CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

SEPTEMBER 2018

Cyber Policy Initiative Working Paper Series | "Cybersecurity And The Financial System" #2

Protecting Financial Institutions Against Cyber Threats: A National Security Issue

Erica D. Borghard

For your convenience, this document contains hyperlinked source notes indicated by this teal colored text.

© 2018 Carnegie Endowment for International Peace. All rights reserved.

Carnegie does not take institutional positions on public policy issues; the views represented herein are the author's own and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Carnegie Endowment for International Peace. Please direct inquiries to:

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: +1 202 483 7600
F: +1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Cybersecurity and the Financial System

Carnegie's working paper series 'Cybersecurity and the Financial System' is designed to be a platform for thought-provoking studies and in-depth research focusing on this increasingly important nexus. Bridging the gap between the finance policy and cyber policy communities and tracks, contributors to this paper series include government officials, industry representatives, and other relevant experts in addition to work produced by Carnegie scholars. In light of the emerging and nascent nature of this field, these working papers are not expected to offer any silver bullets but to stimulate the debate, inject fresh (occasionally controversial) ideas, and offer interesting data.

If you are interested in this topic, we also invite you to sign up for Carnegie's FinCyber newsletter providing you with a curated biweekly update on latest developments regarding cybersecurity and the financial system: CarnegieEndowment.org/subscribe/fincyber.

If you would like to learn more about this paper series and Carnegie's work in this area, please contact Tim Maurer, Co-director of the Cyber Policy Initiative, at tmaurer@ceip.org.

Papers in this Series:

- *Toward a Global Norm Against Manipulating the Integrity of Financial Data*
  Tim Maurer, Ariel (Eli) Levite, and George Perkovich, March 2017
- *Protecting Financial Institutions Against Cyber Threats: A National Security Issue*
  Erica D. Borghard, September 2018

Some cyber threats targeting financial institutions pose a risk to national security. This working paper presents a comprehensive proposal for conceptualizing and implementing operational collaboration between the U.S. government and critical elements of the financial sector to defend against significant cyber threats.

Erica D. Borghard is an assistant professor at the Army Cyber Institute at the United States Military Academy at West Point. The views expressed herein are personal and do not reflect the policy or position of the United States Military Academy, Department of the Army, Department of Defense, or the U.S. Government.

The National Security Implications of Cyber Attacks Against the Financial Sector

The U.S. economy is susceptible to offensive operations carried out by national security adversaries in cyberspace. States and highly capable nonstate actors are causing increasing strategic concerns, reflecting a deeper appreciation of the national security—rather than solely criminal—dimensions of the cyber challenge. In February 2018, the director of national intelligence and heads of the National Security Agency, Central Intelligence Agency, and the Federal Bureau of Investigation warned in congressional testimony that cyber attacks perpetrated by foreign adversaries represent one of the greatest national security concerns and the top priority of the intelligence community. Director of National Intelligence Dan Coats proclaimed that the U.S. was "under attack."

The U.S. government has focused on defending government networks and developing offensive capabilities to counter adversaries in cyberspace. However, the U.S. economy remains highly vulnerable to cyber attacks carried out by foreign threat actors. While this challenge spans many facets of the U.S. economy, this working paper focuses on cyber threats to the financial sector, especially to so-called Section 9 firms that are critical for the stability of the financial sector as a whole.[1]

Given the evolution of the threat landscape, foreign threats to the U.S. financial sector in cyberspace should be conceptualized as a national security challenge. The U.S. government has made important strides in identifying the problem, developing the authorities that could justify deeper operational collaboration with the financial sector, and taking initial steps toward collaboration. However, implementation remains mired in stale models of information sharing, occasional low-context "tear lines" (separating intelligence approved for release from that which remains classified), and irregular classified briefs. A well-conceptualized, comprehensive, and fully resourced plan for deep operational collaboration between the government and critical infrastructure is needed to address the scope and scale of the challenge.

This working paper presents a comprehensive proposal for conceptualizing and implementing operational collaboration between the U.S. government and critical elements of the financial sector to defend against significant cyber threats. In particular, prioritized intelligence collection against sector-specific threats, side-by-side analytic collaboration between government and private sector analysts, fully articulated playbooks, routinized exercising of playbooks, and the development of organizational connective tissue between the sector and government would substantially enhance defense in cyberspace of a key sector of the U.S. economy.

Several key considerations are worth highlighting up front:

- Because private entities own and operate most of the financial sector's critical infrastructure that would be targeted by foreign adversaries for strategic purposes, the government and Section 9 firms must collaborate as partners to defend this aspect of the U.S. homeland in cyberspace.
- Implementing a truly collaborative relationship between Section 9 firms in the financial sector and the U.S. government faces important hurdles that need to be acknowledged and addressed. For instance, the multinational nature of many companies raises potential tensions between U.S.-based firms with global financial interests and the U.S. government. This creates challenges for sharing sensitive national security information.
- Stakeholders on both sides should consider the potential unintended consequences of deepening cooperation between the U.S. government and Section 9 firms on national security issues in cyberspace. The cooperation may inadvertently produce escalatory dynamics or justify retaliatory attacks against the financial sector.
- Extending these recommendations to other sectors of the U.S. economy requires considering the distinctive needs of each sector. Although there are elements that could be replicated across other sectors, this working paper presents a proposal specifically directed at collaboration between the financial sector and the U.S. government.

The paper first analyzes the nature of the national security challenge and discusses existing efforts by the government and financial sector to confront it. Next, it presents a case for deepening operational collaboration between the government and the sector based on existing authorities. Then, it proposes specific policy recommendations that could be implemented to improve defense of the financial sector against cyber-related national security threats. Subsequently, it articulates how these recommendations could be implemented from an organizational perspective. Finally, the paper concludes by presenting avenues for future efforts.

A Growing National Security Challenge

There is a long history of criminal entities targeting the financial sector via cyberspace for the purposes of economic gain. Policymakers have developed robust programs to confront criminal behavior in cyberspace, ranging from congressional legislation through the 1984 Computer Fraud and Abuse Act to extensive law enforcement efforts to investigate cyber crime in close collaboration with the private sector, such as the National Cyber Investigative Joint Task Force (NCIJTF).

However, identifying economic espionage and theft as the only challenges stemming from cyberspace for the financial sector risks marginalizing the potentially significant threats posed by foreign adversaries seeking to inflict damage on the U.S. economy for political objectives or to lay the foundations for future attacks.

In recent years, the threat landscape has evolved to encompass not only criminal or profit-motivated actors but also state and nonstate actors leveraging cyberspace to target financial institutions. The use of cyberspace for national security–related objectives ranges from the merely provocative, such as defacing websites or hijacking social media accounts, to cyber operations in support of conventional military operations, to highly disruptive or even destructive attacks against a state's critical infrastructure. In response, states have increasingly invested in developing cyber capabilities for strategic purposes. Perhaps the most notable example is the unanticipated pace of the evolution of North Korea's offensive cyber capabilities, from relatively simple distributed denial of service (DDoS) attacks to malware attacks such as WannaCry in 2017.

Nation states, either directly or working through proxy actors, have already demonstrated a willingness and capability to target global financial services infrastructure. North Korean cyber attacks against the financial sector, for instance, are highly connected to the U.S. sanctions regime; Pyongyang has circumvented sanctions and funded its nuclear program through, among other things, a series of heists using SWIFT, a global messaging system, against the Bank of Bangladesh in 2016 and Taiwan's Far Eastern Bank in 2017. The Iranian DDoS attacks against the U.S. financial sector between 2011 and 2013 and the North Korean attack against South Korean banks in 2013 are other notable examples. Beyond criminal entities, the actors targeting financial institutions are highly capable states, such as Russia, China, Iran, and North Korea, or proxy actors enabled by these governments.

The U.S. financial system is a target for foreign cyber adversaries for several reasons. First, the financial sector is one of the bedrocks of the U.S.—and global—economy. Significant disruptive or destructive attacks against the financial sector could have catastrophic effects on the economy and threaten financial stability. This could occur directly through lost revenue as well as indirectly through losses in consumer confidence and effects that reverberate beyond the financial sector because it serves as the backbone of other parts of the economy. For instance, cyber attacks that disrupt critical services, reduce confidence in specific firms or the market itself, or undermine data integrity could have systemic consequences for the U.S. economy.[2]

Second, after over two decades of global military leadership, cyberspace is the only domain of warfare in which the United States faces near-peer, or even peer, competitors. Put together, this makes the financial sector an exceptionally attractive target for adversaries because it provides them with an asymmetric advantage: targeting the financial sector in cyberspace is one of the few ways adversaries can directly challenge the United States, through significant and potentially catastrophic effects on the U.S economy.[3] Thus, when a conventional confrontation is out of the question, rivals may prefer to target the "soft underbelly" and coerce the United States via cyber means.[4]

This risk is only likely to grow as the financial sector increasingly relies on digital infrastructure and financial technology, systems become more interconnected and processes become more automated, threat actors become more capable and adaptive, and geopolitical dynamics create motivations to disrupt the U.S. economy. However, the infrastructure of information and communications technology was not designed with security as a priority.

These risks are compounded by the international and interdependent nature of the global financial system. Specifically, U.S.-based firms that are essential to U.S. financial stability have interests and operations that span the world, creating an exceptionally large surface area of attack for foreign threat actors to challenge U.S. interests far from the homeland. Moreover, global financial interdependence also breeds global financial vulnerability. A U.S. financial institution designated to be "too big to fail" in cyberspace could be held at risk indirectly through cascading effects on the global financial system if foreign threat actors target financial institutions in foreign countries. In turn, the outsized role the United States plays in the global economy also implies that the stability and integrity of U.S. financial sector firms are critical to global financial stability. Therefore, properly resourcing the defense of U.S. Section 9 firms will have positive effects that extend beyond U.S. economic and national security.

The Protective Gap

These kinds of attacks raise important questions about the sufficiency of existing plans and capabilities for defending elements of the private sector that have been designated as critical infrastructure against foreign adversaries. The U.S. government protects the private sector from physical threats—for example, ballistic missiles. But firms in the cyber realm currently bear the brunt of the defensive burden to protect their networks against sophisticated foreign states. Most private firms lack the capabilities (such as intelligence collection and offensive action) and expertise (such as expertise in campaign planning) to contend with advanced state adversaries. And for the more

sophisticated ones, the government does not grant private entities the legal authority to engage in more proactive measures to defend their networks. While some of these capabilities are inherently governmental, it is likely that, if granted the authority, firms would invest even greater resources to enhance their capabilities.

This conundrum has prompted some within the private sector to advocate legalizing "active defense" or "hacking back," which would loosen existing constraints on how firms can defend their networks and potentially even allow them to operate outside of their networks to contend with cyber threat actors.[5] However, enabling these kinds of activities would create considerable risks for private entities in the United States, particularly because actions taken by private actors could result in unanticipated and undesirable responses by foreign adversaries. Indeed, the advocacy for more active defensive measures by some elements in the private sector underscores the gap between the significance of the problem and the measures currently in place.

The challenge is compounded by the insufficiency of a normative framework at the international level to limit harmful behavior.[6] The most recent meeting of the United Nations Group of Governmental Experts (GGE) ended in failure in the summer of 2017, with representatives unable to agree on fundamental issues such as the extent to which international law applies to cyberspace.[7] This was a significant regression from 2015, when the GGE achieved consensus on the application of international law to cyberspace as well as a voluntary norm against targeting civilian critical infrastructure. More promisingly, in 2016, the G7 states issued nonbinding principles regarding guidelines for protecting the financial sector against cyber attacks, which were reaffirmed in 2017. And, in 2017, the G20 states agreed to address cyber risks to the global financial services industry. However, mechanisms for actually operationalizing and enforcing these principles are poorly defined and fleshed out.

Overall, the current international environment presents uncertainty regarding the extent to which targeting a nation's critical infrastructure would impose significant reputational or legal costs. Furthermore, the impact of previous efforts to deter or punish attacks against critical infrastructure in cyberspace, such as imposing sanctions or indicting individuals, remains ambiguous.

As the apparent threat to U.S. critical infrastructure stemming from highly capable and highly motivated cyber adversaries has grown over time, the U.S. government has appropriately framed the scope of its mission in cyberspace to include defending the nation against these threats. However, there are continuing gaps in authorities, policy, and capabilities that should be remedied.

The Status Quo: Existing Government Efforts and Authorities for Operational Collaboration With the Financial Sector

The government has made some important steps in conceptualizing foreign threats in cyberspace and in developing the authorities to confront it. A February 2013 executive order, Improving Critical Infrastructure Cybersecurity, identifies the cyber threat to critical infrastructure as "one of the most serious national security challenges we must confront." It defines defense of critical infrastructure in cyberspace in explicitly national security and strategic terms, rather than solely criminal or economic ones. Section 9 of the executive order directs the secretary of homeland security to identify critical infrastructure at greatest risk. The Section 9 designation encompasses a subset of private sector firms designated by the U.S. government as owning or operating infrastructure where "a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." This executive order focuses on institutionalizing mechanisms for information sharing and adopting a framework to mitigate cyber risk to critical infrastructure.

Information sharing has been the focus of the federal government's initiatives to foster partnerships with the larger U.S. private sector (as distinguished from Section 9 firms that are classified as critical infrastructure). These initiatives were designed to distribute technical indicators useful for network defense as quickly and broadly as possible. For example, the Department of Homeland Security (DHS), the National Cybersecurity and Communications Integration Center, and the United States Computer Emergency Readiness Team automatically distribute indicators of compromise and threat information via Trusted Automated eXchange of Indicator Information, Structured Threat Information eXpression, and Automatic Indicator Sharing.

In April 2015, the U.S. Department of Defense (DOD) articulated the concept of "defending the nation" in cyberspace, moving beyond the previous framework of information sharing to reduce risk. According to the Department of Defense Cyber Strategy, one of the DOD's three priority strategic goals for its cyber mission is to "defend the nation against cyberattacks of significant consequence." This strategic objective is distinguished from only defending DOD networks and is therefore more encompassing in scope. The strategy document calls for working with the private sector in support of the "defend the nation" mission and identifies specific DOD functions that support this mission. These include developing intelligence and warning capabilities to anticipate threats and developing and exercising capabilities to defend the nation. Within the DOD, the Cyber National Mission Force (CNMF) is responsible for defending the nation's critical infrastructure in cyberspace.

Presidential Policy Directive 41 (PPD-41) of July 2016 articulates principles for a federal response to cyber incidents involving either the government or private sector entities. This builds on Presidential Policy Directive 21 of February 2013, which stipulated the development of a national unity of effort, including the private sector, to ensure the security and resilience of critical infrastructure. Notably, PPD-41 expresses that "the private sector and government agencies have a shared vital interest in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences."

U.S. President Donald Trump's administration articulated in a May 2017 executive order, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, that "it is the policy of the executive branch to use its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure." The 2017 National Security Strategy explicitly identifies the financial sector as part of critical infrastructure to be protected from cyber threats. It states that the government will furnish owners and operators of critical infrastructure with the authorities, information, and capabilities to prevent cyber attacks; that the government will respond with "swift and costly consequences" to the latter if they occur; and, beyond information sharing, "expand collaboration with the private sector . . . [to] better detect and attribute attacks."

Continuing Gaps Hampering an Effective Response to Increasing Risks

Achieving a greater understanding of the threats facing Section 9 firms requires precise analytics that are best derived from focused, full-cycle, joint intelligence efforts. Information-sharing mechanisms between the government and the financial sector should be institutionalized and routinized, with clearly defined thresholds that would trigger the sharing of threat information. More critically, both the government and the private sector would benefit from contextual information and intelligence. From the private sector side, this would enable specific efforts to defend critical infrastructure networks being targeted by nation-state adversaries for their economic and national security value. From the government perspective, this would support more focused and relevant intelligence collection efforts—as allowed by existing authorities—and a deeper understanding of the adversary and the threat environment.

As the designated Sector-Specific Agency for the financial sector, the Department of Treasury's Office of Intelligence and Analysis (OIA) provides intelligence support to the sector. However, the agencies that would be coordinating and responding to an attack of consequence on financial institutions, such as the DHS and DOD, need to receive sector-specific intelligence collection and

analysis that would enable that mission. In short, to effectively defend the nation, the government needs precise information from critical infrastructure owners and operators in the financial sector that would enable it to support government intelligence collection against foreign sector-specific threats. Without knowledge of the systems firms use, the structure of their networks, and the types of threats they face, government collection cannot possibly be properly focused and is likely to miss the most pertinent intelligence that would aid defenders.

In light of this review, a more comprehensive executive order that specifically addresses defense of the nation in cyberspace would be useful to drive developing and exercising operational plans commensurate with the scope and nature of the threat and to mobilize the resources required for its successful implementation.[8] To date, the 2015 DOD cyber strategy document offers the most robust articulation of the government's active, operational role in confronting foreign adversaries targeting critical infrastructure. The 2017 National Security Strategy employs the term "collaboration" as well. Yet, a fully articulated vision for defending Section 9 firms in cyberspace, with the private sector and government actively working together in a shared effort, does not yet exist. Therefore, an executive order that comprehensively tackles this issue is important to address existing gaps.

A Proposal for Collaborative Defense of Section 9 Firms in Cyberspace

A comprehensive proposal for the collaborative defense of Section 9 firms against national security threats in cyberspace would have several components:

- The U.S. government should prioritize government intelligence collection against foreign national security threats to the financial sector, within existing intelligence collection authorities.
- Firms and the U.S. government should formalize and institutionalize mechanisms for intelligence collaboration so that firms can share pertinent information with the government, work with intelligence community analysts on assessing threats, and utilize the intelligence produced across classification levels.
- Leaders from both the government and the private sector should work together to develop implementable playbooks for collaborative defense of the private sector and define the resources required to successfully implement them. These playbooks should drive capability development and should be validated through exercises that feed back into informing further capability development and refinement of the playbooks.

Implementing all the components of this proposal would better enable the government and the private sector to be proactive, anticipate national security threats, and have actionable plans in place to protect and defend critical elements of the financial sector against a range of malicious actors, rather than waiting until an attack has already occurred.[9] It is worth noting that this proposal represents an initial step toward contributing to broader financial stability in cyberspace that focuses on the relationship between the U.S. government and Section 9 firms. A more holistic effort that includes the broader financial sector and international partners could be explored in subsequent initiatives.

Prioritized Intelligence Collection

Section 9 firms have invested significant resources in developing cyber threat intelligence capabilities, controls to better protect their networks, and protocols for crisis management and incident response. Despite these efforts, they are hampered in network defense by an incomplete view of the adversary. Firms simply do not have the full range of intelligence collection authorities or capabilities that are necessary to support a robust defense of their networks and infrastructure against state-level adversaries. While the U.S. government possesses these authorities and capabilities, and the DOD strives to "defend the nation" in cyberspace, it lacks a deep understanding of cyber threats to the financial sector. Put simply, a program for routine side-by-side analytic efforts does not exist. Therefore, prioritized and sector-specific foreign intelligence collection and analysis in a collaborative environment is a critical first step toward an improved model to support defending critical infrastructure in cyberspace against national security threats. Without good intelligence, defenders are blind to the threats they face and operations will not be optimized to counter them.

Within the U.S. intelligence community, the National Intelligence Priorities Framework (NIPF) establishes the nation's priority intelligence requirements and informs how the intelligence community allocates resources for intelligence collection and analysis. The U.S. president and national security advisor provide overall guidance for the most significant issues within the NIPF, with contributions by secretaries and cabinet-level department/agency heads. Integrating a standing Title 50 intelligence collection requirement into the NIPF would ensure that there is dedicated collection against national security threats to the financial sector.[10] Without a prioritized effort within the NIPF, any intelligence collection on cyber threats to the financial sector is likely to be ad hoc and will lack sufficient resources to support the effort.

The executive branch should make certain that appropriate guidance is provided to the NIPF to identify cyber threats to the financial sector as a priority. Section 9 firms should be formally

incorporated into every step in the intelligence cycle: planning and direction, collection, processing, analysis and production, and dissemination. This would drive the behavior and prioritization of the intelligence collectors engaged in this effort, who are many levels removed from the president. Dedicated intelligence should encompass

- traditional geopolitical factors that would indicate an intent to target the U.S. financial sector;
- indicators and warnings of threat actor interest in the systems critical to the financial services sector (developed in conjunction with the sector); and
- general collection on threat actor behavior and capabilities, including the means and methods for exploitation and attack (such as threat signatures).

Formalized Mechanisms for Analytic Collaboration

To facilitate analytic collaboration between Section 9 firms and the government, the government should consider downgrading the classification of intelligence to enable broader dissemination to key players in the financial sector. The 2015 Cybersecurity Information Sharing Act (CISA) requires the director of national intelligence, DHS, DOD, and the Department of Justice (DOJ) to facilitate and promote "the timely sharing of classified cyber threat indicators . . . with cleared representatives of relevant agencies . . . [and] cyber threat indicators or information in possession of the Federal Government that may be declassified and shared at an unclassified level." The act also provides liability protection to private entities sharing information with the government. CISA led to a much-improved system for rapid notification of particular private sector firms where classified collection indicated adversary interest or a potential breach. This notification may take the form of classified briefs or unclassified "tear lines."

Section 9 firms responsible for protecting critical infrastructure need a deeper, more routinized relationship across classification lines than the current one-way process. To be effective, intelligence should be both informed by and useable by the consumer. This would be nearly impossible absent a routine program of side-by-side analytic collaboration between intelligence community analysts and private sector critical infrastructure. Analysts in each camp may not be operating according to the same analytic priorities or the same data and, therefore, may have vastly different perspectives on identical threat actors. Additionally, side-by-side collaboration would enable private sector analysts to provide input into the complex problem of identifying information that might be of more use if downgraded to a different classification level or recast in an unclassified product.

A significant impediment to side-by-side analytic collaboration is the dearth of owners and operators of critical infrastructure with the right security clearances. While the U.S. government has a fairly robust process for clearing private sector personnel in the Defense Industrial Base (DIB) to accomplish their national security mission, that same system is inadequate—and not scoped—for use outside of the DIB. The largest (and, therefore, most important) Section 9 firms in the financial services sector are multinational entities. Their operations and interests span the globe, and they employ foreign nationals. By definition, this introduces a risk that sensitive intelligence information could fall into the hands of foreign governments, including adversaries. The protocols used to evaluate defense contractors for risks associated with the sharing of classified information do not translate well when applied to these firms. Taking this into account, DHS was charged with developing a hybrid process to sponsor clearances for a specific number of individuals within Section 9 firms. However, progress has been slow on this element, which is key to the overall success of operational collaboration.

Relatedly, intelligence collectors within the government should be furnished with actionable feed on which to collect. Pursuant to all legal, regulatory, and compliance regimes, the financial sector should share unique information about the sector's networks, systems, infrastructure, and threat landscape to enable the government to collect information within its own authorities that is pertinent to firm defenders.

Playbooks

Existing playbooks addressing cyber contingencies were designed for the financial services sector as a whole, not specifically focused on designated critical infrastructure firms. For instance, the All-Hazards Crisis Response Coordination Playbook was produced following the 2014–2016 Hamilton Series exercises, which comprised thirteen exercises between representatives from several U.S. government agencies and the financial sector that addressed decisionmaking and cooperation in different types of crisis scenarios that could impact the sector. These initiatives served an important purpose by identifying some of the key risks and challenges faced by the sector across a range of contingencies and spurring investment in specific programs to enhance resiliency, such as the Sheltered Harbor initiative.

Playbooks should go a step further and be more systematically integrated into the full spectrum of the policymaking process—feeding back into intelligence collection efforts, driving resource allocation and capability development, and operating as dynamic documents that are exercised, refined, and updated over time. Fully articulated playbooks developed together by the private sector

and appropriate government agencies (including the DHS, Treasury, and U.S. Cyber Command) can enable a better-coordinated, shared national cyber defense of financial sector critical infrastructure. Playbooks should be developed around threat actors; types of attack, including persistent versus one-time events; and systems to be defended.

Specifically, playbooks should detail how government agencies and firms will operate together to defend the sector, and clearly define the authorities, roles, and responsibilities of all stakeholders. Additionally, the playbooks should be linked with the dedicated intelligence collection and information-sharing piece described in the previous section; sector-specific indicators and warnings in playbooks should inform intelligence collection, such that the observation of specific indicators and warnings would then trigger the activation of specific playbooks.

Several key aspects of developing playbooks should be taken into account. Currently, there is ambiguity regarding the locus of command and control (C2) responsibilities in the event of a cyber attack on critical infrastructure. Explicitly defining C2 is essential for a collaborative public-private defense of the financial sector. C2 is indispensable for ensuring that the multiple actors and agencies participating in the cyber fight are coordinating activities and staying within appropriate lanes. National roles and responsibilities are presently articulated such that the DOJ and the Federal Bureau of Investigation are responsible for investigation and enforcement; the DHS takes the lead on protection; the DOD is in control of national defense; and the intelligence community support all of these entities by providing cyber threat intelligence and attribution. However, in practice, there is considerable overlap between these responsibilities as they have been defined.[11] For instance, while the DHS is responsible for protecting critical infrastructure, the DOD is charged with defending the nation from attack; a systemic attack against the financial sector would fall under both of these categories. Uncertainty regarding the roles and responsibilities of various federal agencies in the midst of a crisis will inevitably hinder response efforts and cause preventable damage. Additionally, C2 considerations should move beyond clarifying lines of authority across the various relevant government agencies to also incorporate the private sector as an essential actor in the chain with stipulated roles and responsibilities.

Moreover, there is some inconsistency between how these responsibilities are articulated in PPD-41 and how they are interpreted in the 2016 DHS National Cyber Incident Response Plan (NCIRP). The latter states that if there is a significant cyber event (defined as one that is likely to cause harm to U.S. national security, foreign relations, the economy, public confidence, civil liberties, or public health and safety) that affects a private entity, "the Federal Government will typically not play a role . . . but the cognizant Sector Specific Agency(ies) will generally coordinate the Federal Government

efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure." For the DHS to designate specific private sector firms as operating infrastructure where a cyber attack could have catastrophic national and economic security effects, on the one hand, and then, on the other hand, promulgate plans that define a limited federal role in the response to generalized private sector cyber attacks, as described in the NCIRP, would seem to indicate that the U.S. government's thinking on this topic is incomplete.

Additionally, playbooks should identify the conditions under which DOD capabilities would be deployed in support of defense of the private sector in the event of a significant, systemic attack. While the financial sector is responsible for defensive operations on its own networks, there are potential actions that could be taken external to the United States against adversaries, such as targeting adversary command and control nodes, which would aid the private sector's defensive efforts. In theory, existing guidance under the DOD's Defense Support of Civil Authorities (DSCA) authorizes deploying DOD capabilities and resources, including federal military forces, to support civil authorities under both Title 10 and Title 32 authorities. Under this framework, playbooks could potentially provide for capabilities deployed under Title 10 through a sector-specific national mission team (NMT) that could serve as an offensive surge capacity to augment the defensive operations that would remain under the auspices of private firms. However, using a DSCA framework to support this concept is problematic for several reasons. A DSCA request is typically initiated by a state government, requires presidential approval, and is fundamentally geared toward crisis response rather than prevention. Therefore, new authorities would ideally be needed to support planning and resourcing for a standing capability within the DOD to confront foreign threats to U.S. critical infrastructure continuously and in real time as they arise.

Of course, incorporating any kind of planning for offensive operations as part of operational collaboration between the government and financial sector firms has complexities and challenges from planning and capabilities perspectives, as well as political and strategic ones. In terms of the former, the offensive operations that would be components of playbooks must be planned. This is because there is an intelligence component that supports offensive operations and a corresponding capability requirement that necessitates advanced preparation to deliver a desired effect to prevent further damage.

Additionally, in evaluating potential responses stipulated in playbooks, these factors should be assessed:

- The dynamic pace of capability development and adversary ingenuity means that playbooks should be sufficiently flexible, or dynamically reassessed, to accommodate changes in technology, adversary capabilities, and vulnerabilities.
- If playbooks are developed for specific contingencies against specific threat actors, this may require a team to hold many targets continually at risk—a feat that is costly and operationally complex. Under some conditions, it may be more efficient to develop response plans against specific categories of operations that are relatively target-agnostic.[12]
- Possible responses should consider the existing access and tools that the government has or can acquire and the timeline for developing responses (acknowledging that having the means to respond, especially through access-dependent means, may vary unpredictably over time).
- Specific thresholds that would invoke different categories of offensive actions should be clearly defined and observable such that there is little ambiguity that they have been crossed.
- Playbooks should consider the level of confidence in attribution that would be sufficient to prompt an offensive action against a target.

Relatedly, the private sector is constantly engaged with threat actors in cyberspace on a routine basis below the threshold of significant cyber attacks that would merit requests for supporting forces from the government. These include cyber intrusions or attacks stemming from unsophisticated criminal actors, patriotic hackers, and hacktivist groups. An example of the latter is Anonymous's OpIcarus DDoS campaign in 2016, which targeted banks around the world but resulted in minimal disruption of business processes. In constructing playbooks, it will be important for the private sector and government to address how daily, routinized cooperation and coordination should be structured and implemented, as well as collaboration in times of crises. The former will enhance the latter, because establishing clearly understood lines of communication and points of collaboration under business-as-usual conditions will strengthen the relationship between the private sector and government and enhance interoperability during crises. It will also better inform all stakeholders of their respective interests, capabilities, and priorities and enable the private sector to prevent the escalation of some incidents into crises.

The playbooks should also drive capability development on the part of both the private sector and government to ensure that, if a contingency should occur, involved parties are properly equipped. Examples of capabilities informed by playbooks include, for example, acquiring and maintaining access and tools against adversary infrastructure, investing in intelligence collection capabilities

against sector-specific indicators and warnings (for the government), and investing in technology and controls to protect against threat actor tactics, techniques, and procedures (TTPs) (for the private sector). For all parties, capability investment should go beyond tools and technology to include developing and resourcing organizations that support the effort and attracting, training, and retaining skilled personnel.

From a strategic perspective, extremely careful consideration of the potential conditions—given appropriate authorizations—under which the DOD would undertake any kind of offensive operations to support the defense of critical infrastructure is essential because these operations could create unanticipated and unintended negative effects. For example, knowing that there are specific conditions under which the government has agreed to come to the aid of the financial sector could create a moral hazard, emboldening the latter to take greater risks.

There is also the concern that operational collaboration between the financial sector and the government may generate escalatory risks against the former. Hypothetically, the contingencies that would activate U.S. government action against adversary command and control nodes could produce escalatory pressures. This could also incentivize adversary behavior short of established thresholds if the latter are made public. Adversaries may test the limits of thresholds or be willing to take risks to escalate just up to the point of a threshold known to invoke a government response.

If foreign adversaries generally perceive the U.S. private sector to be simply an arm of the U.S. government, this could inadvertently undermine norms against targeting the civilian economy in cyberspace. These concerns could be mitigated by establishing relatively high thresholds for offensive cyber operations and/or keeping thresholds secret. However, maintaining secret thresholds for responses would not serve the overall policy of deterring adversary behavior.

Overall, playbooks should ideally include a whole-of-government approach to the challenge of defending Section 9 firms against national security threats. While this proposal focuses more narrowly on collaboration among the DOD, DHS, Treasury, and Section 9 firms, there are other instruments of national power, such as diplomacy and law enforcement, that should be incorporated into playbooks to ensure a comprehensive U.S. government effort. Playbooks could also incorporate service providers (such as telecoms) and relevant third parties.

Exercising the Playbooks

Joint exercises are important for planning and coordination purposes. They also serve as a vehicle for assessing and remediating the flaws in playbooks. The Hamilton Series exercises, for example, were a good first step in terms of bringing together stakeholders from the U.S. government and the financial sector (beyond just Section 9 firms) and identifying key challenges and risks faced by the sector and gaps in response plans. The Hamilton Series exercises gave rise to two initiatives to enhance the resiliency of the financial sector, the Wholesale Payments Initiative and Sheltered Harbor.[13]

However, rather than serve as a stand-alone event (or series of events) not explicitly linked to national policies or integrated into a broader process, joint exercises should be systematically integrated into a full-spectrum program for operational collaboration. Specifically, the processes of intelligence collection and analysis, information sharing, playbook development, and exercising playbooks should be iterative. Exercising the playbooks should drive remediation of gaps in capabilities, feed back into refining and improving playbooks, and inform government intelligence collection.

Organizational Implementation

To implement this proposal, stronger connective tissue needs to be developed between the financial sector and the government. Some organizations already exist (but their roles and responsibilities need clarifying), while others could be created or repurposed under existing authorities. The following provides more specific suggestions for both the private sector and the government.

On the financial sector side, the Financial Systemic Analysis and Resilience Center (FSARC) could be envisioned to be the implementing arm for the joint program for operational collaboration. The FSARC was established in October 2016 by eight CEOs from some of the largest U.S. financial services firms. The organization operates under the broad umbrella of the Financial Services Information Sharing and Analysis Center (FS-ISAC), which is one of many information sharing and analysis centers that exist across different sectors of the economy that constitute critical infrastructure.[14] The FSARC is at an early stage in its development but its institutional framework could mature to become the organizational hub for intelligence analysis and collaboration with the U.S. government. The FSARC represents the interests of all member firms and was designed to enhance collaboration with the intelligence community, Treasury, and DHS on threats to the financial sector's critical systems; develop an early warning capability; and reflect the financial

sector's perspective on identifying and defining thresholds for different types of responses and developing playbooks.

Project Indigo, a pilot program that began in 2017, is illustrating the FSARC's potential to play an integral role in facilitating information sharing between some financial institutions and the U.S. government. In this nascent and informal program, firms have reportedly shared threat data with U.S. Cyber Command regarding nation-state threat actors. Ideally, routinizing this kind of cooperation, together with opportunities for joint training and exercises, could ensure the government is better equipped to recognize and respond to systemic threats to the sector and provide it with early warning of impending cyber attacks. However, Project Indigo is only in the pilot stage. Therefore, while it represents an important proof-of-concept for deeper collaboration between the government and Section 9 firms, there are nevertheless significant additional measures that should be taken.

On the government side, significant gaps remain in integrating U.S. government efforts with respect to Section 9 financial firms. Given existing authorities, the DHS would be the natural hub to coordinate the federal government's role across the different aspects of this proposal because the DHS's core mission is to safeguard the U.S. homeland. A DHS program office for financial sector critical infrastructure could synchronize the government's sector-specific foreign intelligence collection across the intelligence community, in conjunction with the OIA and Treasury's Office of Critical Infrastructure Protection and Compliance Policy. It could coordinate liaising between the FSARC and the intelligence community to receive the input from the financial sector that would guide government intelligence collection and facilitate side-by-side analytic efforts by government and industry intelligence analysts. Finally, it could lead the process for playbook development and exercises. Importantly, this proposal would not replace the DHS's key function in continuing to share vulnerability information through traditional mechanisms.

The operational arm of this effort inherently lies within U.S. Cyber Command, given its "defend the nation" role. An organizational reform to enhance this mission would be to create a standing national support team (NST) dedicated to the financial sector. Support teams have already been stood up under the Cyber Mission Force and are tasked with providing analytic and planning support to NMTs and combat mission teams (CMTs). Organizing some teams around resources and assets to be defended would contribute to more cohesive operational planning. A financial sector-specific NST, equipped with a sector-based understanding of threats and vulnerabilities based on information shared from the financial sector via the FSARC, could devise operational plans for defense of the sector based on integrated and sector-focused foreign intelligence collection and

analysis. The NST could also confirm or deny indicators and warnings developed through the playbooks.

Additionally, there is a potential function that National Guard or reserve units could serve in this initiative. For example, under Title 32 authorities, a dedicated cyber protection team (CPT) could be requested by the private sector to provide surge capacity in the event of an ongoing cyber attack in the form of advanced analysis and network and endpoint forensics. The CPT could also assist in coordinating and synchronizing response actions to attacks in support of NMTs. Therefore, playbooks should account for the potential role of CPTs. Furthermore, cybersecurity and operations teams within financial sector firms in all likelihood already employ personnel who serve as members of the National Guard and/or the reserve. Many of these individuals may possess security clearances and all have sector-specific knowledge and expertise. They could bridge the gap between the private sector and government both during a crisis and routine planning and collaboration. NSTs, for instance, could incorporate reservists and enable U.S. Cyber Command to seed personnel across the financial sector. An idealized, fully resourced version of deep operational collaboration between the government and the private sector would support joint day-to-day co-location of personnel. In practice, members of the National Guard or reserve could play this role.

The benefits this would grant to the financial sector are obvious, but there are also considerable gains that the government could reap from this arrangement. The intelligence community would derive measurable advantages from attaining a more holistic understanding of the threat landscape if the financial sector would share information about threat actor capabilities and TTPs. Within U.S. Cyber Command, this would enable operational teams to be better postured to deny the adversary the ability to conduct attacks against critical infrastructure.

Looking Ahead

Defending the critical economic engines of the United States is a vital national security concern. There are concrete steps that both the financial sector and government could take now, within current authorities, to improve operational collaboration to defend critical infrastructure in cyberspace.

Implementing the recommendations put forth in this working paper would go a long way toward making the U.S. safer against cyber threats of systemic consequence to critical infrastructure. If the intelligence community were better informed about the financial sector's key risks and worked side

by side with industry analysts in a classified environment, it would drive sector-specific intelligence collection that has greater fidelity to assess the specific threats to financial sector critical infrastructure. This would drive capability development for both the private sector and government so that all parties would be better equipped to counter adversarial actors. If joint playbooks were developed and exercised in conjunction with the financial sector based on sector-specific indicators and warnings, it would better inform capability development and intelligence collection. It would also ensure that stakeholders are better prepared for collaborative action if a systemic attack were to take place, because exercising and refining playbooks would improve interoperability, reduce friction, and augment capabilities.

Several important issues are beyond the scope of this working paper but merit further examination for a truly comprehensive approach to the defense of Section 9 firms in cyberspace. For instance, Congress should ultimately play a role in crafting legislation to support defense of Section 9 firms in cyberspace. This would ensure that the government does not have to play a patchwork game with existing authorities. Congressional action, for instance, could formalize through legislation that the DOD's "defend the nation" mission could include the government choosing, under some defined circumstances, to take countermeasures against nation-state adversaries attacking critical financial sector infrastructure through cyber means, clarify authorities for doing so, ensure sufficient resourcing, and institute liability protections for the private sector—essentially building and expanding on the 2015 CISA. However, the current political climate portends poorly for the prospects for congressional action in the near term.

More broadly, several issues must be highlighted, particularly the international dimension of this problem set. There is the potential for increased risks to U.S. Section 9 firms that adopt a national-security approach to cybersecurity that involves deeper collaboration with the U.S. government. For instance, this may jeopardize firms' business in foreign countries. However, the reality is that U.S. banks, in many respects, are already enforcement arms of U.S. foreign policy. For instance, banks are expected to enforce sanctions regimes against adversary states and nonstate actors—regimes they play no role in crafting. This has invited retaliation via cyber means against the U.S. financial sector. If anything, the risks to banks outweigh the benefits that would likely be conferred on these firms through better protection against the national security threats they already confront. But—to expand the scope beyond the U.S. government and U.S. firms—playbooks should anticipate attacks against the global financial infrastructure and consider potential multinational, allied, and coalition lines of effort to support the defensive mission.

A separate question is if other countries will replicate this model. From a U.S. national security perspective, it would be contributing to the global public good of a more secure and well-defended global financial system if allied nations would adopt similar types of arrangements. In fact, if the special intelligence relationship between the Five Eyes alliance partners were to be expanded to include sharing intelligence about threats to the financial sector, this would also facilitate increased global financial stability. Moreover, it would be naïve to assume that traditional U.S. competitors, such as China, do not already provide such support to their parastatals.

Finally, if successfully implemented, this proposal could also serve as a model to be replicated across other critical infrastructure sectors beyond the financial services sector, taking into account the former's specific requirements.

Notes

[1] Specific firms have been given the moniker "Section 9" to reflect their essential economic role and, therefore, the heightened risk to economic and national security of a significant cyber attack against them. Section 9 refers to the section of former president Barack Obama's February 2013 executive order, "Improving Critical Infrastructure Cybersecurity." While Section 9 firms exist across U.S. critical infrastructure, this working paper focuses on Section 9 firms within the financial sector because it is among the most highly targeted sectors in the United States and because it has already taken initial steps at establishing mechanisms to work more closely with the government on these issues, described in greater detail below.

[2] "Cybersecurity and Financial Stability: Risks and Resilience," Office of Financial Research, February 15, 2017. For more on cyber threats to financial stability, see Martin Boer and Jaime Vazquez, "Cyber Security & Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System," Institute of International Finance, September 2017; Juan Carlos Crisanto and Jermy Prenio, "Regulatory Approaches to Enhance Banks' Cyber-Security Frameworks," Financial Stability Institute, August 2017; Emanuel Kopp, Lincoln Kaffenberger, and Christopher Wilson, "Cyber Risk, Market Failures, and Financial Stability," International Monetary Fund, August 2017; "Understanding Systemic Cyber Risk," World Economic Forum, October 2016; "Guidance on Cyber Resilience for Financial Market Infrastructures," Bank for International Settlements, June 2016; and Eric S. Rosengren, "Strengthening Financial Sector Supervision and Current Regulatory Priorities," Basel Committee on Banking Supervision and the Financial Stability Institute, January 30, 2015.

[3] For a theoretical discussion on targeting a state's civilian economy, including the financial sector, with cyber means to achieve strategic objectives, see Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (May 2017): 452–81. While the term "catastrophic" may come across as hyperbolic, it is the term used by the Obama administration in executive order 13636 in 2013 to identify Section 9 firms that, if attacked in cyberspace, could result in "catastrophic regional or national effects on public health or safety, economic security, or national security."

[4] Richard K. Betts, "The Soft Underbelly of American Primacy: Tactical Advantages of Terror," *Political Science Quarterly* 117, no. 1 (Spring 2002): 19–36.

[5] As a recent report by the Center for Cyber & Homeland Security at the George Washington University notes, "Businesses never anticipated the scale to which they would be responsible for defending their interests against the military and intelligence services of foreign countries. Yet in many instances, this is exactly what certain industries and companies are facing." Also see the discussion of active measures in Wyatt Hoffman and Ariel (Eli) Levite, "Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?," Carnegie Endowment for International Peace, June 14, 2017.

[6] That said, significant work has been done to advocate cyber norms. See, for example, Tim Maurer, "Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cyber-Security?," Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011; Michael Schmitt and Tim Maurer, "Protecting Financial Data in Cyberspace: Precedent for Further Progress on Cyber Norms?," Just Security, August 24, 2017; Tim Maurer, Ariel E. Levite, and George Perkovich, "Toward A Global Norm Against Manipulating the Integrity of Financial Data," Carnegie Endowment for International Peace, March 27, 2017; and Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (July 2016): 425–79.

[7] However, there has been measured success in bilateral agreements between nation-states, such as the 2015 agreement between Obama and Chinese President Xi Jinping regarding refraining from engaging in economic espionage. In public remarks on September 25, 2015, following a meeting with Xi, Obama stated: "The United States government does not engage in cyber economic espionage for commercial gain. And today, I can announce that our two countries have reached a common understanding on the way forward. We've agreed that neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage." It appears that China has been largely holding up its end of the agreement; see Robert Hackett, "China's Cyber Spying on the U.S. Has Drastically Changed," *Fortune*, June 25, 2016.

[8] For statements on this topic, see Frank J. Cilluffo and Sharon L. Cardash, "Global Ransomware Attack Reinforces Message of Trump's New Cybersecurity Order," *Conversation*, May 11, 2017; Michael Chertoff and Frank Cilluffo, "Trump Administration Can Help Finance Sector Shift Cybersecurity Paradigm," *Forbes*, January 18, 2017; "Gen. Michael Hayden Gives an Update on the Cyberwar: Former Head of the CIA and NSA Says Government Moves to Protect Cyberspace Are Too Little, Too Late," *Wall Street Journal,* February 9, 2016; and Michael V. Hayden, "An American Strategy for the Internet," American Enterprise Institute, October 27, 2017.

[9] Examples of public-private collaboration in other sectors include the Defense Industrial Base (DIB) Cybersecurity Program and the relationship between the DHS's Industrial Control Systems Computer Emergency Response Team (ICS-CERT) and industry. These are useful models for conceptualizing what operational collaboration between the federal government and the elements of the financial sector designated as critical infrastructure could look like, but there are specific aspects of the financial sector that warrant a sector-specific arrangement.

[10] Within U.S. Code, Title 50 is the authority to conduct foreign intelligence collection. For a discussion of Title 50 versus Title 10 authorities, see Robert Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *Journal of National Security Law & Policy* 5, no. 2 (2011–2012).

[11] Furthermore, even within the DOD, there is uncertainty regarding which command would play a C2 role in the event of a cyber attack requiring DOD support to civil authorities, with U.S. Cyber Command, U.S. Northern Command, and U.S Pacific Command each articulating a separate understanding of which commands would play a supported versus supporting command role. See, "DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities During Cyber Incidents," U.S. Governmental Accountability Office, April 2016.

[12] However, these types of operations are typically less effective and cannot be employed against an adversary's strategic national assets. For further discussion of the different types of effects and costs that can be generated by different types of cyber operation, see Borghard and Lonergan, "The Logic of Coercion in Cyberspace."

[13] The Wholesale Payments Initiative was pioneered under the auspices of the Financial Systemic Analysis and Resilience Center (FSARC). The objective of the Wholesale Payments Initiative was to develop industry standards to increase the resilience of high-value payments systems and a playbook for banks in the event of an outage in those systems. In the United States, Fedwire Funds Service and the Clearing House Interbank Payments System process a daily average of $4.5 trillion high-value wire payments. Therefore, an attack against the high-value payments systems would present an extraordinary risk to financial stability. Sheltered Harbor was a program associated with the Financial Services Information Sharing and Analysis Center (FS-ISAC). Sheltered Harbor is a voluntary initiative that enables financial institutions to store encrypted customer account data in a vault and reconstitute it in the event of a cyberattack.

[14] The FSARC differs from the FS-ISAC in several respects. First, membership in the FSARC is significantly smaller than the FS-ISAC, focusing on systematically important financial services firms. Second, the FSARC is focused on mitigating systemic risk to the U.S. financial system, whereas the FS-ISAC focuses on the global risk. Finally, the FSARC's key mission is to foster deeper collaboration with the U.S. government, in contrast with the role of the FS-ISAC in sharing more general information about security threats and vulnerabilities across the global financial sector.

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: +1 202 483 7600

CarnegieEndowment.org