6

Cyber Governance and the Financial Services Sector

The Role of Public–Private Partnerships

Valeria San Juan[1] *and Aaron Martin*[2]

[1] *Fundbox, San Francisco, CA, USA*
[2] *Tilburg Institute for Law, Technology, and Society, Tilburg Law School, Tilburg University, Tilburg, Netherlands*

6.1 Introduction

In 2016, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), the network used by financial institutions to send and receive transaction information,[1] experienced a series of attacks resulting in the theft of millions of dollars. The first reported attack, which occurred in February 2016, resulted in an $81 million theft from the Central Bank of Bangladesh.[2] Hackers were able to exploit a vulnerability in the SWIFT network: they used the credentials of Bangladesh Central Bank employees to send fraudulent money transfer requests to the Federal Reserve Bank of New York, asking the bank to transfer money from the Central Bank of Bangladesh into accounts throughout Asia.[3] While the $81 million heist received most of the media exposure, there were several other theft attempts in June of the same year, some of which were also successful in sending fraudulent payment instructions.

In a private letter to clients, SWIFT stressed that "the threat is persistent, adaptive and sophisticated – and it is here to stay."[4] This suggests an increase in threats and attacks targeting financial institutions, not just directly but also through third-party networks and external systems like SWIFT. The SWIFT attacks demonstrate both the varied points of vulnerability within financial institutions and the interconnectedness of the global financial system. Meanwhile, the incident has prompted regulators around the world to refocus on cybersecurity requirements.

Regulatory scrutiny of cybersecurity in the financial industry is by no means new – particularly in the United States, where banks have seen more than 40

Rewired: Cybersecurity Governance, First Edition. Edited by Ryan Ellis and Vivek Mohan.

new cybersecurity-related standards, guidelines, examination expectations, regulations, and other requirements since 2014.[5] The Clearing House, an association that advocates on behalf of large banks, points to research showing that large multinational banks spend about 40% of their cybersecurity efforts on regulatory compliance.[6]

While this flurry of regulatory activity seeks to address the wide-ranging cybersecurity challenges facing the financial services sector (FSS) by prescribing various guidelines and rules, such an approach is not the only way of governing cybersecurity. The use of public–private partnerships (PPPs) provides an alternative vehicle for achieving cybersecurity outcomes. Therefore, in this chapter we aim to explore governance through the lens of the PPPs devised by the sector to address cybersecurity challenges. In particular, we focus on sector-led bodies and their role in organizing, coordinating, and governing cybersecurity efforts.

This contribution is the first to explore in depth the various FSS organizations focused on cybersecurity and critical infrastructure (CI) protection.[7] We first discuss how governance over security and the protection of CI has increased the focus on the role of PPPs in addressing issues of cybersecurity. We continue by highlighting three sector-led bodies – the Financial Services Information Sharing and Analysis Center (FS-ISAC), the Financial Services Sector Coordinating Council (FSSCC), and the Financial Systemic Analysis and Resilience Center (FSARC) – and how each facilitates PPPs to address challenges primarily in the areas of information sharing, policy coordination, and threat analytics, respectively. The chapter concludes with a discussion of lessons learned and remarks on future cyber governance research avenues. These lessons include: (i) validation of the PPP model, with some important caveats; (ii) the need to extend PPPs beyond information sharing to address systemic risks; and (iii) the limitations of PPPs in regulated industries like finance.

6.2 Governance, Security, and Critical Infrastructure Protection

While "government" refers to an entity – most often the state – with the recognized ability to make and enforce policy decisions, the concept of "governance" is generally defined in broader terms.[8] Governance concerns the exercise of authority by both formal institutions like the government and less formal organizations like markets or civil society.[9] Governance structures can therefore exist outside of government. In fact, governance often refers to the development of governing structures and mechanisms within and across the public and private sectors that do not explicitly relate to a formal government. Another defining characteristic of governance is that it does not rely on the legislative or authoritative power of the state to drive or command action.

It is widely understood and accepted that the state is responsible for the provision of national security, the protection of the nation-state and its citizens. Since it developed after World War II, the concept of national security initially had a strong military connotation.[10] While national security is still associated with the military, the use of the term has broadened to include nonmilitary security, such as the economic security of a nation. With the broadened understanding of national security, there has been increased focus on CI and the role it plays in maintaining national security. CI refers to services, assets, systems, and networks, whether physical or digital, considered vital to society.[11] Countries define their CI based on the criticality of services or sectors to the security and safety of the government, economy, and society.[12]

CI protection has been the focus of many national laws, guidelines, and frameworks. In the United States, there have been executive orders and presidential policy directives focused on CI protection since the Clinton administration. Executive Order 13010 ("Critical Infrastructure Protection"), in effect since 1996, was key to demonstrating the government's focus on CI.[13] It established a steering committee composed of representatives from different federal agencies. This committee was responsible for identifying and consulting with the public and private sectors deemed to be CI or that support and conduct elements related to the nation's CI. This executive order paved the way for public and private entities to collaborate on issues of national security, and laid a foundation for the development of PPPs between CI and the government. Issued in 2001, Executive Order 13231 ("Critical Infrastructure Protection in the Information Age") focused more on protecting the operation of information systems important to CI.[14] Aside from highlighting the importance of CI information, the executive order also discussed the use of PPPs to enhance the security and protection of CI. Significantly, this executive order proclaimed the importance of the information systems that underpin CI and catalyzed the focus on the security of these systems.

The CI systems underpinning the economy and society are complex and diverse. They include widely distributed networks, embody a variety of operating models and ownership structures, and many times function both in a physical and cyberspace capacity.[15] Additionally, CI has complex governance structures that include varied regulations, responsibilities, and authorities.[16] Since much of the CI (e.g. finance, utilities, and transport) is owned and/or operated by the private sector, the state cannot be the sole actor responsible for ensuring its protection and security. In the United States, maintaining CI security is considered a "shared responsibility between the federal, state, local, tribal, and territorial entities, and public and private operators of critical infrastructure."[17] Due to the extensive and profound risks associated with a potential breach of CI, government and private industry have recognized and accepted the shared responsibility to assure its protection against security threats, including cyber threats.

Table 6.1 Comparison of FS-ISAC, FSSCC, and FSARC.

Industry group	Founded	Purpose	Membership
Financial Services Information Sharing and Analysis Center	1999	Information sharing	Organizations across the financial services sector (e.g. insurance, banking, and asset management)
Financial Services Sector Coordinating Council	2003	Policy coordination and critical infrastructure protection	Organizations that provide critical financial services including utilities, plus trade associations
Financial Systemic Analysis and Resilience Center	2016	Resilience and systemic risk	Limited to organizations within the financial services sector designated as critical infrastructure

The cybersecurity of CI has thus become a priority for both the public and private sectors. The shared responsibility of the state and private industry – with the state responsible for providing national security and private industry responsible for ensuring protection of the provision and operation of critical services – has resulted in the widespread use of PPPs to drive cybersecurity efforts. The FSS, in particular, has witnessed numerous PPPs in the area of cybersecurity. The next sections explore three of these partnerships in depth: the FS-ISAC, a well-established operational group; the FSSCC, a policy coordination body; and the FSARC, a newly established industry group. We discuss each organization's origins, purpose, membership/constituency, relationship to government, and (when they exist) notable accomplishments (Table 6.1).

6.3 Financial Services Information Sharing and Analysis Center

The FS-ISAC was created in 1999 in response to Presidential Decision Directive 63 (PDD-63), released in 1998.[18] The directive strongly encouraged CI industries to create private sector information sharing and analysis centers (ISACs) to gather, analyze, and share private sector information with other industry members and with the National Infrastructure Protection Center (NIPC), the unit of the government that – until its elimination in 2003 – was responsible for protecting computer and information systems of CI.[19] FS-ISAC's purpose, operations, and organizational structure were highly influenced by the operational concepts and high-level institutional framework outlined in PDD-63.

The directive outlined two main concepts that would shape the purpose and structure of FS-ISAC. In regards to the purpose, the directive called for a clear and mutual communication channel between the NIPC and the ISAC created by each CI industry. As a reciprocal communication mechanism, FS-ISAC was designed by the FSS to be both a receiver and contributor of information about physical and cybersecurity vulnerabilities, intrusions, threats, and anomalies between government and industry. As a result, the FSS uses FS-ISAC to create and disseminate information to members, as much as to collect and ingest information. Importantly, the directive mandates that an analysis and information sharing center cannot interfere with the exchange of information between private sector companies and government agencies. Considering that the FSS is in constant contact with federal and state regulatory agencies, it was important to design FS-ISAC such that its analysis and information-sharing operations did not infringe upon or emulate regulatory communications.[20]

As for structure, PDD-63 suggested that industry-specific ISACs model themselves on institutions deemed effective at information exchange with private and nonfederal sectors. The directive gave the Center for Disease Control and Prevention (CDC) as a model primarily because of its efficacy at communicating, analyzing, and reporting on different initiatives. In response to this suggestion, FS-ISAC adopted a technical focus with objectives outside regulatory and law-enforcement requirements. The directive also noted that the effectiveness of an industry-specific ISAC would depend on its capability to develop statistics and patterns across its objectives as well as on its ability to become an instrument for collecting data and sharing information within and among industry and government stakeholders.[21]

With PDD-63 largely informing its purpose and structure, FS-ISAC has evolved as the financial industry's main resource for sharing and analyzing physical and cyber "threat intelligence."[22] It operates as a member-owned nonprofit entity with a membership base of over 7000 financial services institutions as of 2016.[23] FS-ISAC's Community Institution and Associations (CIA) membership, which includes credit unions, has increased from 231 members to more than 3800 community institutions between 2014 and 2017.[24] FS-ISAC membership extends across different areas of the FSS, including financial institutions, insurance companies, utilities, payment processors, pension funds, and more. These members and partners also extend across regions including North and South America, Europe, the Middle East, and Asia Pacific. Though FS-ISAC has always had members with global operations, it was not until 2013 that board members approved sharing information with financial services firms worldwide.

FS-ISAC membership is recommended by several US federal agencies including the Department of Homeland Security (DHS), the Treasury Department, and the Office of the Comptroller of the Currency (OCC). This recommendation from multiple federal agencies demonstrates the buy-in from

the government and delineates the collaborative nature of the relationship between these entities. In particular, the Treasury Department and the DHS heavily rely on FS-ISAC to quickly disseminate critical information to the sector during crises. US state and local government agencies and law enforcement also use FS-ISAC to communicate physical and cyber threat information and alerts. In addition to closely collaborating with US government and law-enforcement organizations, FS-ISAC also increasingly works with international government entities, regional computer emergency response teams (CERTs), and computer security incident response teams (CSIRTs) to meet international member requirements.[25]

FS-ISAC is particularly focused on providing anonymous information-sharing capabilities across the entire sector. Its main purpose is to disseminate information about current physical and cyber threats in a timely and organized manner to industry members and government. It constantly works to gather reliable information from its members, as well as from other financial service providers, security firms, law enforcement, and government agencies.[26] FS-ISAC fulfills its information-sharing purpose by maintaining a database where members voluntarily report information about vulnerabilities, threats, incidents, and solutions.[27] This data is only accessible to members and is used to develop trend and benchmark information for members. Though FS-ISAC operations primarily focus on communicating current and existing threats, FS-ISAC also conducts research on these threats and breaches. The research and communication operations are organized into different focus areas such as consumer payments, wholesale payments, or destructive malware.[28] In addition to research, FS-ISAC runs simulated cybersecurity exercises related to different FSS operations. For example, in 2013, FS-ISAC conducted a two-day simulated exercise related to payment, Automated Clearing House (ACH), and online banking processes deployed by banks and credit unions. This exercise enabled participating member institutions to experience realistic breach and threat scenarios, in order to train and test critical incident response practices. These exercises are often conducted in coordination with the Treasury Department and are designed to improve the attack responses of participating members.

FS-ISAC's accomplishments have centered on improving the collection, distillation, and communication of threat intelligence to member organizations and partners. Most of these accomplishments have resulted from increasing partnerships with national and international government agencies, developing ventures with FSS vendors and software providers, and establishing separate but connected organizations to improve specific aspects of communicating and assessing threat intelligence.

One such accomplishment is Soltra, the joint venture between FS-ISAC and the Depository Trust & Clearing Corporation (DTCC), a provider of post-trade market infrastructure. Created in 2014 with the support of the DHS, Soltra was built

to improve the speed and security of threat intelligence information sharing between companies.[29] The name Soltra refers to a beacon fire network used to warn communities of invaders in medieval Europe.[30] As the name implies, the joint venture was designed to transfer information to a vast number of organizations for their own use. Soltra Edge was the "first industry-driven threat intelligence sharing platform designed to enable community-driven cyber defense."[31] After operating from 2014 to 2016, Soltra was sold to NC4 in November 2016.[32]

One of FS-ISAC's most notable accomplishments, Sheltered Harbor, resulted from internal efforts to create a different entity to address a specific component of cyber threat within the sector. A limited liability company (LLC) within FS-ISAC, Sheltered Harbor exclusively focuses on strengthening the sector's resilience to a major cyberattack.[33] Created in 2016, Sheltered Harbor allows financial institutions to safely store and quickly reconstitute customer data following an attack. It also allows a customer to access their own data through other financial institutions, in case the customer's bank suffers an attack and is unable to recover quickly.[34] The idea for Sheltered Harbor arose from the "Hamilton Series" of cybersecurity simulations between the private and public sectors (named after Alexander Hamilton, the first Treasurer of the United States).

The Sheltered Harbor operational model of mutual assistance in case of a damaging attack exemplifies the partnerships present within the FSS. While the financial industry competes on nearly every front, from customers to service, it organizes and collaborates on issues of cybersecurity. Similarly, the relationship between the FSS and government in matters of business operations and regulatory requirements is rigid and wary. However, in the case of cybersecurity, close collaboration and partnership is favored. This collaboration is clear through the many partnerships FS-ISAC has formed with different government agencies, both national and international. In 2015, FS-ISAC came to an arrangement with the Federal Reserve Banks to provide over 10 000 of their financial institution members with direct access to security threat information.[35] The partnership is meant to strengthen the communications between this part of the government and the sector by allowing the Federal Reserve Banks to provide FS-ISAC members with access to their Weekly Risk Summary Report, which outlines significant security threats.

As for efforts to strengthen collaboration between the FSS and international government bodies, FS-ISAC has signed memoranda of understanding and agreed to more deeply engage in threat information sharing. In 2016 alone, FS-ISAC signed a memorandum with the European Banking Federation (EBF) to intensify threat information sharing between financial institutions based in Europe and those in the Americas, Asia Pacific, and other regions.[36] The main goal of the cooperation is to increase the resilience of the FSS at a global level through "regional threat advisories, working groups, and sharing mechanisms."[37] FS-ISAC's focus on partnerships with international organizations and governments demonstrates the need to improve collaboration in order to

better analyze, mitigate, and recover from cyber threats. Similar to the memorandum with EBF, FS-ISAC and the Monetary Authority of Singapore (MAS) agreed to establish an Asia Pacific Regional Intelligence Center to improve information sharing and analysis for the FSS within the region.[38] The center, launched in late 2017, is run by FS-ISAC but will primarily focus on building robust intelligence gathering, sharing, and analysis for regional financial institutions.

Members of FS-ISAC realized the need for an organization specifically focused on longer-term threat analysis, to complement FS-ISAC's focus on enhancing real-time threat information sharing, response to cyberattacks, and international cooperation. Since FS-ISAC primarily occupies itself with real-time information sharing and analysis, successful resilience-building across the FSS also requires an organization that is more strategic and deliberately focused on long-term analysis, strategy, and response. To fill this gap, FS-ISAC members formed the FSARC, the mission of which is to "proactively identify, analyze, assess and coordinate activities to mitigate systemic risk to the United States financial system."[39] This new organization is explored in depth below, following a discussion of the FSSCC.

6.4 Financial Services Sector Coordinating Council

The FSSCC was established in 2002. It is the main policy coordination and planning entity through which the sector collaborates with the Treasury Department and other government agencies to address security and resilience.[40] The FSSCC is a self-organized, self-run, and self-governed entity that uses its collaborative relationship with the federal government to provide members with a channel to promote and shape government efforts and policies on security and resilience – areas increasingly dominated by cybersecurity issues. A year after the FSSCC was formed, the Homeland Security Presidential Directive 7 (HSPD-7) established a national policy for federal agencies to "identify and prioritize critical infrastructure" to better protect these industries.[41] HSPD-7 more clearly defined the role of the Treasury Department as the sector-specific federal agency responsible for facilitating vulnerability assessments and encouraging risk-management strategies for the FSS.

In addition to addressing the need for improved security and resilience outlined in HSPD-7, the FSSCC also seeks to fulfill the national efforts indicated in Presidential Policy Directive 21 (PPD-21), released in 2013. PPD-21 called for the clarification of government and industry relationships in regards to physical and cyber threats by enhancing PPPs.[42] It outlined a PPP framework in which the private sector would work with sector-specific agencies (such as the Treasury Department in the case of the FSS) to address and mitigate risks, threats, and vulnerabilities. In turn, these agencies would coordinate and

support DHS analysis and reporting requirements around CI security and resilience. HSPD-7 provided a basic outline of the federal government's responsibilities in developing a collaborative relationship with the private sector, while PPD-21 clarified the role of the DHS in coordinating efforts and providing strategic guidance for CI security and resilience. As a result, the FSSCC maintains a strong partnership with the Treasury Department and the DHS, with the goal of "identifying, prioritizing, and coordinating the protection of critical infrastructure and key resources" and of "facilitating the sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices."[43]

Membership in the FSSCC is open to nongovernmental organizations within the sector. However, membership is limited to financial institutions considered CI – institutions that are systemically significant, with operations that broadly affect financial services operations and infrastructure.[44] Given the CI restriction, FSSCC membership is much smaller than that of FS-ISAC. The 70 members include financial utilities, trade associations, insurance providers, banks, and other financial institutions. Membership is predominantly composed of US organizations and those subject to US regulatory oversight and requirements.[45] International organizations that have a significant effect on United States and global operations, and that provide services widely used across the FSS, are also eligible to apply for membership. Aside from these core members, as of 2017 the FSSCC has an additional 64 volunteer member associations and financial institutions, including clearinghouses, credit rating agencies, financial advisory services, insurance companies, government-sponsored enterprises, information-sharing organizations, and electronic payment firms.[46]

The FSSCC's mission is to strengthen the resilience of the sector against physical and cyber threats by serving as the sector's main tool to communicate and collaborate with US federal government agencies. The FSSCC drives collaboration with the US federal government to proactively identify threats and to promote preparedness and protective measures for the sector. Arguably, the most important role of the FSSCC is to advocate for the interests of the sector as it relates to cybersecurity policy. As the main method of communicating and collaborating with the government, the FSSCC provides a unique mechanism for financial firms considered CI to provide their perspectives on the cyber policies and frameworks developed by the federal government. In practice, the organization seeks to inform the federal government of the sector's specific needs and pain points in regards to physical, and more importantly, cyber threats so that policy is developed with industry perspective and input.

Much of what the FSSCC does is "improve the content and process of bi-directional threat information sharing."[47] As a major enhancement to bi-directional threat information sharing, the FSSCC created an Intelligence Community (IC) Coordinator meant to facilitate the coordination of classified interactions with the federal IC. The IC Coordinator position was created to

maintain and expand the FSS's influence on government agencies in cyber policy matters. The sector already has a well-established partnership with the Treasury Department and the DHS through FS-ISAC, so the FSSCC IC Coordinator is largely focused on increasing and improving information sharing with other partners, such as the FBI Cyber Crime Division.

Along with improving threat information sharing through stronger government partnerships, the FSSCC seeks to increase government research, development, and policy efforts that support the improvement of security and resilience in the sector. The FSSCC uses lobbying, letter writing, and press releases to voice the sector's opinions and to influence government actions as they relate to cybersecurity and resilience. For example, in January 2017, the FSSCC released a letter containing cybersecurity priorities and recommendations in response to the new presidential administration and Congress.[48] The campaign focused on several areas of improvement, including risk-based research and development, cybersecurity regulation, global deterrence, and cyber event response.[49]

Many of FSSCC's public letters and press releases mention the need for more government investment in risk-based research and development related specifically to the FSS. The FSSCC has advocated for stronger federal resourcing within the IC for programs that detect and analyze cyber threats as well as contingency planning and cyber event exercises. An additional FSSCC advocacy priority is a clearer and more holistic approach to federal and state cybersecurity regulation. In their January 2017 letter to the new presidential administration and Congress, FSSCC members called for more coordinated cybersecurity regulation – based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework – that would reduce the number of divergent proposals, mandatory guidelines, and frameworks that federal and state governments release.[50] The FSSCC is also encouraging the government to develop a consistent data protection and breach notification law across national and state platforms, in order to reduce the burden of translating and mapping legal requirements to the current frameworks they have in place.[51] The FSSCC's call for more consistent and holistic cyber regulation was endorsed by a report on "Securing and Growing the Digital Economy," released by the Commission on Enhancing National Security (established by President Obama's Executive Order 13718). The report, completed in December 2016, outlined short- and long-term recommendations for strengthening cybersecurity in the public and private sectors.

Aside from collaborating with the Treasury Department and the DHS, the FSSCC also works with the Financial and Banking Information Infrastructure Committee (FBIIC). The FBIIC was created in 2001 by federal financial regulators in order to address the resilience of the financial sector, promote PPPs, and improve the communication and coordination of financial regulators.[52] The FBIIC consists of 18 federal and state financial regulatory organizations, including the OCC, the Securities and Exchange Commission (SEC), the Federal

Reserve Board (FRB), and others.[53] Members of the FBIIC meet monthly to work on operational and strategic issues related to CI, including cybersecurity. These monthly meetings inform the strategic and policy-level direction of the FBIIC, especially with regards to removing information-sharing obstacles, identifying best practices for cybersecurity controls, and improving incident-response planning. The FBIIC and FSSCC often hold joint meetings to promote discussion of regulatory harmonization and public–private collaboration on addressing legal barriers to information sharing, as well as to collectively discuss cyber threat, risk, and communication initiatives in the sector.

In addition to partnering with the FBIIC, the FSSCC collaborates with the Federal Financial Institutions Examination Council (FFIEC), the interagency body that prescribes standards and principles for federal examination of the FSS.[54] Through the FFIEC, regulators are able to make recommendations to promote uniformity in the regulation and supervision of financial institutions in various areas including cybersecurity.[55] In 2015, the FFIEC released the Cybersecurity Assessment Tool (CAT) to support financial institutions in their identification and analysis of cyber risk, preparedness, and response capabilities.[56] While use of the CAT is not mandatory, it is highly recommended by FFIEC regulators, resulting in its wide adoption and incorporation throughout the sector. In response, the FSSCC created an automated tool to facilitate the collection and scoring of firms' responses to the CAT (Table 6.2).

Table 6.2 FBBIC membership.

Financial and Banking Information Infrastructure Committee	
American Council of State Savings Supervisors	Federal Reserve Bank of New York
Commodity Futures Trading Commission	Federal Reserve Board[a]
Conference of State Bank Supervisors	National Association of Insurance Commissioners
Consumer Financial Protection Bureau[a]	National Association of State Credit Union Supervisors
Department of the Treasury	National Credit Union Administration[a]
Farm Credit Administration	North American Securities Administrators Association
Federal Deposit Insurance Corporation[a]	Office of the Comptroller of the Currency[a]
Federal Housing Finance Agency	Securities and Exchange Commission
Federal Reserve Bank of Chicago	Securities Investor Protection Corporation

[a] Also member of FFIEC.

6.5 Financial Systemic Analysis and Resilience Center

The FSARC was created in June 2016 after eight CEOs of the largest US banks[57] decided to improve the cyber capabilities of CI within the FSS.[58] The FSARC was established under FS-ISAC so as to better partner and collaborate with FS-ISAC members and the US government, including the Treasury Department, the DHS, the FBI, and others.[59] The FSARC's mission is "to proactively identify, analyze, assess and coordinate activities to mitigate *systemic risk* to the US financial system" (emphasis added).[60] While FS-ISAC focuses on real-time analysis and information sharing of cybersecurity threats, the FSARC takes a long-term strategic approach to improving cybersecurity capabilities at the sector and firm level. FSARC operations are not meant to replace FS-ISAC initiatives, but are intended to fill a perceived gap in the analysis of threats that affect the sector. Prior to the FSARC, there was no organization that carried out analysis specifically focused on assessing current and future cybersecurity threats with the purpose of improving sector-wide defense capabilities. Part of the FSARC's mission is to "identify ways to enhance the resilience of the critical infrastructure that underpins the US financial system," which entails identifying and analyzing systemic sector risks.[61]

Since the FSARC operates under FS-ISAC, it is able to collaborate with FS-ISAC members and government partners. The FSARC is also able to use the cybersecurity threat intelligence identified through FS-ISAC operations and its government partners for a deeper analysis of identified threats. Ultimately, the eight bank CEOs envisioned the FSARC as a mechanism to reduce the systemic risk of the FSS and as a way for CI to collaborate to understand the sector's evolving threats and develop better defenses.[62] Because the FSARC is focused on systemic risk to CI, it is led by FSS companies that the federal government has designated as "most crucial to national safety, security, and economic integrity."[63]

The FSARC was created around the time federal regulators released cybersecurity draft rules that required the FSS to recover critical business functions within two hours of a cyberattack.[64] Though the FSARC was not a response to these draft rules, its creation clearly accompanies the increased focus of the public and private sectors on cyber defense capabilities. The FSARC was designed to provide "contextualized and in-depth analyses of long and short term cyber threats," with more of a "hands-on perspective" than government or information-sharing organizations.[65] The creation of the FSARC also demonstrates the FSS's increased focus on the systemic risk facing the US financial system.[66]

The FSARC's prevention, detection, and mitigation tactics are meant to complement already established partnerships across the private and public sectors, such as FS-ISAC and FSSCC, creating a stronger connection and coalition between the different FSS PPPs. Similar to the FSARC is the National Cyber-Forensics & Training Alliance (NCFTA), a nonprofit focused on

real-time information sharing and analysis of cyber threats. Founded in 2002, the NCFTA is focused on identifying, mitigating, and neutralizing cyber threats at a global level.[67] The NCFTA collaborates with subject-matter experts in the private, public, and academic sectors to proactively identify cyber threats and determine the best preventive measures to mitigate such threats.[68] While the NCFTA is not primarily focused on systemic threats facing the US financial system, it shares the FSARC's focus on best practices to mitigate threats through response planning efforts and threat analytics.

As of 2018, the FSARC has three main focus areas: intelligence collection, advanced analytics capabilities, and sharing of workforce resources with government. In collecting actionable intelligence, the FSARC seeks to identify the most critical elements and operations of the US financial system so that the gathering of intelligence can be focused on cyber threats that pose the greatest systemic risk.[69] Leaders of the FSARC argue that while government agencies are good at collecting threat intelligence, they do not necessarily have the sector-specific expertise required to contextualize and determine the motivation of attacks, assess the importance of threats to the systemic operations of the sector, or identify trends in the sector's vulnerabilities. Members of the FSARC also want to engage with government to prioritize the collection of threat intelligence in order to develop a more organized approach to sourcing.[70]

While most of the industry-led organizations work to improve PPPs in the areas of policy making and information sharing, the FSARC is also meant to enhance the sharing of advanced analytics between the private sector and government.[71] More specifically, it wants to include machine learning, artificial intelligence, and the coordination of operations in its partnership with federal government agencies.[72] Additionally, FSARC members would like the government to use the organization to coordinate public–private cyber defense operations and measures to drive broader cyber deterrence.[73] The FSARC is also advocating for the government to assign a dedicated and shared workforce of government employees to the FSARC mission of improving FSS CI security.

6.6 Lessons for Cybersecurity Governance

Having reviewed the varied roles and functions of FS-ISAC, FSSCC, and the FSARC, what are some of the lessons for cyber governance emanating from the financial sector's experiences in creating and cultivating PPPs? While the lessons are potentially innumerable, we will focus on three key observations here:

6.6.1 Lesson One: Affirmation of PPP Model, but Focus and Clarity Needed

The FSS's experience with cyber partnerships demonstrates their effectiveness in addressing complex challenges, including operational (FS-ISAC), policy

(FSSCC), and increasingly strategic (FSARC) challenges. It is clear that neither government nor industry is capable of achieving cybersecurity on its own. Industry leaders must work together through mechanisms like FS-ISAC to identify and respond to ongoing threats. Industry must also be able to rely on government partners when necessary, as in moments of crisis (e.g. sector-wide Distributed Denial of Service [DDoS] or catastrophic destructive malware attacks). Industry and government must collaborate in order to develop and implement cyber policy that is fit for its purpose and does not unintentionally harm firms' cyber defenses. Likewise, industry must increasingly rely on government partnerships to provide insights into the strategic cyber threats facing the sector, particularly with respect to systemic risk.

Though cooperation among PPPs highlights the shared purpose and interest of government and private industry in pursuing common goals like cybersecurity, at times the roles and responsibilities assigned to each set of actors in these partnerships may appear ambiguous. PPPs within cybersecurity typically avoid directly assigning strict responsibility and accountability. Instead, the governance practices resulting from these partnerships can be unclear and often revert back to legacy governance and relationship structures between government and industry (e.g. what can government do for industry?). This is particularly clear in the FSS, where government has often taken the role of a regulator.

Moreover, with the expansion of PPPs and the formation of new initiatives like FSARC, there is a risk that the respective roles and responsibilities of each organization may become confused. Tight coordination among organizations tasked with facilitating partnerships will become increasingly necessary to maintain focused objectives and eliminate duplicative or wasteful effort.

6.6.2 Lesson Two: Addressing Systemic Risk Requires more than Just Information Sharing

FS-ISAC is considered a highly successful venture and an Information Sharing and Analysis Organization (ISAO) *par excellence*. It is widely viewed as one of the premiere industry cybersecurity organizations and a leading example of an effective ISAC. However, the increasing cyber threat demands more focused analysis of longer-term strategic trends, as well as tighter industry–government coordination, particularly for highly interconnected CI sectors.

It is one thing for each CI organization within a sector to strengthen its own cyber defenses and to share information about day-to-day incidents, but underlying systemic risks may persist. Critical third parties and essential utilities must be a part of the cyber risk calculus when identifying and addressing these systemic risks. This is where constructs like the FSARC enter the fray to fill an important gap.

One challenge in this respect is how to scale constructs like the FSARC internationally, particularly where engagement with national intelligence

organizations may be required. Financial systemic risks are more often than not international in scope, but the international sharing of sensitive intelligence and analytics about these risks is not yet commonplace.

6.6.3 Lesson Three: Limitations of PPPs in Regulated Industries

As noted in the introduction, the FSS has experienced a tidal wave of new regulation and policy focused on cybersecurity risk. While well intended, this has created an unfortunate situation in which financial institutions are left to reconcile differing regulatory approaches, both domestically and internationally. Industry groups, including the FSSCC in the United States, have sought to engage regulators to harmonize and align their efforts, but this has proven challenging so far.

Looking beyond the world of finance, other highly regulated industries may soon experience similar challenges. This demonstrates a potential limitation of the PPP model, in cases where government partners are regulators with different incentives than nonregulatory government agencies, and with a perceived disinterest in collaboration.

6.7 Conclusion

In this chapter, we provided a deep dive into three key FSS-led organizations that facilitate PPPs for cybersecurity across different specialty areas. We also drew out broader lessons for cyber governance, with attention to the value and limitations of the PPP model, the need to advance beyond information sharing to address the cyber threat, and the complexities of relying on PPPs for security governance in regulated sectors. We hope that these insights aid both scholars and policymakers in better understanding the benefits and challenges associated with organizing the public and private sectors around shared goals like cybersecurity.

This chapter also raises interesting questions that merit further research, particularly around the effectiveness of sector-led international partnership on security matters. It also exposes the need for a better understanding of how regulatory environments shape PPPs, particularly in the domain of cybersecurity.

Acknowledgments

The authors would like to thank Deanna Girani for her support during the drafting of this chapter. As a member of the Global Data Justice project at Tilburg University, Aaron Martin has received funding from the European Research Council under the European Unions Horizon 2020 research and innovation programme (Grant Agreement n° 757247).

Notes

1 Susan V. Scott and Markos Zachariadis, *The Society for Worldwide Interbank Financial Telecommunication (SWIFT): Cooperative Governance for Network Innovation, Standards, and Community*, Routledge Global Institutions Series (London: Routledge, 2013).
2 Kim Zetter, "That Insane, $81M Bangladesh Bank Heist? Here is What We Know," *Wired*, May 17, 2018, https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know.
3 Ibid.
4 Jim Finkle, "Exclusive: SWIFT Discloses More Cyber Thefts Pressures Banks on Security," *Reuters*, August 31, 2018, http://www.reuters.com/article/us-cyber-heist-swift-idUSKCN11600C.
5 Ibid.
6 Greg Baer and Rob Hunter, "A Tower of Babel: Cyber Regulation for Financial Services," *The Clearing House*, June 9, 2017, https://www.theclearinghouse.org/banking-perspectives/2017/2017-q2-banking-perspectives/articles/cyber-regulation-for-financial-services.
7 But for case studies of ChicagoFIRST and FSSCC, see: Brian S. Tishuk, "Effectively Managing Partnership Evolution: A Case Study from Chicago," *Journal of Business Continuity & Emergency Planning* 6, no. 2 (2013): 111–121.
8 OECD, "Governance," last modified July 23, 2007, https://stats.oecd.org/glossary/detail.asp?ID=7236.
9 Gerry Stoker, "Governance as Theory: Five Propositions," *International Social Science Journal* 155 (1998): 17–28.
10 Joseph J. Romm, *Defining National Security: The Nonmilitary Aspects* (New York: Council on Foreign Relations Press, 1993).
11 OECD, "The Development of Policies for the Protection of Critical Information Infrastructure," *OECD Ministerial Background Report,* 2007.
12 Ibid.
13 Executive Office of the President. Executive Order 13010 (July 15, 1996). "Critical Infrastructure Protection." https://www.gpo.gov/fdsys/pkg/FR-1996-07-17/pdf/96-18351.pdf.
14 Executive Office of the President. Executive Order 13231 (October 16, 2001). "Critical Infrastructure Protection in the Information Age." https://www.gpo.gov/fdsys/pkg/FR-2001-10-18/pdf/01-26509.pdf.
15 Presidential Policy Directive/PPD-21 (February 12, 2013), "Critical Infrastructure Security and Resilience," https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
16 Ibid.
17 Ibid.

18 FS-ISAC, "Mission," https://www.fsisac.com/about/mission.
19 Presidential Decision Directive/PDD-63 (May 22, 1998), "Critical Infrastructure Protection," https://fas.org/irp/offdocs/pdd/pdd-63.htm.
20 Ibid.
21 Ibid.
22 Threat intelligence is a term of art, which Gartner defines as: "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging threat to an organization or its assets." Gartner, "Definition: Threat Intelligence." May 16, 2013, https://www.gartner.com/doc/2487216/definition-threat-intelligence.
23 FS-ISAC, "FS-ISAC Community Institution and Association Membership Grows 3,800 Members. Heather McCalman Joins as Credit Union Council Manager," March 22, 2017, https://www.fsisac.com/sites/default/files/news/FS-ISAC_Press_Release_Community_Inst_3-22-2017_Final.pdf.
24 Ibid.
25 FS-ISAC, "Membership Benefits," https://www.fsisac.com/join.
26 FS-ISAC, "About FS-ISAC," https://www.fsisac.com/about.
27 Sue Eckert, "Protecting Critical Infrastructure: The Role of the Private Sector," University of Pittsburgh Center for International Securities Studies 2005, http://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf.
28 FS-ISAC, "Best Practices for Financial Institutions Reducing Risks Associated with Destructive Malware," November 23, 2015.
29 FS-ISAC, "New Soltra Network Offering to Connect and Coordinate Cyber Threat Intelligence Sharing," October 12, 2014, https://www.fsisac.com/sites/default/files/news/Soltra%20Network%20Press%20Release%20101215%20%28final%29.pdf.
30 Soltra, "The Soltra Story," https://www.soltra.com/en/about.
31 FS-ISAC, "New Soltra Network."
32 NC4, "NC4 to buy cyber threat intelligence company, Soltra, from FS-ISAC, DTCC," November 23, 2016, https://www.fsisac.com/sites/default/files/news/PR-NC4_and_Soltra_Press_Release.pdf.
33 Jeff Stone and Kate Fazzini, "U.S. Financial Sector Begins 'Sheltered Harbor' Rollout," *Wall Street Journal*, March 9, 2017, https://www.linkedin.com/pulse/us-financial-sector-begins-sheltered-harbor-rollout-jeff-stone.
34 FS-ISAC, "Sheltered Harbor," November 23, 2016, https://www.fsisac.com/sites/default/files/news/SH_FACT_SHEET_2016_11_22_FINAL3.pdf.
35 FS-ISAC, "FS-ISAC to Offer Security Threat Information to Over 10,000 Federal Reserve Bank Financial Institution Customers," September 16, 2015, https://www.fsisac.com/sites/default/files/news/FRB-FS-ISAC-Press_Release_Sept_2015FINAL.pdf.
36 FS-ISAC, "European Banking Federation and the Financial Services Information Sharing and Analysis Center (FS-ISAC) Partner on Trans-Atlantic Initiative to Fight Cyber Crime," September 30, 2016, https://

www.fsisac.com/sites/default/files/news/EBF%20and%20FS%20ISAC%20agree%20Trans-Atlantic%20cybercrime%20cooperation.pdf.

37 Ibid.

38 Monetary Authority of Singapore, "FS-ISAC and MAS Establish Asia Pacific (APAC) Intelligence Centre for sharing and analysing cyber threat information," December 1, 2016, www.mas.gov.sg/News-and-Publications/Media-Releases/2016/FS-ISAC-and-MAS-Establish-APAC-Intelligence-Centre.aspx.

39 FS-ISAC, "Preliminary Findings from Latest DDoS Attacks," November 2016, http://iiac.ca/wp-content/uploads/FS-ISAC-SIRG-Cybersecurity-Brief-for-North-America-November-2016.pdf.

40 FSSCC, "About FSSCC," https://www.fsscc.org/About-FSSCC.

41 Homeland Security Presidential Directive 7/HSPD-7 (December 17, 2003), "Critical Infrastructure Identification, Prioritization, and Protection," https://www.dhs.gov/homeland-security-presidential-directive-7.

42 PPD-21, "Critical Infrastructure Security and Resilience."

43 Ibid.

44 FSSCC, "Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security Charter," March 20, 2015, https://www.dhs.gov/sites/default/files/publications/FSSCC-Charter-03-15-508.pdf.

45 FSSCC, "About FSSCC," https://www.fsscc.org/About-FSSCC.

46 FSSCC, "Letter to Senator Warren and Representative Cummings," December 9, 2014, https://www.fsscc.org/files/galleries/FSSCC_12-09-14_Letter_to_Sen_Warren-Rep_Cummings.pdf.

47 FSSCC, "Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security Annual Report 2013-2014," https://www.aba.com/Tools/Function/Cyber/Documents/FSSCCAnnualReport2013-2014.pdf.

48 FSSCC, "Financial Services Sector Cybersecurity Recommendations," January 18, 2017, https://www.fsscc.org/files/galleries/FSSCC_Cybersecurity_Recommendations_for_Administration_and_Congress_2017.pdf.

49 Ibid.

50 Ibid.

51 Ibid.

52 FBIIC, "Mission and History," https://www.fbiic.gov/mission-history.html.

53 FBIIC, "FBIIC Members," https://www.fbiic.gov/fbiic-members.html.

54 The FFIEC is composed of: the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, and the State Liaison Committee.

55 FFIEC, "Federal Financial Institutions Examination Council (FFIEC) About," https://www.ffiec.gov/about.htm.

56 FFIEC, "Cybersecurity Assessment Tool," https://www.ffiec.gov/cyberassessmenttool.htm.
57 Specifically, the CEOs of Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street, and Wells Fargo.
58 JPMorgan Chase & Co., "Annual Report 2016," 2017, https://www.jpmorganchase.com/corporate/investor-relations/document/2016-annualreport.pdf.
59 Ibid.
60 FS-ISAC, "FS-ISAC announces the formation of the Financial Systemic Analysis & Resilience Center (FSARC)," October 24, 2016, https://www.fsisac.com/sites/default/files/news/FS-ISAC%20Announces%20the%20Formation%20of%20the%20Financial%20Systemic%20Analysis%20%28FSARC%29.pdf.
61 Ibid.
62 Michael Chertoff and Frank Cilluffo, "Trump Administration Can Help Finance Sector Shift Cybersecurity Paradigm," *Forbes*, January 18, 2017, https://www.forbes.com/sites/realspin/2017/01/18/trump-administration-can-help-finance-sector-shift-cybersecurity-paradigm/#3b7561db645d.
63 Ibid.
64 "New Financial System Analysis & Resilience Center Formed," *Dark Reading*, October 24, 2016, http://www.darkreading.com/threat-intelligence/new-financial-system-analysis-and-resilience-center-formed-/d/d-id/1327276.
65 Chertoff and Cilluffo, "Trump Administration."
66 JPMorgan Chase & Co., "Cybersecurity: Maintaining Strong Defenses," Vol. 2 (Spring 2017).
67 NCFTA, "Who We Are," https://www.ncfta.net.
68 Ibid.
69 JPMorgan Chase & Co., "Cybersecurity: Maintaining Strong Defenses."
70 Chertoff and Cilluffo, "Trump Administration."
71 Ibid.
72 Ibid.
73 Ibid.