-of-scope, some topics are too important to omit without mention. In the section on **Additional Priorities**, we briefly address some other areas that demand urgent attention from federal policymakers.

Action Steps at a Glance

Education and Workforce

Appropriate new grant funding and direct grantmaking agencies to support organizations dedicated to grow the representation of underrepresented communities in the cybersecurity field.

Change how employers recruit cybersecurity workers to diversify and expand the talent pool.

Authorize and fund a national repository of K-12 cybersecurity resources.

Create and scale an industry-to-school pipeline for part-time instructors.

Elevate and scale apprenticeship models.

Create a leadership structure for coordinating federal cybersecurity workforce activities.

Improve equitable access to broadband Internet services for all communities.

Expand pay flexibility for all federal departments and agencies.

Increase funding for CyberCorps: Scholarship for Service to expand its focus.

Public Core Resilience

Designate the commercial space sector as critical infrastructure.

Publish a national strategy to secure the public core.

Create a new cyberspace office within the U.S. State Department.

▶ Action Steps at a Glance

Supply Chain Security

Promote security transparency.

Publish a national industrial base strategy to maximize competition and innovation.

Promote financial support for free and open source software.

Measuring Cybersecurity

Establish a Bureau of Cyber Statistics.

Assess the cost-effectiveness of cybersecurity frameworks and risk analysis tools.

Improve state and local law enforcement's ability to report cybercrime incidents.

Establish a cross-sector partnership on modeling cybersecurity risk.

Operational Collaboration

Establish a National Cyber Director (NCD) to enhance public-private operational collaboration for proactive disruption and cyber event response.

Update federal law enforcement employee incentives to reward disruption of adversary operations.

Create a personnel exchange program between companies and federal agencies.

Direct and publish a review of legal barriers to deeper intelligence and operational coordination between federal agencies and private companies.

Create a framework to measure the outcomes of disruption and event response activities.

Education and Workforce Development

Diversity, equity, and inclusion in cybersecurity is a national security issue.

What is cybersecurity education and workforce development?

Efforts to educate and sustain the nation’s cybersecurity workforce can be divided into at least three overarching categories of activities:

- **Youth awareness**: Capturing the imagination and interest of a diverse array of students, many of whom will otherwise dismiss cybersecurity as a potential career pathway.
- **Education and skill development**: Working through schools, companies, governments, and intermediaries to guarantee equitable access to the financing and resources needed to transform interest into relevant knowledge, skills, and abilities for cybersecurity roles.
- **Employer engagement**: Changing how companies and government agencies recruit, hire, train, and retain cybersecurity workers to expand participation by underrepresented groups across all cybersecurity roles.

Why is this a priority?

People are the most important element in cybersecurity, and organizations are in desperate need of trained workers who can spend limited budgets wisely and use technology correctly. The past two administrations have described the nation’s cybersecurity workforce as a “strategic asset” that suffers from a persistent supply gap: employers in the United States alone report over 520,000 open cybersecurity roles. Driving this gap are (a) structural barriers to education and employment opportunities and (b) outdated hiring practices that disadvantage women and racial minorities, artificially restricting the pool of available cybersecurity talent.

Addressing these inequities is not only a moral and ethical imperative—it is an essential component of national security strategy. Our nation boasts enough citizens with the talent and passion to perform cybersecurity roles, and diversity, equity, and inclusion are not merely "nice to have." They are a core business objective. Without serious, consistent, and persistent recognition that representation is an inseparable part of the cybersecurity mission, government and industry will continue to leave untold talent on the table and a mature national risk posture will continue to elude us.

Unlike many other domains in cybersecurity policy, addressing the cybersecurity skills shortage is not just another budget item. Transforming how the nation approaches cybersecurity talent will reduce unemployment, bring high-skill jobs and wage-growth to geographically isolated communities, and fight systemic racism that excludes underrepresented groups from the technology workforce. Because of this, cybersecurity education and workforce initiatives have captured the imagination of countless state, local, and nonprofit leaders who are eager to scale past successes and achieve rapid progress.

Outcomes

- More filled cybersecurity positions in companies and government agencies.
- A cybersecurity workforce that reflects our nation's gender, ethnic, racial, geographic, and ideological diversity.

What have been the obstacles to progress?

- *Funding*: Limited funding for cybersecurity education in schools, upskilling for entry-level employees, and training programs for career-switchers means restricts opportunities for underrepresented groups to discover and enter the cybersecurity field.

- *Too little, too late*: Career awareness development targets young adults or high school students—far too late considering that many learners start narrowing their interests in middle school or even earlier.
- *Structural barriers*: Lack of qualified instructors in K-12 schools and higher education frustrates efforts to scale cybersecurity instruction. Most learning standards, assessments, and teacher certifications—all critical to shaping course design and directing limited resources—do not treat cybersecurity as even a minor component of education.
- *Narrow talent aperture*: Outdated recruitment and hiring practices artificially limit the talent pool with unnecessarily restrictive job qualifications and relying on off-putting or vague job descriptions that dissuade potential high performers.

Action Steps

1) **Appropriate new grant funding and direct grantmaking agencies to support organizations dedicated to growing the representation of underrepresented communities in the cybersecurity field.** Like the STEM field, the cybersecurity profession tends to discourage, exclude, or mistreat women and communities of color. Not only is this morally reprehensible—it also undermines cybersecurity as an objective matter. By excluding (even unintentionally) so many candidates from the talent pool, employers virtually guarantee that the industry will never fill its 500,000 open positions. A growing number of organizations have already established real-world programs to support underrepresented groups interested in cybersecurity. Grantmaking agencies such as the Department of Labor and the Department of Homeland Security should explore flexibility to direct existing grant funds toward nonprofit, industry, and academic partnerships with demonstrated success in improving diversity across the cybersecurity workforce, and

gress should appropriate new funds to support this new emphasis.

2) **Change how employers recruit cybersecurity workers to diversify and expand the talent pool.** A primary driver of the cybersecurity skills gap is the outdated recruitment practices by companies and agencies. Too many entry-level cybersecurity job openings list prerequisites that are more appropriate for more senior roles, demanding mid-career certifications or requiring applicants to have four-year degrees when less onerous, less expensive credentials suffice. Terminology alone can also discourage potential cybersecurity workers from applying to open positions. The result is a cybersecurity workforce ecosystem that imposes a disparate impact on underrepresented groups that undermines national security. The Principles for Growing and Sustaining the Nation's Cybersecurity Workforce offers actionable steps for employers who want to expand their talent aperture, and the Aspen Cybersecurity Group has assembled a voluntary coalition of over 30 companies that have publicly committed to instituting or strengthening practices to diversify their cybersecurity talent pool. Leveraging the authority of the White House, and convening bodies like the American Workforce Policy Advisory Board, and influential leadership organizations like the Business Roundtable, the next administration should build on the Aspen coalition to rapidly scale the number of employers—including federal agencies—who commit to reviewing and revising their hiring practices.

3) **Authorize and fund a national repository of K-12 cybersecurity resources.** Congress should direct and pass appropriations for the National Initiative for Cybersecurity Education to create and sustain a searchable, living repository of K-12 cybersecurity curricula and practical resources with a transparent classification system that is easy for non-experts to navigate. Such a repository should clearly indicate which curricula

are aligned with existing state education standards. This repository can also serve as a foundation for an Open Knowledge Network for the K-12 cybersecurity community.

4) **Create and scale an industry-to-school pipeline for part-time instructors.** Many experts working in industry are willing to volunteer their time and expertise to instruct students or help teachers apply curricula guides. Yet there is not a widely known, trustworthy mechanism for connecting volunteers with schools that need and are ready for such assistance. As a start, the White House and Congress should identify incentives for companies with deep benches of technical experts to launch initiatives that pair volunteer computer science experts with schools to expand computer science course offerings, such as Microsoft's TEALS Program.

5) **Elevate and scale apprenticeship models. Cybersecurity apprenticeships offer an excellent avenue for growing a more diverse, skilled cybersecurity workforce.** More and more employers and educational partners are proving that cybersecurity apprenticeships improve opportunities for underrepresented groups and allow employers not only to train but also *retain* skilled workers. Stakeholders are primed to scale similar programs nationwide if the federal government—led by the Office of Apprenticeships at the Department of Labor—assumes a greater leadership role. A first step is pushing federal hiring managers to value apprenticeships, starting with an executive order establishing a task force to pilot a cybersecurity apprenticeship pathway for federal employees. More broadly, Congress should revive and prioritize proposed legislation to (a) create state-level apprenticeship hubs that build new programs in regions with high demand for cybersecurity skills and (b) convert state apprenticeship expansion grants to formal block grants. Finally, workforce development champions must fight an emerging partisan split over registered apprenticeships versus industry-recognized apprentice-

ship programs (IRAP). Both models are important pieces to the overall mission of aligning employer needs with equitable worker access to high-quality job opportunities.

6) **Create a leadership structure for coordinating federal cybersecurity workforce activities.** A coherent planning and implementation structure is essential to avoid duplication of work and inoculate workforce efforts—for which success depends on steady, long-term commitments—against political and leadership changes. As recommended by the U.S. Cyberspace Solarium Commission, the White House should establish an interagency leadership structure centered on building:

   a) A high-level steering committee comprising the key agencies involved in cybersecurity workforce development (OMB, OPM, CISA, NIST/NICE, NSA, DOD) that creates a unified federal vision for these activities and apportion resources.

   b) A staff-level working group available to all federal offices to implement guidance from the steering committee.

7) **Improve equitable access to broadband Internet services for all communities.** One advantage of cybersecurity roles is their ability to allow geographically isolated communities tap into high-skill job markets. But as the COVID-19 pandemic has made painfully obvious, many students and working adults (both rural and urban) do not have access to Internet speeds that are necessary to either take advantage of online cybersecurity education or perform cybersecurity roles remotely. The Coronavirus Aid, Relief, and Economic Security Act enacted in early 2020 allows states to use federal relief funding to expand broadband connectivity access, and the White House and Congress should ensure that additional relief and recovery support includes similar authorization. In addition, recent innovation in satellite broadband offers new potential for overcoming the digital divide in low population areas, and the

White House and Federal Communications Commission should encourage robust competition in this sector to lower costs and improve service delivery.

8) **Create pay flexibility for all federal departments and agencies.** Many talented cybersecurity experts who might otherwise work in federal service choose private employment because (a) the federal hiring process, particularly for sensitive cybersecurity positions, lasts too long and (b) traditional federal pay scales cannot compete with private sector salaries. While cutting the time needed to conduct background checks for new employees has long been an elusive goal for reform-minded federal leaders, enabling more flexibility to incentivize cybersecurity experts to join the civil service is more immediately achievable. As the U.S. Cyberspace Solarium Commission has recommended, Congress should expand past changes in federal law that provide the Department of Defense and Department of Homeland Security with more pay flexibility for cybersecurity experts to apply to all federal offices.

9) **Increase funding for CyberCorps to expand its focus.** One highly successful cybersecurity workforce initiative is CyberCorps: Scholarship for Service (SFS), which is jointly administered by OPM, DHS, and the NSF. CyberCorps aims to steer more students toward government service, offering interest-free financing to those who agree to work for a limited term in a federal, state, local, or tribal office after they graduate with a cybersecurity degree. However, federal law requires that at least 80% of CyberCorps participants must be placed in a federal agency, limiting the program's ability to strengthen the overall cybersecurity talent pool. While this reflects an understandable desire to focus federal funding on improving federal institutions, the restriction (a) misses an opportunity to build on the success of SFS to solve multiple problems at once and (b) reduces pressure on federal agencies to improve their own hiring systems to be competitive on their own merits.

Dig Deeper on Education and Workforce Development

Learn More

- Aspen Cybersecurity Group – Growing and Sustaining the Nation's Cybersecurity Workforce
- Cyberspace Solarium Commission – White Paper #3: Growing a Stronger federal Cyber Workforce
- New America – Teach Cybersecurity with Apprenticeship Instead
- Frost & Sullivan – Innovation Through Inclusion: The Multicultural Cybersecurity Workforce
- Cyber.org – Empowering Educators to Teach Cyber

Legislation, Regulations, Executive Orders, and Guidance

- NIST — NICE Cybersecurity Workforce Framework
- Executive Order — America's Cybersecurity Workforce
- Legislative Proposal from the Cyberspace Solarium Commission — Recruit, Develop, and Retain a Stronger Federal Cyber Workforce (Page 29)

Securing the Internet's Public Core

Global leadership requires protecting the foundation of the Internet.

What is the public core?

Most individuals and organizations interact with the Internet through personal computers, mobile devices, servers, and software applications. These are the technologies that users touch, feel, purchase, and control. As a result, cybersecurity companies and policymakers tend to invest the majority of their time and resources in protecting them. But all Internet services depend on a vast, global, interconnected foundation of hardware and software infrastructure—the public core—that most stakeholders take for granted. This bedrock operates below the surface of our digital lives, always in the background, and always out of sight.

Yet without this shared infrastructure, the Internet and the endless services it provides would cease to function. The public core comprises a combination of rules, processes, and technology systems that are responsible for:

- **Internet Addressing**: Determining who owns and controls which digital addresses, i.e., IP addresses.
- **Naming**: Translating IP addresses into domain names that humans can understand and communicate.
- **Routing**: Logically and physically transmitting data between a sender and the intended recipient.
- **Cabling**: Physical communications cables for transmitting data between networks.
- **Cryptography**: Allowing Internet users to exchange data securely without ever meeting in person.
- **Position, Navigation, and Timing (PNT)**: Providing precise timing and positioning data to digital systems.

▶ Securing the Internet’s Public Core

Why is this a priority?

Most elements of the public core were originally developed long ago without robust security features. By the time their designers recognized their central importance to the Internet and the global economy, it was too late to replace them with more secure alternatives. Security improvements instead relied on partial modifications that have left many critical vulnerabilities unaddressed.

The situation is unacceptable. Because any of the organization or services that use the Internet depends on the same elements of the public core, these shared vulnerabilities affect all Internet users. The clear risks for Internet resilience prompted the Global Commission on the Stability of Cyberspace in 2018 to propose a universal norm that “state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.” Little has changed since then, and the corruption, manipulation, and disruption of the public core continues to present a systemic threat to the global Internet and, therefore, the economic and social stability of the United States and its allies and partners.

Outcomes

- Increased security, reliability, and resilience for the public core.
- Defined roles and responsibilities for federal agencies vis-à-vis the public core.
- U.S. leadership in international dialogue to secure and modernize the public core.

What have been the obstacles to progress?

- *No one in charge*: There is no single organization responsible for protecting the public core. Efforts to improve its security and stability depend on global coordination between a variety of stakeholders, some with opposing interests. Further, different groups control different parts of the public core, making coordination more difficult.
- *Privately-owned commons* – The public core is generally managed by private companies and international nonprofits. Government agencies play a marginal role in managing or overseeing the public core, leading many to dismiss the role of federal policy in securing the public core.
- *No first-mover advantage*: The Internet generates network effects that create a strong disincentive to be the first organization to adopt a new standard or protocol that might enhance security for some element of the public core. Yet adoption is only effective if many or all organizations participate as well.

Action Steps

1) **Designate the commercial space sector as critical infrastructure.** Space satellites and their command and control networks are an overlooked and increasingly important part of the public core. More and more critical services depend on timing information transmitted by GPS satellites or Earth observation data, and important Internet communications transit orbiting infrastructure, with the global 5G networks being built now. Space Policy Directive-5 articulates the federal government's interest in promoting cybersecurity best practices in the space sector. Operationalizing SPD-5 should include concerted efforts to (a) persuade all space companies—from large Original Equipment Manufacturers to new startups—to implement reasonable cybersecurity practices and (b) facili-

itate government and industry assistance to accelerate implementation.

To that end, designating the commercial space sector as critical infrastructure will facilitate prioritization of limited government resources, grow personal relationships between industry operators and policymakers, and help overcome obstacles to interagency coordination. This could be accomplished either by (a) amending federal law to expressly name space as a critical infrastructure sector or (b) designating space infrastructure as a subsector of an existing sector, following the precedent of election infrastructure in 2017. This designation would not create any new regulatory authority or impose any mandatory burdens on commercial space companies.

2) **Publish a national strategy to secure the public core.** While threats to the public core imperil national security, the federal role in protecting this infrastructure should be limited as it is fundamentally a private and nonprofit ecosystem. But federal agencies can assist public core stakeholders in important ways. NIST is managing a competition to select new cryptographic protocols that can withstand potential attacks from quantum computers. The Department of Homeland Security is leading an effort to define and enhance PNT resiliency. The National Security Agency has published guidance suggesting methods for network operators and users to mitigate vulnerabilities in the Internet routing system, while the U.S. Cyberspace Solarium Commission has recommended that DHS and the NTIA do the same for the Domain Name System (naming) and the Border Gateway Protocol (routing). These and other programs should be combined into a single interagency strategy that communicates the compelling reason to protect the public core and outlines a clear path toward resiliency. It should also identify incentives and processes to speed the adoption of security practices. While a strategy document might strike some as unambitious, it is the most helpful first

first step for at least two reasons. These are outlined below. impose any mandatory burdens on commercial space companies.

a) **Awareness.** Many potential corporate and institutional victims of attacks on public core infrastructure are simply unaware of how the compromise of systems like the Domain Name System, the Border Gateway Protocol, and Global Positioning System can affect their core business interests. Similarly, they do not recognize their potential to promote a more secure public core by coalescing and requesting as a unified customer base that responsible stakeholders take certain steps. Many of the largest barriers to a more resilient public core are not technical, but rather organizational. Better security is a matter of prioritization and leadership from the right entities. A highly visible, coherent strategy will facilitate more serious and focused discussions with the right decision makers in industry.

b) **International leadership.** Because the public core spans the globe, its resilience depends on transnational coordination. This is especially important in the case of reinforcing norms—such as those outlined by Global Commission on Stability in Cyberspace or pursued through the United Nations Group of Governmental Experts—and in circumstances where some governments might decide to institute new guidelines or standards related to the public core specifically. A coherent strategy will clearly and consistently communicate American priorities for public core resiliency and ensure they are integrated with current efforts to strengthen norms. In addition, aside from international standards, successful efforts to secure the public core will depend on international coalitions of industry stakeholders, from software developers to network operators, that can coordinate operational security practices. A public core strategy should also outline new transnational, public-private processes for securing elements of the public core that fall outside of the scope of today's Internet governance regimes.

3) **Restore federal capacity for international engagement by creating a new cyberspace office within the Department of State led by an Assistant Secretary.** In recent years, the United States has withdrawn from international fora and partnerships that aim to agree on norms and standards for creating a resilient public core. Restoring (and in some cases, creating for the first time) American leadership on public core security demands a dedicated office backed by a senior political appointee who can become an expert on the issues and defend public core priorities during interagency negotiations. Per the U.S. Cyberspace Solarium Commission, Congress should create a "Bureau of Cyberspace Security and Emerging Technologies" to lead these efforts and "ensure the coherence of U.S. efforts abroad and ensure the alignment of these efforts with U.S. national strategy."

Dig Deeper on Securing the Internet's Public Core

Learn More

- Atlantic Council – The Politics of Internet Security
- NATO – Strategic Importance of, and Dependence On, Undersea Cables
- Harvard Belfer Center – Too Connected to Fail

Legislation, Regulations, Executive Orders, and Guidance

- Executive Order – Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services

▶ Securing the Internet's Public Core

- NIST – Draft Profile for the Responsible Use of PNT Services
- Legislation – Strategy to Secure Foundational Internet Protocols and E-Mail
- Cyberspace Solarium Commission Legislative Proposal – Create a Cyber Bureau and Assistant Secretary at the U.S. Department of State (Page 48)

Supply Chain Security

More choice leads to lower risk.

What is supply chain security?

A supply chain is the beginning-to-end process of designing, making, selling, and using a product. It is rare for one business to control the entire cycle, and most technology companies rely on many different suppliers spread across the globe. One organization mines raw materials. Another turns them into parts. Several others assemble the parts into larger building blocks, and the final goods assembler manufactures the product before distributing it. While software does not require physical shipping, it has its own supply chains, with software engineers across multiple countries developing applications with code from a wide variety of public or proprietary sources.

As these technology supply chains have become more complex, it has become increasingly difficult for individuals, organizations, and nations to understand and manage the associated risks. How can a power plant operator be confident that a safety sensor manufactured abroad has not been tampered with? How does a government agency ensure its new teleworking platform will not provide a backdoor for foreign intelligence agencies? How should an entire industry plan for the possibility of losing access to a rare element sourced from one country? Supply chain security aims to provide answers to these types of questions.

Why is this a priority?

Globalized technology supply chains have left the United States, its allies and partners, and critical industry sectors dependent on hardware and software components that could contain security vulnerabilities because of substandard design or malicious compromise. These vulnerabilities are especially serious because they can be difficult to detect and extremely costly to remedy once discovered, particularly when they are embedded in installed hardware that has a long lifecycle, which is a common scenario in critical infrastructure. And because supply chain components can constitute single points of failure, a security compromise in a widely used component could allow adversaries to launch devastating attacks with far-reaching impacts. In addition, overreliance on technologies produced or controlled by a small number of entities raises the specter of sudden restrictions that could cripple critical agencies or sectors.

While industry and government might diverge on specific methods for achieving supply chain security, most stakeholders agree on the goal: reliable and secure supply chains. Virtually all security practitioners and company managers want to reduce the degree of risk in their supply chains, which requires increased transparency, information, and choice.

Outcomes

- Robust competition in all markets that produce security-critical technology products and services.
- Increased information on and transparency of the components and security features of technology products and services, allowing businesses and agencies to better manage their supply chain risks.

What have been the obstacles to progress?

- *Business realities*: Companies and their executives need to generate—they are compelled by economic competitiveness and the fiduciary duty. As such, many firms select the lowest cost provider for components. This often compromises security to some degree, and many companies factor that additional risk into their decision making. At the same time, the *na-*

tional security risks of their decision—using lower cost options—are not necessarily apparent from available information. As a result, policymakers may frequently have trouble persuading some private companies to switch to alternative suppliers that the policymakers believe pose less of a risk to national security.

- *Lack of choice*: Companies who *might* be willing to pay more for less risky supply chain components run into another challenge. In many sectors, a few technology suppliers dominate the market for certain products and services, limiting the ability of companies to take their business elsewhere.
- *Reactive policy*: Supply chain security demands foresight. Companies need to anticipate changes to their industry years in advance to adjust their business and plan investments. For example, it was clear many years ago that 5G networking equipment would become a central element of critical infrastructure. Yet policymakers only recently began working with industry to improve market competition in this space.
- *The country-of-origin approach*: National security concerns relating to supply chains sourced from specific countries are unlikely to persuade multinational, profit-minded businesses to upend their technology supply chains. Country-agnostic risk management strategies are more likely to appeal to CEOs and their board members.

Action Steps

We propose that the next administration and Congress advance supply chain security through two interrelated lines of effort:

- **Market competition**: Expand market competition in critical technology sectors to maximize access to products and services that meet acceptable security standards and can be sourced from trustworthy suppliers.

- **Organizational risk management**: Promote practices that can minimize the risk posed by threats (known or unknown) and vulnerabilities introduced via hardware, software, and technology suppliers, whether they are trustworthy or not.

Our aim is to generate a virtuous cycle of market incentives. Robust market competition incentivizes suppliers to meet customer demands for more secure technology. This in turn strengthens organizational risk management by creating a marketplace of trustworthy suppliers.

Of course, even the most secure, vetted technology system presents some security risk. Adversaries will always seek to exploit vulnerabilities and compromise supply chain integrity. Guaranteeing affordable access to trusted suppliers does not reduce the importance of defense-in-depth and risk mitigation strategies. Thus, promoting organizational risk management among critical companies and agencies must always remain a central concern for supply chain security.

1) **Promote security transparency.** Organizational risk management benefits from transparency on how products and services are designed, implemented, and managed over time. Consumers, security practitioners, and procurement professionals need information on coding practices and the security features of hardware and software products. Some ongoing initiatives offer a solid foundation for encouraging more transparency among technology manufacturers and software developers:

    a) **Device labeling.** As the Internet of Things (IoT) continues to expand, insecure IoT devices are becoming integrated into home, small business, and larger enterprise networks.

Many of these products fail to adhere to consensus security standards, such as the Aspen Cybersecurity Group's IoT Security First Principles or more detailed guidelines like the NIST IoT Device Cybersecurity Capability Core Baseline and the C2 Consensus on IoT Device Security Baseline Capabilities.

For years, observers have floated the development of a security labeling regime akin to the "Energy Star" label for efficient home appliances. The idea is to give security-conscious customers enough information to base at least part of their purchasing decision on cybersecurity risk, while creating demand for better security among customers who never think about it. This will in turn create market pressures for IoT manufacturers to adhere to best security practices. Researchers at Carnegie Mellon University have developed a prototype label design, and the Food and Drug Administration has issued draft guidance for medical device manufacturers with recommendations regarding labeling.

Some doubt the value of IoT security labeling, questioning if labels that simple enough to understand might mislead users and create a false sense of security. Some research indicates otherwise, and Finland, Singapore, and the United Kingdom are all rolling out their own labeling regimes. The European Union's cybersecurity agency also has plans to develop IoT security certifications following a new landmark law in 2019. The time is ripe for the White House and Congress to assemble a handful of willing IoT manufactures to pilot real-world IoT security and privacy labels. This pilot will allow researchers to test the real-world effects of labels and zero in on standardized labeling criteria.

b) **Tools for managing risk of third-party software components.** Many modern software products are a mishmash of smaller, third-party components that are created by a wide range of software developers. In most cases, it is extremely difficult for purchasers to know exactly what these components are and what vulnerabilities they might contain. Even for knowledgeable users and security practitioners, a lack of transparency makes managing risk challenging. The development and implementation of best practices, both for transparency and risk management, can support organizations as they integrate and leverage third-party components and software. Through an open, multi-stakeholder process, the National Telecommunications and Information Administration (NTIA) is developing the technical and operational practices for software developers to communicate the "ingredient list" of their software products, known as a Software Bill of Materials–a potentially helpful tool, albeit one with limitations. In addition, the Software Assurance Forum for Excellence in Code (SAFECode) has detailed recommendations for a lifecycle approach to managing security risks inherent in third-party software components.

2) **Create critical technology testing centers.** Per a recommendation by the U.S. Cyberspace Solarium Commission, Congress should authorize federal agencies to designate, and provide appropriations for, three independent research organizations to evaluate and test the security of critical technologies in networking, industrial control systems, and open source software. As appropriate and lawful, the results of such tests should be published to inform industry supply chain management decisions, similar to the kinds of research products published by the United Kingdom's Huawei Cyber Security Evaluation Centre.

3) **Publish a national industrial base strategy to maximize competition and innovation.** Efforts to promote market competition in security-critical technology markets will require a proactive, whole-of-government approach that reflects the

need for more active government participation while explicitly rejecting the kind of aggressive, nationalist market interventions practiced by other countries. The first step is a joint government-industry strategy "to ensure more trusted supply chains and the availability of critical information and communications technologies," a key recommendation of the Cyberspace Solarium Commission.

At a minimum, such a strategy should:

a) Identify critical technology dependencies now and in the foreseeable future;

b) Analyze where present and future market concentration could undermine the reliability or security of critical technology components;

c) Articulate how current statutory and presidential authorities support specific programs for promoting market competition in those sectors to reduce market concentration;

d) Specify statutory or regulatory changes necessary to promote such market competition;

e) Consider both immediate and long-term impacts of potential actions on the competitiveness and R&D capabilities of U.S. and allied industries; and

f) Outline objectives for generating a consensus with allies and partners on ensuring long-term, sustainable competition in critical technology markets.

Notably, this strategy should not seek to identify and strengthen "national champions"—individual companies that receive special, targeted federal assistance or regulatory relief. The stated purpose of this strategy should not be to ensure that only U.S.-based firms dominate every critical technology market worldwide. This could lead allies and industry partners overseas to conflate supply chain security with trade disputes, which turn on politics, not risk-based security analysis. The goal of an industrial strategy for supply chain security is to promote market competition and innovation to increase the availability of trustworthy technology suppliers, some of whom will have overseas headquarters in Europe or elsewhere. Yet this approach will clearly benefit American workers for the simple reason that competition and innovation are chief comparative advantages of American industry.

Promote financial support for free and open source software. The digital economy is built on a foundation of free and open source software (FOSS). Countless companies depend on FOSS tools, libraries and applications to conduct critical business functions. Yet despite its central importance, FOSS code is often supported by volunteers who work without any dedicated budget and struggle to ensure its security. This presents serious risks for the digital economy. In 2014, after experts discovered a potentially disastrous security flaw called Heartbleed in an open source encryption tool used globally, one open source expert remarked, “[The] mystery is not that a few overworked volunteers missed this bug; the mystery is why it hasn’t happened more often.” Addressing this resource gap requires that executives in all major industries (not just the tech sector) recognize their dependence on FOSS and commit to supporting the nonprofits that develop and maintain it. The Open Source Security Foundation (OpenSSF) is a new effort to promote collaboration between industry leaders interested in investing in open source security. The federal government should facilitate progress by encouraging more companies to join OpenSSF and directing more federal funding toward research on and the operational management of more secure open source infrastructure.

Foundations and other philanthropic organizations are a destination for such funding, but in the early 2010s, the Internal Revenue Service began applying more scrutiny when granting 501(c)(3) status to organizations focused on open source development. This has generated a perception across the tech community that open source nonprofits might struggle to obtain tax-exempt status. In 2017, researchers with the Berkman Klein Center at Harvard observed that "501(c)(3) status appears harder to obtain than ever for open source software organizations." This is a key barrier to the secure and responsible management of the nation's open source digital infrastructure, and IRS leadership should publicly clarify the rationale, if any, behind applying additional scrutiny to open source software nonprofit applications, as well as issue guidance to assist applicants in expediting the process.

Dig Deeper on Supply Chain Security

Learn More

- Cyberspace Solarium Commission – White Paper #4: Building a Trusted ICT Supply Chain
- Ford Foundation – Roads and Bridges: The Unseen Labor Behind our Digital Infrastructure
- National Telecommunications and Information Administration – Introduction to Software Bill of Materials

Legislation, Regulations, Executive Orders, and Guidance

- Proposed Regulation – Securing the Information and Communications Technology and Services Supply Chain and Business Roundtable Comments
- Executive Order – Securing the Information and Communications Technology and Services Supply Chain
- Executive Order – Securing the United States Bulk-Power System

▶ Supply Chain Security

- Executive Order – Executive Order on Addressing the Threat to the Domestic Supply Chain from Reliance on Critical Minerals from Foreign Adversaries
- Legislation – MICROCHIPS Act of 2019
- Legislation – Secure 5G and Beyond Act of 2020
- Legislation – Cyber Supply Chain Management and Transparency Act of 2014
- Cyberspace Solarium Commission Legislative Proposal – Designate Critical Technology Security Centers (Page 114)

Measuring Cybersecurity

We can't solve problems if we don't know what works and what doesn't.

What is cybersecurity measurement?

Cybersecurity measurement comprises at least two distinct activities:

- **National and sector data collection**: Collecting and analyzing high-level data that allows policymakers to assess where to direct limited resources and how to shape risk management practices (e.g., recording how many hospitals were hit by ransomware in the past year, and how many of those hospitals had dedicated cybersecurity staff).
- **Cybersecurity metrics**: Creating a taxonomy as well as tools that allow organizations to assess their own compliance with cybersecurity standards and their return-on-investment for measures taken (e.g., determining whether a company's cybersecurity program meaningfully reduces risk).

Why is this a priority?

Evidence-based cybersecurity policy requires a fact-based picture of the nature and scope of malicious activities across the economy and the ability to assess whether policy changes reduce their impact. Today, the federal government lacks the most basic, reliable data on (a) the frequency and severity of cyberattacks across all sectors, including government and private industry; (b) the most common security failures that lead to attacks; and (c) the technical, procedural, and administrative steps that thwart attacks most often. This means policymakers cannot make evidence-based decisions on how to either allocate limited resources or incentivize government agencies and private industry to better manage risk. Nor can they engage in systemic risk analysis—the key to proper national-level cybersecurity strategy. Without better data, policymakers might as well be grasping at straws.

Outcomes

- A standardized terminology, definition, and ontology framework for cybersecurity measurement.
- Evidence-based federal strategy and policy to support state, local, tribal, and territorial (SLTT) entities and the private sector.
- Higher quality risk modeling to support more accurate insurance pricing.

What have been the obstacles to progress?

- *No denominator*: Without knowing the total volume of malicious activity, it is very difficult to assess the impact of specific policies, controls, or actions.
- *Lack of incentives*: High-quality data on cybersecurity incidents and the effectiveness of defense measures is often proprietary, and companies may not share it unless doing so provides a competitive edge to either their security products and services or their organizational risk management capabilities.
- *Liability*: Organizations that are victims of cybersecurity incidents are often reluctant to share security incidents with the public except where legally required, fearing that transparency might expose them to embarrassment or lawsuits.
- *Overly narrow focus*: Many cybersecurity policy discussions tend to revolve around discrete software vulnerabilities and data breaches, instead of the risk management practices and resiliency measures that depend on better metrics (e.g., the average time it takes to restore functionality *after* a breach.

Action Steps

1) **Establish a Bureau of Cyber Statistics.** The U.S. Cyberspace Solarium Commission has recommended "Congress should establish a Bureau of Cyber Statistics charged with collecting and providing statistical data on cybersecurity and the cyber ecosystem to inform policymaking and government programs." Indeed, a dedicated data collection office is necessary to build a more accurate, ground-truth picture of cybersecurity. While codifying a Bureau of Cyber Statistics could take years, the White House can kickstart the effort and demonstrate its potential value by merging established data collection efforts, such as the Internet Crime Complaint Center, National Incident Based Reporting System (NIBRS), and the FTC Consumer Sentinel Network. In addition, any centralized federal office set up to gather cybersecurity statistics should adhere to at least three principles in its early days:

   a) **Data first, metrics later.** Developing and deriving value from cybersecurity metrics has vexed the cybersecurity community for years, and private sector entities have clear incentives to identify and test metrics on their own, without any Bureau of Cyber Statistics. Addressing the gap in nation- and sector-level data presents a less technical challenge, and will yield real and more rapid benefits for the policymaking process. Such data will help policymakers address even the most basic but essential questions such as, "How many companies act on threat data provided by federal agencies?" It will also help to answer the more technical ones, such as "How many route hijacks affecting U.S.-based organizations occur every year?"

   b) **Government first, industry later.** A common sticking point in many cybersecurity discussions arises when the federal government requests that private companies implement steps that should apply equally to federal agencies but that federal agencies have yet to adopt. The area of data collection and metrics presents an excellent opportunity for the federal government to take a leadership role and demonstrate tangible progress. Unlike efforts to gather information on the private sector or state and local government, federal leaders are already empowered and well-equipped to gather relevant data on cybersecurity incidents and defensive measures across the federal government.

c) **Voluntary, not mandatory.** Once the Bureau of Cyber Statistics has collected useful data from all relevant federal offices, it can begin the vital (but often overlooked) phase of demonstrating that data collection generates useful insights. Armed with a convincing case that data collection is not a pointless exercise, the Bureau should persuade (a) state, local, territorial, and tribal entities and (b) critical infrastructure owners and operators to begin providing narrow sets of data voluntarily. Mandatory data collection would be practically unenforceable and would likely poison the Bureau's relationships with its most important partners. Dedication to voluntary partnerships with non-federal entities is how the Bureau will stay nimble, rapidly iterate its data requests based on honest feedback, and maximize its value-add.

2) **Assess the cost-effectiveness of cybersecurity frameworks.** A common critique of government cybersecurity regulation is that it incentivizes "box-checking" that oversimplifies the fast-moving dynamics of real-world cyber defense. The federal government uses a wide range of frameworks to guide implementation of cybersecurity controls for agencies and private companies, but it remains unclear how cost-effective these frameworks are in reducing risk. Have agencies or companies that use the NIST Cybersecurity Framework to implement cybersecurity programs met their risk reduction

goals at lower cost than those who rely on other methodologies? Do organization that supplement frameworks with risk analysis tools like Factor of Analysis Information Risk experience better outcomes? No overarching study has answered these questions, and the federal government is well-positioned to lead one. While assessing the comparative cost -effectiveness of frameworks and risk analysis tools would fit the mission of the Bureau of Cyber Statistics, the National Institute for Standards of Technology should prioritize engaging with willing industry stakeholders to answer these questions even before the Bureau is established.

3) **Improve state and local law enforcement's ability to report cybercrime incidents.** A successful Bureau of Cyber Statistics will need capable partners in SLTT governments who have the capacity to record and communicate relevant data. In A Roadmap to Strengthen US Cyber Enforcement, Third Way found that only half of the 18,000 state and local law enforcement agencies in the United States report data to the NIBRS, the primary federal program that collects crime data. This database also faces problems with how agencies log incidents of cybercrime, leading to vast undercounts. The next administration should closely examine how to improve cybercrime reporting processes and incentives nationwide.

4) **Establish a cross-sector partnership on modeling cyber risk.** Cybersecurity insurance is a nascent tool for private and public organizations that want to spread the risk and costs of cyber incidents, but the industry lacks sufficient data on cybersecurity incidents to inform its actuarial models and has yet to establish a uniform process for pricing insurance for cybersecurity risks. Many of the data sets available to insurance actuaries (including those collected directly from their customers) do not allow them to either account for the full range of cybersecurity risks that exist or develop the quantitative tools common to other insurance contexts. As the U.S. Cyber-

space Solarium Commission has recommended, DHS should establish a public-private working group that convenes insurance companies and cyber risk modeling firms to explore avenues for purchasing and/or combining proprietary data that can support more rigorous methodologies for cyber insurance pricing.

Dig Deeper on Measuring Cybersecurity

Learn More

- Lawfare – Considerations for the Structure of the Bureau of Cyber Statistics
- Federal News Network – Reinvigorating CyberStat in Fiscal 2021
- OMB – Federal Cybersecurity Risk Determination Report and Action Plan
- NIST – Measurements for Information Security

Legislation, Regulations, Executive Orders, and Guidance

- Legislative Proposal — Establish a Bureau of Cyber Statistics (Page 120)

Promoting Operational Collaboration

The government does not control cyberspace. The road to success runs through the boardroom.

What is operational collaboration?

Operational collaboration is the process by which multiple organizations coordinate planning and synchronize their actions to achieve a shared goal in cyberspace using lawful methods. Typically, that shared goal is proactive: disrupting adversaries or threat actors before they cause unacceptable harm. In some cases, the goal is to respond to a significant cyber event, mitigate the consequences, and facilitate recovery operations. Whether dealing with proactive disruption operations or jointly orchestrated crisis response, operational collaboration combines legal, economic, law enforcement, intelligence, and/or technical measures employed by the private sector and government agencies.

Operational collaboration takes several different forms. It can involve coordination between companies and federal agencies, such as a recent FBI collaboration with private sector companies, or business-to-business coordination to disrupt adversary capabilities or disable adversary infrastructure. It can involve highly-capable security companies, internet service providers, information sharing organizations, and platform providers—all working together to mitigate the effects of an ongoing significant cyber incident. In both cases, success requires a clearly defined objective and mutually agreed outcomes, enabling participants to align interests and focus on the same adversary. It must also clearly provide mutual benefit to all stakeholders involved (e.g., a company protects its customers and law enforcement obtains intelligence or an indictment).

What operational collaboration does *not* mean: (a) hacking back, (b) mandating industry cooperation with government cybersecurity programs, or (c) responding to routine cyber incidents on a regular basis.

Why is this a priority?

Operational collaboration aims to achieve two fundamental objectives in cybersecurity policy: (a) increase costs for adversaries by disrupting their activities and (b) prepare for and respond to adverse cyber events that harm U.S. or allied interests. Because neither the government nor the private sector acting alone can achieve the scale, scope, speed, and sustainability required to achieve these goals, the only way to reach the desired end-state is to enable more effective operational collaboration across the digital ecosystem.

The increasing costs of malicious cyber activities demonstrates that current processes and structure are insufficient to safeguard national security, economic prosperity, and public health and safety. Numerous adversaries, whether nation-states or cybercriminals, can attack consumers, businesses, and government agencies with relative impunity. For many types of attacks, adversaries' direct costs also remain relatively low, allowing them to achieve greater scale and damage. Simply sharing information about threats is not enough. We need to increase costs for adversaries. Too often, our efforts to shut down adversary networks only impose minor setbacks that still allow them to pivot and quickly recover operations. Industry and government must work together to turn these into strategic defeats that force adversaries to invest in entirely new attack campaigns.

Notwithstanding proactive efforts to disrupt these malicious activities, sometimes adversaries will succeed in conducting a major attack. As the impact of cybersecurity events increases, we need to respond to significant cybersecurity events (such as the NotPetya outbreak) more effectively when they occur, limiting their spread and mitigating their effects. Because a major cybersecurity crisis will likely spread across multiple businesses, sectors, and regions, the corresponding response will require a high degree of coordination and rapid communication. And unlike proactive disruption planning, when stakeholders can wait until the right moment to strike, actively responding to a significant cybersecurity incident introduces the additional element of extreme time pressure.

Outcomes

- Reduced impact of routine cybercrime on the digital economy.
- Higher costs for sophisticated nation-state attackers.
- Increased number of high-capability companies and nations involved in cybersecurity coalitions.
- Better measurement of the effectiveness of adversary disruption operations.

What are past obstacles to progress?

- *No defined framework*: In many cases, federal agencies and potential partners in the private sector lack the policies, processes, procedures, and organizational structures to prioritize and enable effective operational collaboration, either proactively or reactively. Although the federal government has Presidential Policy Directive-14 for coordinating event response actions between agencies, how those agencies will work with private sector entities is not clear.
- *Lack of intra- and interagency leadership*: Individual agencies or offices simultaneously and separately ask to coordinate with private entities, frustrating a holistic government response and the scalability of public-private partnerships and joint actions.
- *Lack of prioritization and focus on impact*: Given the sizeable and growing number of highly sophisticated cyber adver-

saries, defenders lack the resources to capitalize on all opportunities to disrupt attacks. Without prioritization based on potential impact, operational collaboration is often opportunistic, simply gravitating toward threats that are most relevant to an ongoing investigation or customer segment.

- *Classification barriers*: Government participants are often unable or unwilling to share information in an unclassified setting and in a manner that allows private entities to act.
- *Agility*: Many efforts to improve coordination among the private sector and government mistakenly include too many parties, creating unwieldy processes while saddling coalitions with some partners who lack the technical capabilities to implement necessary activities.
- *Cultural barriers*: Many federal officials are uncomfortable engaging regularly and openly with the private sector, and some agency incentive structures almost exclusively reward law enforcement officers based on criminal justice outcomes, which sets a very high bar, reducing incentives to engage in otherwise effective disruption activities.
- *The "agent" problem*: Many companies might want closer collaboration with federal agencies in the name of better cybersecurity for their customers, but they are wary of being seen as agents of the U.S. government.
- *Liability*: Particularly when unknown dependencies or connections are involved, entities hesitate to act in concert if the potential second- or third-order consequences might cause unforeseen damage affecting other parties.
- *Antitrust*: While Congress has exempted narrow kinds of information sharing from antitrust rules, some coordinated activities could raise similar concerns.

Action Steps

1) **Establish a National Cyber Director to enhance public-private operational collaboration for proactive disruption and cyber event response.** The U.S. Cyberspace Solarium Commission has recommended that Congress codify a Senate-confirmed National Cyber Director (NCD) as "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." To be an effective advocate for and enabler of operational collaboration, the NCD should have both visibility into offensive government operations against adversaries and authority to coordinate public-private response activities to cyber events. The NCD can set common protection or disruption priorities and objectives; identify new ways to act in a unified, holistic manner to achieve those objectives; and help to scale coordination with the private sector by acting as a single point of contact, rather than requiring each agency to maintain their own direct connections to industry teams. The NCD should look to work by the Aspen Cybersecurity Group, Third Way, the World Economic Forum's Partnership against Cybercrime, and Columbia University's New York Cyber Task Force to develop the practical policies, processes, and structures to promote operational collaboration, both for proactive disruption and significant incident response.

2) **Update incentives for federal law enforcement employees to reward disruption of adversary operations.** The FBI and other law enforcement agencies are important partners for private entities that are interested in taking proactive steps to disrupt adversary networks. However, current cultural barriers and institutional incentive structures, including rewards and opportunities for advancement, reflect a traditional focus on indictment and prosecution as a means of deterrence, limiting disruption frequency and impact. Due to attribution challeng-

es and the fact that many of the responsible individuals live overseas, indictment and prosecution are unusual outcomes. Moreover, attribution is often a lengthy process, during which threat actors can continue harming technology users and the economy. Finally, prevention and deterrence—two of the most important theories of criminal law—can be achieved without indictment or prosecution when operational collaboration produces effective disruption.

1)Changing the incentive structures for federal law enforcement agents will help align the objectives of cybersecurity defenders in the private sector with those of the agency that is authorized to act aggressively against cyber criminals and foreign adversaries. Incentive structures should shift in favor of disrupting adversary infrastructure and operations, recognizing the value that such actions have for minimizing harm and protecting technology users.

3) **Create a personnel exchange program between companies and federal agencies.** Better coordination requires strong personal relationships between staff-level operators and senior decisionmakers in companies and agencies. A two -way exchange program will forge long-term networks of trust that laws or regulations cannot. Potential models include the Center for Long-Term Cybersecurity's Workforce Incubator and the Information Technology Exchange Program. Key federal government departments and agencies, such as DHS, DOD, and the FBI, should strive to conduct joint cyber defense activities, including systemic risk identification and contingency planning should-to-shoulder with corporate cyber teams and operational industry collaboratives of critical infrastructure operators.

4) **Direct and publish a review of legal barriers to deeper intelligence and operational coordination between federal agencies and private companies.** Some legal concerns cit-

ed as barriers to operational collaboration do not necessarily reflect the reality of statutory or regulatory restrictions. Federal agencies raise concerns about taking coordinated action with a limited number of private sector participants, but experience demonstrates that only a few private sector actors are truly capable of acting and motivated to do so. Progress requires a comprehensive, authoritative opinion on the existing legal barriers to closer coordination among federal agencies and between industry and government. Where barriers are identified, including constitutional protections when "agent of the state" provisions are triggered, safe harbor protections for limited and targeted cybercrime reporting (such as those that exist for reporting related to child protection) should be explored.

5) **Create a framework for measuring the outcomes of disruption and event response activities.** While successful examples of operational collaboration have become more common, the absence of a clear methodology for assessing the true impact of disruption operations or investments in event response prevents government, the private sector, and independent researchers from recommending evidence-based improvements to strategy and policy. Building on ongoing research by Columbia University, the Department of Homeland Security should partner with appropriate Federally Funded Research and Development Centers and universities to fund the creation and maintenance of a database of disruption activities and research to uncover the most effective practices. This research should also include reviewing past event response actions to map participants and draw out lessons learned. The NCD should ensure the resulting framework for operational disruption and metrics is included in national plans and policies that inform future efforts to take disruptive action against attackers to deter incidents and to collaborate on event response.

Dig Deeper on Operational Collaboration

Learn More

- Aspen Cybersecurity Group – An Operational Collaboration Framework for Cybersecurity
- World Economic Forum – Partnership against Cybercrime
- Atlantic Council – Innovation on Cyber Collaboration: Leverage at Scale
- Carnegie Endowment – International Strategy to Better Protect the Financial System Against Cyber Threats (Page 93)
- Council to Secure the Digital Economy – International Botnet and IoT Security Guide 2020
- Chris Inglis – Statement Before the Senate Armed Services Committee

Legislation, Regulations, Executive Orders, and Guidance

- Legislation — Cyber Security Exchange Act
- Legislative Proposal — Codify Processes for Identifying Private Sector Cyber Intelligence Needs and Priorities (Page 204)
- Legislative Proposal — Create a Joint Cyber Planning Office (Page 228)
- Legislative Proposal — Institutionalize DoD Participation in Public-Private Cybersecurity Initiatives (Page 232)

Additional Priorities

Information Operations

By weaponizing social networks and digital media, a wide range of malicious governments, organizations, and individuals are actively undermining American society's shared understanding of evidence -based reality. Left unchecked, malign influence campaigns present a threat to modern democracy and national security. Foreign adversaries are leveraging these tactics as a purposeful, long-term strategy to paralyze and poison public life. Domestic groups and individuals use similar tactics to sow social division and advance unsubstantiated conspiracies. Even worse, innovation in fields such as artificial intelligence are allowing foreign and domestic actors to scale their efforts to infect public discourse with false narratives.

Given the stakes, many observers are clamoring for a more aggressive defense. For the federal government, confronting this challenge means resolving at least three problems. First, we must review, improve, and institutionalize tested processes and capabilities for disrupting *foreign* influence operations. Structures such as the FBI's Foreign Influence Task Force and CISA's Countering Foreign Influence Task Force provide a solid foundation for establishing long-term partnerships between relevant federal agencies and the private companies that supply the information ecosystem.

Second, the federal government must take the basic step of defining which information operations merit attention in the first place. When should we start to care about a specific information operation? How should we think about adversary campaigns, where seemingly unimportant, separate operations actually combine to achieve a serious impact? What threshold level of harm must be crossed to trigger action by federal authorities? How should we even measure the harm? A chief priority for the White House and Congress should be to select criteria for identifying the specific types of information operations that deserve federal scrutiny and potential intervention. This will be essential not only for targeting limited resources but also to start addressing the third, most difficult challenge.

While the First Amendment generally prohibits government restrictions on freedom of speech, our leaders today cannot ignore the pernicious epidemic of misinformation, disinformation, and violent extremist content produced and disseminated by domestic actors. Unlike the case of foreign-directed information operations, there is no obvious toolset for addressing domestic campaigns, which create effects that may be identical to those led by foreign governments. Any action is likely to be met with serious political repercussions. Enhancing public resilience to these false narratives is an incredibly hard problem, and it is not surprising that the most important stakeholders—social media companies, federal agencies, state or local governments, and education leaders—have yet to raise their hand and offer to lead the charge. This must change. Focusing on foreign influence as the sole source of information operations lets our nation off the hook, abdicating the soul-searching it needs to reexamine the responsibility of social media companies and government leaders in cultivating a healthy public discourse.

Dig Deeper

- First Draft News – Understanding and Addressing the Disinformation Ecosystem
- DHS – Combatting Targeted Disinformation Campaigns
- RAND Corporation – Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life

Algorithmic Bias and Cybersecurity

Algorithms, advanced behavioral analytics, and facial recognition technologies are increasingly becoming a part of everyday life. Banks, judges, and law enforcement agencies rely on computer code to make life-altering decisions on lending, sentencing, and criminal investigations. These systems are already causing disparate impacts that perpetuate discrimination against racial and ethnic minorities due to unintentional—but very real—biases in the underlying datasets. A recent study by NIST, for example, found that the majority of facial recognition algorithms it tested exhibited demographic differentials. Others have found strong evidence of racial discrimination in housing loan and criminal justice recidivism tools.

Even when used in good faith, these tools support critical and opaque decisions on behalf of vulnerable populations, including racial and ethnic minorities who have no opportunity to inform how these systems are created, and who are more likely to be harmed by their use. Yet cybersecurity risks allow attackers to manipulate algorithms and introduce deliberate bias, notwithstanding the good intentions of authorized users. Malicious actors may try and obtain the underlying data powering the algorithm, manipulate that data to affect the algorithm's calculus, or alter the algorithmic code itself. Without greater transparency into how algorithmic tools are developed and deployed, it will be difficult to show that decision outcomes are legitimate.

At a minimum, government and independent bodies should establish auditing standards for the private and public sectors to use as benchmarks before decision-making algorithms are deployed--particularly when they apply to racial and ethnic minorities and other vulnerable groups. Organizations that use them, from courts to schools, should also develop clear guides for assessing algorithms during procurement processes, borrowing lessons from the World

Economic Forum's AI Procurement Guide or the EdTech Equity Project's School Procurement Guide. In doing so, the public sector can establish a role in cultivating industry-wide standards.

Dig Deeper

Learn More

- NIST – Study Evaluates Effects of Race, Age, Sex on Face Recognition Software
- World Economic Forum – Guidelines for AI Procurement
- EdTech Equity – School Procurement Guide
- My Fair Data – How the Government Can Limit Bias in Artificial Intelligence
- Aspen Tech Policy Hub – Fair Algorithmic Housing Loans
- Aspen Tech Policy Hub – Pretrial Risk Assessment
- Aspen Tech Policy Hub – Florida Schools

Legislation, Regulation, Executive Orders, and Guidance

- Legislation – Algorithmic Accountability Act of 2019

State and Local Cybersecurity

SLTT governments are on the frontlines of cybersecurity. Since 2016, federal support for state and local leadership in cybersecurity has focused on election security. It is possible that in the wake of the 2020 election season, notable for the absence of known cases of malicious compromise in election infrastructure, members of Congress or state leaders might dismiss continued investment and planning in election security. This would be a mistake. Recent disinformation campaigns to delegitimize the electoral process only increase the risk that even isolated, limited security incidents could undermine public confidence in future results. The need to fund and, critically, professionalize all aspects of cybersecurity in the elections sector is greater than ever.

However, election security is only one slice of state and local cybersecurity. State and local homeland security officials, law enforcement, and National Guard units commonly provide the on-the-ground response for ransomware incidents. State and local regulatory commissions set rules and guidelines for energy distribution, water facilities, and insurance standards. And universities, community colleges, and K-12 institutions are the primary source of the nation's cybersecurity talent pool.

Many state and local officials are eager for closer partnerships with federal cybersecurity departments and agencies. They need assistance with developing statewide cybersecurity strategies, exercising response plans, scaling cybersecurity education, and partnering with industry. A principal obstacle to progress is a lack of dedicated personnel in federal and state offices to drive these priorities. Legislation to create a cybersecurity liaison for each state within DHS, if enacted and supported with sufficient funding, would supply a partial solution. Federal policymakers should also strongly encourage the governor of every state and territory to create and fund a dedicated, statewide cybersecurity coordinator, not merely designate a preexisting department head. Federal liaisons and state coordinators could form state-specific duos equipped to communicate state and local needs to federal policymakers, integrate federal capabilities into statewide cybersecurity plans, and standardize effective strategies nationwide.

Dig Deeper

Learn More

- NASCIO – Stronger Together: State and Local Cybersecurity
- Pitt Cyber, R Street, Brennan Center, German Marshall Fund – Defending Elections: Federal Funding Needs for State Election Security

Legislation, Regulations, Executive Orders, and Guidance

- Legislation – Cybersecurity State Coordinator Act of 2020
- Legislation – State and Local Government Cybersecurity Act of 2019

Federal Support for Basic Research

Foundational research is the bedrock of innovation. The National Science Foundation defines it as "activity aimed at acquiring new knowledge or understanding without specific immediate commercial application or use." It fosters discovery that informs and strengthens the application of new technologies down the road. The success of foundational research is neither immediately tangible nor guaranteed; it is by design an exploration of the unknown.

The case for government R&D funding—particularly foundational research—is simple: no one else will do it at scale. Foundational research frequently does not reward the original spender. Investing in technological innovation is risky, and long-term research often fails to yield profits. Our economic competitiveness relies on federal investment in foundational research that allows industry to direct its own research dollars into applied technologies where payoff is more likely.

Unfortunately, federal R&D funding—which encompasses foundational research—as a percentage of GDP has fallen steadily since the 1960s. Although industry R&D investment continues to rise, dwindling federal government investment is troubling. By contrast, China doubled its foundational research funding in the last five years and spent a record $254 billion on R&D in 2017, narrowing the gap between it and the United States in R&D spending. If the United States wants to lead the world in innovation, this must change. To start, Congress should ensure that federal agencies have the budget authority and appropriations to bring the federal government back to at least a 50% share of basic research nationwide. Authorizing language should be accompanied by statutory language that expressly embraces risk and encourages federal agencies to adopt a risk tolerant approach to awarding federal research grants.

Dig Deeper

Learn More

- Aspen Cybersecurity Group – An Innovation Challenge for the United States
- AAAS – Federal R&D Budget Trends: A Short Summary

Legislation, Regulations, Executive Orders, and Guidance

- Legislation – Resolution on Principles for a National Artificial Intelligence Strategy
- Legislation – Securing American Leadership in Science and Technology Act of 2020

Basic Cyber Hygiene

Many dimensions of cybersecurity strategy and policy would be unnecessary if most organizations implemented a relatively limited set of cybersecurity measures, including but not limited to those outlined in the CIS Critical Controls. Foundational cyber hygiene practices include deploying multifactor authentication, mandating regular software updates, enforcing least privilege access, inventorying devices and software, monitoring networks, recording security anomalies, exercising crisis response procedures, and backing up critical data.

For a variety of reasons, many of these relatively best practices are simply not employed by government organizations, companies, or individuals. Decision makers might not understand the risks. If they do, their hiring department might struggle to find skilled personnel to implement basic controls. Even equipped with the right people and resources, some organizations are incentivized to prioritize convenience and service delivery over more mature risk management that adds cost and time to projects. And without better data on where their peers stand and which cybersecurity measures provide the best return on investment, cybersecurity professionals may struggle to persuade leadership to prioritize their advice.

Many recommendations in this report speak to these challenges and offer pathways to drive more widespread adoption of cyber hygiene, particularly among larger, high-capability organizations. But cybersecurity policymakers must focus attention on driving foundational practices for all organizations and individuals, from small businesses to state agencies. Different stakeholders require appropriately tailored guidance and incentives. Across these communities, greater awareness of how to leverage existing and emerging technologies to help manage risk and outsource security maintenance is also essential to scaling an effective defense.

Dig Deeper on Basic Cyber Hygiene

Learn More

- Center for Internet Security – Top 20 Controls
- Carnegie Mellon University Software Engineering Institute – Cyber Hygiene: 11 Essential Practices and Mapping Cyber Hygiene to the NIST Cybersecurity Framework
- NIST National Cybersecurity Center of Excellence – Critical Cybersecurity Hygiene: Patching the Enterprise
- U.S. Government Accountability Office – DHS Directives Have Strengthened Federal Cybersecurity, but Improvements Are Needed

Legislation, Regulations, Executive Orders, and Guidance

- Legislation – Promoting Good Cyber Hygiene Act of 2017 (Senate) and Promoting Good Cyber Hygiene Act of 2017 (House)
- Regulation – Binding Operational Directive 19 – 02: Vulnerability Remediation Requirements for Internet-Accessible Systems
- Guidance – DHS Cyber Hygiene Services for government and critical infrastructure organizations

Individuals are encouraged to cite this report and its contents.

In doing so, please include the following attribution:

Aspen Cybersecurity Group. "A National Cybersecurity Agenda for Resilient Digital Infrastructure."
Washington, D.C. The Aspen Institute. December 2020.