HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

POLICY PAPER
belfercenter.org/homelandsecurity

HOMELAND SECURITY PROJECT | AUGUST 2021

Integration of Effort

Rethinking Cybersecurity for Critical Infrastructure

Sean Atkins and Chappell Lawson

Executive Summary

Because threats to critical infrastructure present a broad danger to society, there is a significant public interest in securing their continuity of operations against cyberattacks. However, because most critical infrastructure is owned by private firms, the government must engage with industry in order to secure them. Unfortunately, the current strategy of engagement is flawed, and the recommendations of the recent Cyber Solarium commission—though valuable—will not solve the problem. A new policy must deliver true integration of effort between the federal government and the relatively small number of systemically important firms. The specific form of this partnership must be tailored to the idiosyncrasies of critical infrastructure sectors.

Background

Cybersecurity and critical infrastructure. The U.S. currently defines critical infrastructure as "the systems and assets, whether physical or virtual, so vital . . . that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[1] In more colloquial terms, critical infrastructure consists of the systems that undergird modern society: the power grid that provides electricity to businesses and households, financial networks that allow the market economy to function, water and sewage systems, and the like. The federal government now recognizes sixteen critical infrastructure sectors (e.g. "transportation"), comprising nearly three dozen "subsectors" (e.g. "aviation"), as well as an overlapping set of "critical functions" (e.g. the "National Critical Function of Conducting Elections").[2]

Digitalization over the last three decades has left much of this critical infrastructure vulnerable to cyberattack. Furthermore, the growing introduction of software-based functions (with new associated supply-chain risks) and the interconnectivity of systems to each other and the Internet has exacerbated this vulnerability.[3] In fact, some analysts warn of the potential for cascading failures within and across sectors in the event of a major assault.[4] For instance, a cyberattack that disrupted natural gas supplies could bring down the power grid, which would in turn prevent water systems from operating, and so forth. A separate concern is that successful cyberattacks on control and safety systems in some sectors could result directly in destruction and loss of life. This concern figures prominently when it comes to dams, pipelines, refineries, aviation, and nuclear power plants.

Some critical infrastructure sectors are near-constant targets of probes and intrusions, including from hostile nation-states. In general, individual owner-operators of critical infrastructure are not sufficiently equipped to respond to potential attacks by well-resourced, sophisticated actors that may have an interest in bringing down a whole system. The broad "attack surface' (that is, the number of systems vulnerable to hacking) therefore creates a potentially significant security threat.

The policy framework. Most critical infrastructures in the United States are owned and operated by the private sector. Private firms often have no financial incentive to take into account the effects that disruptions in their operations could have on other firms—"externalities," in the parlance of economics. Firms may also invest less than security-minded government officials might want them to do for other reasons, especially if they are financially constrained or lack information or expertise. For instance, in some utilities sectors, such as water and electricity, smaller firms may not be able to hire knowledgeable cybersecurity professionals and investment in cybersecurity is subject to rate base constraints. This combination of factors places the federal government in the position of attempting to ensure that firms take precautions against cyberattacks as opposed to relying on firms to institute precautions on their own. Unfortunately, the federal government has yet to clearly specify an overall desired end-state for critical infrastructure cybersecurity that can guide a national strategy.[5] As a result, to date the government's response has been an "improvised patchwork" of policies.[6]

First, the government has fostered voluntary collaborations within critical infrastructure sectors and sub-sectors aimed at sharing information about threats and vulnerabilities. The main institutional manifestations of this approach are the Information Sharing and Analysis Centers (ISACs), typically run by industry and organized by sector or sub-sector. In theory, ISACs give firms access to information from each other and from the government that they could never obtain on their own. Such information allows them to better target their cybersecurity investments and to connect the dots to reveal system-wide threat actor campaigns.[7]

Second, the federal government has invoked regulatory approaches to cybersecurity in some sectors. Some regulatory agencies have expanded legacy authorities to incorporate cybersecurity, to greater (e.g. financial services and electricity) or lesser degrees. Other agencies (such as the Environmental Protection Agency with respect to water systems) have been given new authorities to address critical infrastructure security in general, including cybersecurity. Such purposive federal action on cybersecurity takes a range of forms: prescriptive regulation (i.e. explicit instructions on what specific cybersecurity measures firms should take), "quasi-mandates,"[8] liability shifting (in which firms failing to observe industry standards may be vulnerable to lawsuits), and the like.

Third, some government agencies furnish direct assistance to firms. For instance, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) offers some assistance with planning, response, and simulations, and the Department of Energy has provided grants to firms and funded research and development in the electricity sub-sector to address specific vulnerabilities. The Federal Bureau of Investigation and other federal law enforcement agencies likewise provide some operational support to firms, sometimes facilitated through existing trust relationships between government employees that move on to industry.

Beginning in the financial services sector, the government has begun to test out more intensive coordination with systemically important firms.[9] The Financial Service Analysis and Resilience Center (FSARC) served as the interface for Project Indigo, in which participating firms could reach out (through the Department of Homeland Security) to the Intelligence Community and U.S. Cyber Command in order to respond to threats and forestall attacks.[10] Recently, the FSARC incorporated firms outside of financial services (including leading electricity companies such as The Southern Company), changing its named to "ARC."

Analysis

This policy framework has encouraged greater investment in cybersecurity in some sectors but with uneven and often limited increases in security. With regard to information-sharing, ISACs vary enormously in their coverage of firms in a sector and in their seriousness of purpose. None involves routinized, real-time, two-way sharing of information between industry and government. In many industries, the larger firms perceive relatively little value from the information they receive from the government, believing that their informal connections to officials, in-house detection capabilities, and what they can buy from private cybersecurity service providers are more valuable.[11]

Voluntary information-sharing across firms can work well where there is little competition (as in electricity, nuclear power, water, and dams). However, it can be problematic in other sectors, as it requires firms to pass on findings about threats and vulnerabilities to business competitors. The situation is particularly challenging in sectors where firms often compete against one another *on the basis of their cybersecurity capabilities* (as in certain telecommunications companies). In rare cases, such as financial services, cyber threats to one are perceived as a risk to the entire system that all firms depend on which disincentives competition on cybersecurity.

Regulatory approaches have also bumped up against problematic realities in cybersecurity. Because neither firms nor the government know which cybersecurity investments will prove to be successful against a determined adversary, directives by the government to private firms do not necessarily enhance security, even though they could be very costly to firms; in fact, firms' efforts at compliance with regulatory mandates may cannibalize useful investments. Furthermore, the rule-making process simply cannot keep up with a dynamic threat environment,[12] and even well-crafted mandates that enhanced security at the time they were announced could rapidly become obsolete.

The third element of the current policy framework—direct federal assistance—also remains problematic. Grants provided by the Department of Energy go both to firms that need financial assistance (heavily regulated, cash-starved electric utilities) and firms that could make their own investments. Operational assistance to private owner-operators is *ad hoc* and skewed toward large firms that have hired talent from out of government. The promising element of the existing framework is the creation of the ARC, as it suggests a very different sort of intensive, seamless collaboration between industry and government.

Recommendations

An improved policy framework would have four elements. Together, this mix of policies will produce much greater cybersecurity for critical infrastructure than either a classic regulatory regime or purely voluntary cooperation between industry and government.

1. **The federal government must tailor its policies to the idiosyncrasies of each sector, including their distinctive market dynamics, threat profile, and cybersecurity capabilities.** Information-sharing regimes, regulatory mandates, forms of assistance, and informal interactions between business and government that work well in one industry will fail in another. For instance, heavily regulated and cash-constrained public utilities may require subsidies. By contrast, oil and gas firms or pipeline companies do not need subsidies but may need to be prodded into action through the threat of regulatory activity, in order to compel companies to share information with one another and with the government regarding vulnerabilities that affect control systems. In the communications and information technology sectors, still another mix of policies will be needed to take into account the fact that firms can be extremely averse to sharing information on vulnerabilities with one another.

   Additionally, each sector has a unique composition and market dynamic that can complicate the required trust and organization at the foundation of an effective partnership. For example, in the electricity sub-sector a small number of larger firms account for the majority of the market whereas water is composed of a high number of much smaller providers. In electricity, there is little direct competition between firms, enabling easier trust building. In contrast financial services has intense direct competition (though not on cybersecurity) which creates bounds to the trust developed. Adapting existing trust structures, such as trade groups or informal leadership associations has proven effective in overcoming many of these challenges. In cases where an existing structure does not exist, it will have to be created.

   Voluntary collaboration with the government also depends on having a sector-specific lead agency that has the right authorities, relationship with the private sector, and cyber expertise. In some sectors (such as water and health care), these factors have not been present. Likewise, where the historic relationship between industry and government is adversarial (as in oil and gas), the strategy for engagement must adapt for collaboration to be fruitful.

   The architecture of the whole regime thus needs to be reviewed across all sectors, with an eye toward understanding better what works in each. Although CISA could theoretically

undertake this effort, in practice the way DHS works with the sectors assigned to it will need to be part of that review. Therefore, this effort is best coordinated by a White House office, potentially by the newly established office of the National Cyber Director. In-depth research for the review could be commissioned from universities or not-for-profit organizations operating in this space (e.g. the Center for Internet Security).

Crucially, any policies developed as a result of this review should actively involve the private sector as a full partner. Full partnership does not simply mean involving government agencies close to the private sector (such as the Department of Commerce and the Department of Homeland Security's office of the private sector), though they should be included. Nor does it mean occasional consultations with the private sector. Rather, there should be a private sector review through the Sector Coordinating Councils that runs in parallel to government reviews, with ample coordination between business and government along the way within each sector.

2. **The government should focus its efforts on the most vital sectors, firms, and functions whose failure would truly have significant effects on the country as a whole.** Not all sixteen critical sectors currently identified by the government are equally critical, nor are all firms within each sector equally important. Continuity of operations for nationally important functions in a given sector usually depends on a handful of firms; many sectors are not threatened if smaller firms fail. All told, there are probably 20 to 50 firms or functions where concerns about continuity of operations necessitate aggressive federal involvement.

   The decision about which firms fall into the category of systemically important should be made according to transparent criteria, and reviewed annually within the government. Which firms meet these criteria should also be subject to review, meaning that new firms may be added to the group.

3. **Government collaboration with large firms should be based on true integration of effort in information-sharing, planning investments and resilience, and operational threat mitigation.** Operational integration requires a joint war room involving a few dozen of the largest firms, akin to an expanded version of the ARC. Participating firms would be expected to share information and plan their investments and actions (in both security and resilience) collaboratively, with reciprocal obligations and peer review to ensure that such investments are made. Firms that fail to meet the criteria for membership should be excluded.

   Until this regime is established, fiat regulation may be needed in a small number of sectors (such as pipelines and oil and gas) to ensure that firms take minimal steps against potential cyber attacks. However, the main goal of regulation should be to break down barriers to

integration of effort, not to create a top-down regulatory regime.

In the beginning phases, an expanded ARC would be focused mainly on tactical issues, like threat identification and operational responses. The current mechanisms by which firms engage with operational elements of the government through the Department of Homeland Security are an appropriate way to start, though ultimately direct engagement between firms and operational elements such as Cyber Command may work as well.

Despite the initial tactical focus, an expanded ARC should also become a vehicle for discussion about resilience and related planning efforts. Ultimately, such efforts should involve the broader set of firms through ISACs. However, it is reasonable for certain strategic discussions (e.g. about supply chains) to start within the smaller group of systemically important firms.

As with Recommendation 1, the private sector must be a full partner in this effort. Neither the vision for integration of effort nor the mechanisms of implementation should be imposed by the federal government. Rather, as with other successful partnerships (such as the Air Cargo Advanced Screening Program created by the Department of Homeland Security and international freight carriers), the new regime should be *co-created* with the firms involved. Legislative mandates should only come after the regime is working well and should be aimed at maintaining it.

4. **Although intensive engagement must focus on the largest firms, the policy framework should include federal assistance to smaller and medium-sized owner-operators of critical infrastructure.** Currently, the system informally benefits larger companies. Very large companies will also gain from inclusion in more intensive partnerships with the government (such as an expanded ARC). To reduce this bias, the government should use ISACs as the vehicle through which information can ultimately be disseminated outward from more intensive collaborations with a few larger firms. This approach will in turn require focused government effort to breathe life into ISACs that have not worked well because of collective action problems inside a sector, a poor fit between industry and sector-specific government agencies, lack of trust relationships among firms, and other sector-specific obstacles.

   The federal government should also encourage the development of turnkey cybersecurity solutions that can be purchased by smaller firms, in two ways. First, it should extend the model by which the Department of Energy and national labs have worked with the energy sector in order to design bespoke solutions for specific sectors where heavy regulation (e.g. on rate of return) or municipal ownership has left them without the resources to make adequate investments. Second, it should subsidize the development of cybersecurity solutions

for smaller firms, especially those targeted at less lucrative markets. Entities like ARPA-E, IARPA, or DARPA could play a role in this effort, though other agencies might be also be involved. Again, these efforts should be a product of partnership with organizations that represent smaller firms, not programs invented by the federal government alone.

Acknowledgements

We are grateful to Alan Bersin, Joel Brenner, Nate Bruggeman, Larry Clinton, Brian de Vallance, Mark Montgomery, and Tony Sager for critical comments on an earlier version of this paper.

About the Authors

Sean Atkins is a doctoral candidate in political science at the Massachusetts Institute of Technology and an active duty officer in the U.S. Air Force.

Chappell Lawson is an Associate Professor of Political Science at the Massachusetts Institute of Technology. Dr. Lawson has served in several government positions, including Executive Director of Policy and Senior Advisor to the Commissioner of U.S. Customs and Border Protection.

Notes

1 42 U.S.C § 5195c.

2 Cybersecurity and Infrastructure Security Agency (CISA), "National Critical Functions: Fact Sheet," available at https://www.cisa.gov/sites/default/files/publications/factsheet_national-critical-functions_508.pdf.

3 Nate Bruggeman and Ben Rohrbaugh, "Closing Critical Gaps that Hinder Homeland Security Technology Innovation," Homeland Security Policy Paper 5 (Harvard Kennedy School, Belfer Center for Science and International Affairs, April 2020).

4 See, e.g., Caitlin Durkovich, "Protecting Critical Infrastructure", in Chappell Lawson, Alan Bersin, and Juliette Kayyem, eds. *Beyond 9/11: Homeland Security in the 21st Century* (Cambridge, MA: MIT Press 2020).

5 Sean Atkins, "Defining Success for Critical Infrastructure Cybersecurity Policy," MIT Internet Policy Research Initiative, March 11, 2021, https://internetpolicy.mit.edu/defining-success-for-critical-infrastructure-cybersecurity-policy/.

6 Sean Atkins and Chappell Lawson, "An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure," forthcoming in *Public Administration Review*.

7 See the National Council of ISACs (https://www.nationalisacs.org/).

8 Daniel Crisp, Larry Trittschuh, and Gary Alum, "Cybersecurity in the Banking and Financial Sector," in Larry Clinton and David Perera, eds., *The Cybersecurity Social Contract: Implementing a Market-Based Model for Cybersecurity* (Internet Security Alliance, 2016): 82-99, 89.

9 Financial Services Information Sharing and Analysis Center, "FS-ISAC Announces the Formation of the Financial Systemic Analysis & Resilience Center (FSARC)," Press Release, October 24, 2016, available at http://www.prnewswire.com/news-releases/fs-isac-announces-the-formation-of-the-financial-systemic-analysis--resilience-center-fsarc-300349678.html.

10 Chris Bing, "Inside 'Project Indigo,' the quiet info-sharing program between banks and U.S. Cyber Command". *Cyberscoop*. May 21, 2018, https://www.cyberscoop.com/project-indigo-fs-isac-cyber-command-information-sharing-dhs/.

11 Atkins and Lawson "An Improvised Patchwork."

12 *See* Paul Rosenzweig, "The Unpersuasiveness of the Case for Cybersecurity Regulation – An Introduction," *Lawfare Blog*. May 17, 2012, https://www.lawfareblog.com/unpersuasiveness-case-cybersecurity-regulation-%E2%80%93-introduction. *See also* Congressional Research Service, *The Federal Rulemaking Process: An Overview*, Maeve P. Carey, Coordinator, RL32240, June 17, 2013, https://fas.org/sgp/crs/misc/RL32240.pdf.