CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

International Strategy to Better Protect the Financial System Against Cyber Threats

TIM MAURER AND ARTHUR NELSON

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

International Strategy to Better Protect the Financial System Against Cyber Threats

TIM MAURER AND ARTHUR NELSON

IN COLLABORATION WITH:

WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

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/pubs.

PREFACE

In February 2016, a few months after Carnegie began its work on this project, a cyber attack shook the finance world.[1] Hackers had targeted SWIFT, the global financial system's main information network, trying to steal 1 billion U.S. dollars, nearly 0.50 percent of Bangladesh's GDP,[2] from the Bangladeshi central bank over the course of a weekend.[3] It was a wake-up call revealing that cyber threats targeting the financial sector were no longer limited to low-level theft but could now pose systemic risk.

Only a few months earlier, in 2015, the Carnegie Endowment for International Peace had launched an initiative to better protect the global financial system against cyber threats.[4] Our first step was to develop a proposal for the G20 to launch a work stream dedicated to cybersecurity in the financial sector.[5] In March 2017, the G20 Finance Ministers and Central Bank Governors outlined an initial road map to increase the cyber resilience of the international financial system. In the wake of the Bangladesh incident, Carnegie expanded its work, complementing the G20 project with the development of an action-oriented, technically detailed cyber resilience capacity-building tool box for financial institutions. Launched in 2019 in partnership with the IMF, SWIFT, FS-ISAC, Standard Chartered, the Global Cyber Alliance, and the Cyber Readiness Institute, this tool box is now available in seven languages.[6] And we are continuing to track the evolution of the cyber threat landscape and incidents involving financial institutions through a collaboration with BAE Systems.[7]

To raise more awareness among senior officials of the growing threat, Carnegie also hosted a series of roundtables at the Munich Security Conference, including a cyber war game, dedicated to cybersecurity and the financial system. We co-hosted a high-level roundtable with the IMF for central bank governors and launched a workshop series at Wilton Park to strengthen the relationships among financial authorities, industry, and law enforcement as well as national security agencies.

In July 2019, an international group—convened by Carnegie—of leading experts in governments, central banks, industry, and the technical community decided that there would be value in developing a longer-term international cybersecurity strategy for the financial system.

This report is the result of that project and offers a vision for how the international community could better protect the financial system against cyber threats. The recommendations are designed to inform the deliberations among the G20, the G7, relevant standard-setting bodies as well as the Annual Meeting of the World Economic Forum and the Munich Security Conference.

Written by Carnegie experts, this document includes feedback obtained through consultations with more than 200 stakeholders in government, the financial regulatory community, industry, and academia. An international advisory group, formed in fall 2019, provided strategic advice throughout the project. In February 2020, following Carnegie's presentation of this project at the Forum's annual meeting in Davos the previous month, the World Economic Forum became an official partner.

CONTENTS

PART I: STRATEGY AND OVERVIEW OF RECOMMENDATIONS

Summary

The global financial system is going through an unprecedented digital transformation, which is being accelerated by the coronavirus pandemic.[8] Financial services firms increasingly look like tech companies and tech companies look like financial services firms. Central banks around the globe are considering throwing their weight behind digital currencies and modernizing payment systems.[9] In this time of transformation, when an incident could easily undermine trust and derail such innovations, cybersecurity is more essential than ever.

Malicious actors are taking advantage of this digital transformation and pose a growing threat to the global financial system, financial stability, and confidence in the integrity of the financial system. Malign actors are using cyber capabilities to steal from, disrupt, or otherwise threaten financial institutions, investors, and the public. These actors include not only increasingly daring criminals,[10] but also states and state-sponsored attackers. North Korea, for example, has stolen some $2 billion from at least thirty-eight countries across five continents over the last five years alone,[11] more than three times the amount of money it was able to generate through counterfeit activity over the previous four decades.[12] Other state-sponsored actors have targeted financial institutions, for example, with massive distributed denial-of-service (DDoS) attacks.[13] More dangerous attacks and ensuing shocks should be expected in the future. Most worrisome are incidents that corrupt the integrity of financial data, such as records, algorithms, and transactions; few technical solutions are currently available for such attacks, which have the potential to undermine trust and confidence more broadly.[14]

Increasingly concerned, key voices are sounding the alarm. In February 2020, Christine Lagarde, the president of the European Central Bank (ECB) and former head of the International Monetary Fund (IMF), warned that a cyber attack could trigger a serious financial crisis.[15] At the 2019 annual meeting of the World Economic Forum (WEF), the head of Japan's central bank predicted that cybersecurity could become the financial system's most serious risk in the near future.[16] Industry executives have echoed these concerns. Jamie Dimon, CEO of JPMorgan Chase, said in April 2019 that cyber attacks "may very well be the biggest threat to the U.S. financial system."[17]

In April 2020, the Financial Stability Board (FSB) cautioned that "cyber incidents pose a threat to the stability of the global financial system." The FSB went on to warn that the last few years have seen "a number of major cyber incidents that have significantly impacted financial institutions and the ecosystems in which they operate. A major cyber incident, if not properly contained, could seriously disrupt financial systems, including critical financial infrastructure, leading to broader financial stability implications."[18] The potential economic costs of such events can be immense and the damage to public trust and confidence significant. Cyber incidents could potentially undermine the integrity of global financial markets;[19] equally important, the exploitation of cyber vulnerabilities could cause losses to investors and the general public. Central to the risk is the fact that the global financial system is a complex adaptive system. It is resilient and able to absorb most of the shocks that regularly occur, but its complexity also means that large shocks, although rare, can quickly ripple in unpredictable ways. The system's complexity also makes it impossible to predict exactly when or how such systemic shocks will occur.[20] But one thing is clear: it is not a question of *if* a major incident will happen, but *when*.

This is a global problem. Malign actors are targeting not only financial institutions in North America, Europe, and other high-income countries; many are also hitting less protected soft targets in low and lower-middle income countries. Although fintech is a buzzword worldwide, the trend toward digital financial services has been particularly pronounced in low and lower-middle income countries, where providing access to financial services to the unbanked is a top priority. The past decade's push toward greater financial inclusion, driven by a massive G20 investment, has led many countries to leapfrog to digital financial services. Although they do advance financial inclusion, digital services also offer a target-rich environment for malicious hackers and present new money laundering risks, providing fertile ground for the full range of transnational criminal activity.

SPOTLIGHT

For a more detailed overview of the evolving threat landscape, see the Carnegie paper, "The Evolution of the Cyber Threat Landscape Targeting Financial Institutions," published alongside this strategy report, as well as Carnegie's "Timeline of Cyber Incidents Involving Financial Institutions," created in association with BAE Systems: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

Surprisingly, despite the global financial system's increasing reliance on digital infrastructure, it is unclear who is responsible for protecting the system against cyber attacks. In part, this is because the environment is changing so quickly. Everybody agrees that the global financial system is critical to society, the global economy, and the recovery from the pandemic. Yet the global financial sector remains vulnerable to cyber threats and, absent dedicated action, will only become more vulnerable as innovation, competition, and the pandemic further fuel the digital revolution. Although many threat actors are focused on making money, the number of purely disruptive and destructive attacks has been increasing; furthermore, those who learn how to steal also learn about the financial system's networks and operations, which allows them to launch more disruptive or destructive attacks in the future (or sell such knowledge and capabilities to others). This rapid evolution of the risk landscape is taxing the responsiveness of an otherwise mature and well-regulated system.

Better protecting the global financial system is primarily an organizational challenge. Unlike many sectors, most of the financial services community does not lack resources or the ability to implement technical solutions. The main issue is a collective action problem: how best to organize the system's protection across governments, financial authorities, and industry and how best to leverage these resources effectively and efficiently. The current fragmentation among stakeholders and initiatives partly stems from the unique aspects and evolving nature of cyber risk. Different communities operate in silos and tackle the issue through their respective mandates. The financial supervisory community focuses on resilience, diplomats on norms, national security agencies on cost imposition, and industry executives on firm- rather than sector-specific risks. As lines between financial services firms and tech companies become ever more fuzzy, the lines of responsibility for security are likewise increasingly blurred.[21]

The disconnect between the finance, the national security, and the diplomatic communities is particularly pronounced. Financial authorities face unique risks from cyber threats, yet their relationships with national security agencies, whose involvement is necessary to effectively tackle those threats, remain tenuous in most countries. The FSB did not include "cyber attack" in its 2018 lexicon of key terms related to cyber security and cyber resilience. The term, with its national security connotations, was considered beyond its mandate and beyond the responsibility of central banks. For their part, security agencies generally prioritize defending against threats at the national level rather than from a global system perspective, and therefore focus primarily on loss of life and physical damage. Nothing explodes when a cyber attack hits the financial sector.

This responsibility gap and continued uncertainty about roles and mandates to protect the global financial system fuels risks. Part of this uncertainty is due to the current geopolitical tensions, which hinder collaboration among the international community. Cooperation on cybersecurity has been hampered, fragmented, and often limited to the smallest circles of trust because it touches on sensitive national security equities. For example, participation in the Cyber Expert Group (CEG) created by the G7 Finance Track in 2016 was limited to G7 member states, whereas the process created by the G7 in 1989 to establish the Financial Action Task Force (FATF) included several non-G7 states from the outset. Yet it is clear that individual governments, financial firms, and tech companies cannot address these challenges alone. International and multistakeholder cooperation is not a "nice-to-have" but a "need-to-have."

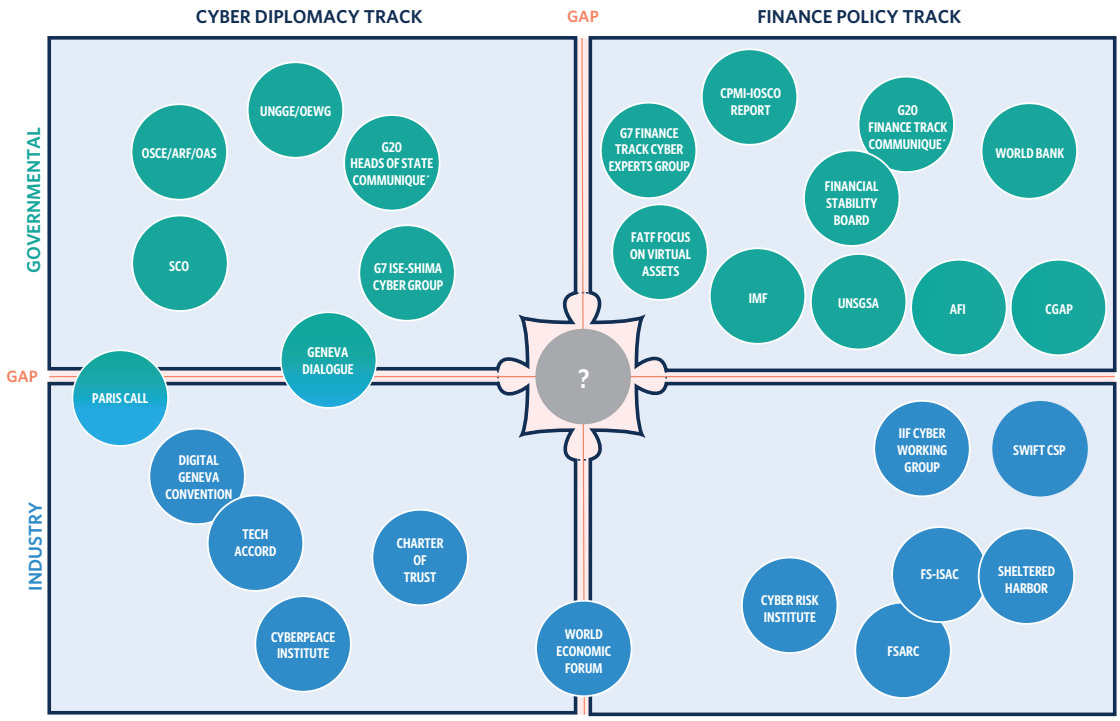
A good illustration of these continuing gaps and the need for greater coordination among the different stakeholders is the G7 itself. Although it has demonstrated international leadership on this issue through the G7 Finance Track's CEG, there is room for improvement. For example, the G7 Finance Track's CEG and the diplomat-led G7 cyber norms group have never met since their creation in 2016, despite clear general synergies and specific crosscutting challenges. Figure 1 illustrates such gaps between the cyber diplomacy and finance policy tracks.

Breaking down silos is a particular challenge for many financial authorities who, in most countries, operate mostly independent of other parts of the state. Cyber threat actors pose a unique type of risk. Many of them operate transnationally and target victims abroad. This requires countries not only to better organize themselves domestically but also to strengthen international cooperation to defend against, investigate, prosecute, and ideally prevent future attacks. This implies that the financial sector and financial authorities must regularly interact with law enforcement and other national security agencies in unprecedented ways, both domestically and internationally.

In sum, these trends, growing concerns, and existing gaps highlight several key points:

- **Greater clarity about roles and responsibilities is required.** The current fragmentation and uncertainty about roles and responsibilities weaken the international system's collective resilience, recovery, and response capabilities. Only a handful of countries have built effective domestic relationships among their financial authorities, law enforcement, diplomats, other relevant government actors, and industry. International cooperation remains limited, partly hampered by the fragmentation.

Figure 1: Gaps Between Cyber Diplomacy and Finance Policy Tracks, 2015–2020



Note: Overlapping indicates that processes/organizations are connected.

- **International collaboration is necessary and urgent.** The threat of cyber disruption has grown and become more aggressive in recent years. Not only criminals but also states are now targeting financial institutions. It is not a question of if a major shock will happen, but when. Given the scale of the threat and the system's globally interdependent nature, individual governments, financial firms, and tech companies cannot effectively protect against cyber threats if they work alone.

- **Reducing fragmentation will free up capacity to tackle the problem.** Many initiatives are underway to better protect financial institutions, but they remain siloed. Some of these efforts duplicate each other, and the diversity of initiatives increases transaction costs. Several of these initiatives are mature enough to be shared, better coordinated, and further internationalized.

- **Protecting the international financial system can be a model for other sectors.** The financial system is one of the few areas in which states have a clear shared interest in cooperation, even when geopolitical tensions are high. An entire international architecture—from the G7 and G20 Finance Tracks to the FSB and the international financial institutions—already exists to drive change. Focusing on the financial sector provides a starting point and could pave the way to better protect other sectors in the future.

Several ongoing initiatives have now reached sufficient maturity and degree of trust among their original members that they could potentially be expanded, strengthened, and coordinated with related efforts. Effective examples of cooperation on issues with a national security dimension do exist; the FATF is a case in point. Candidates for such expansion are the G7 CEG, which has issued several fundamental principles, analyzed systemic risks, and conducted an exercise. The FSB is in the process of updating its cyber lexicon and has finalized its cyber incident response and recovery toolkit, and the Bank for International Settlements (BIS) has established its Cyber Resilience Coordination Centre (CRCC).[22] Industry has also launched new initiatives, such as Sheltered Harbor and the Cyber Defence Alliance (CDA). Individual countries have developed new models, including Singapore's workforce initiatives; Israel's FinCERT; red teaming testing frameworks like the European Union (EU)'s TIBER-EU, Saudi Arabia's FEER, and Hong Kong's iCAST;[23] and the Bank of England's concept of impact tolerances. In September 2020, the European Commission (EC) proposed a Digital Operational Resilience Act (DORA) "to ensure that all participants in the financial system have the necessary safeguards in place to mitigate cyber-attacks and other risks."[24]

To achieve more effective protection of the global financial system against cyber threats, this report, "International Strategy to Better Protect the Global Financial System Against Cyber Threats," outlines thirty-two recommendations and forty-four supporting actions to be implemented ideally in the 2021–2024 timeframe. Figure 2 and Table 1 illustrate how the recommendations and supporting actions are organized into strategic priority areas with three core pillars and three complementary crosscutting issues:

Strategic Priority Areas:

0. ***Strategic Imperative:***

   Clarify roles and responsibilities and create more connective tissue among the various silos and relevant stakeholders.

1. ***Core Pillar #1:***

   Cyber Resilience: Strengthen operational cyber resilience and collective defense to shield the financial sector against cyber threats.

2. ***Core Pillar #2:***

   International Norms: Reinforce international norms at the United Nations and through other relevant processes to clarify what is considered inappropriate behavior—that is, when malicious activity has crossed a line—and hold actors accountable for violations to avoid norms being eroded by impunity.

3. Core Pillar #3:

Collective Response: Facilitate collective response to disrupt malicious actors and more effectively deter future attacks.

4. Crosscutting Issue #1:

Cybersecurity Workforce: Build the cybersecurity workforce required to turn ambitions into actions by assessing and expanding effective models for addressing workforce challenges including limited pipelines and a lack of diversity.

5. Crosscutting Issue #2:

Capacity-Building: Align and expand capacity-building efforts across all three core pillars for those seeking assistance.

6. Crosscutting Issue #3:

Digital Transformation/Financial Inclusion: Safeguard financial inclusion and the G20's achievements of the past decade in this area.

Figure 2: Strategic Framework and Relationship Among Strategic Priorities

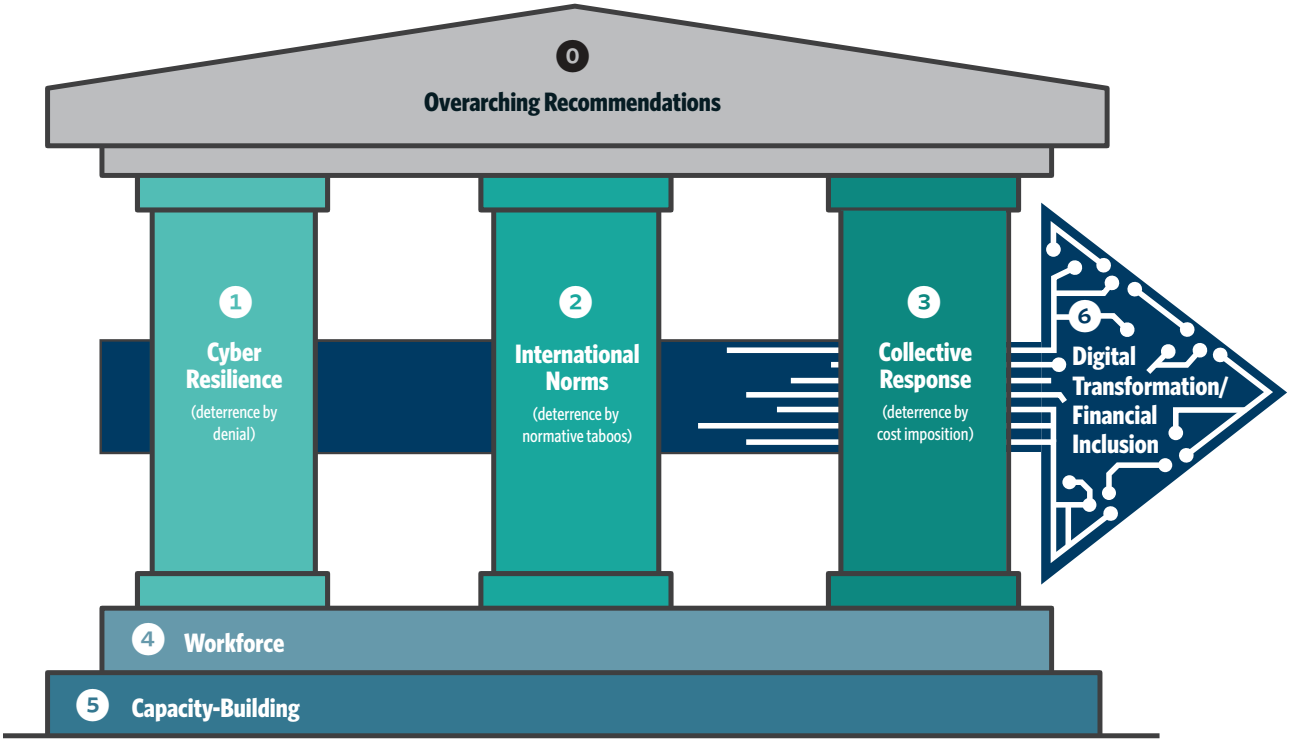


Table 1: Overview of Recommendations and Supporting Actions Across Strategic Priority Areas

Strategic Priority Area	Strategic Imperative, Core Pillars, and Crosscutting Issues	Recommendations and Supporting Actions
	Strategic Imperative	
0	Strategic Imperative	3 Recommendations 1 Supporting Action
	Core Pillars	
1	Core Pillar #1: **Cyber Resilience**	7 Recommendations 17 Supporting Actions
2	Core Pillar #2: **International Norms**	4 Recommendations 9 Supporting Actions
3	Core Pillar #3: **Collective Response**	7 Recommendations 4 Supporting Actions
	Crosscutting Issues	
4	Crosscutting Issue #1: **Workforce**	3 Recommendations 7 Supporting Actions
5	Crosscutting Issue #2: **Capacity-Building**	4 Recommendations 3 Supporting Actions
6	Crosscutting Issue #3: **Financial Inclusion**	4 Recommendations 3 Supporting Actions

Overarching Recommendations

The following overarching recommendations focus on creating the foundation for stronger coordination among the various actors and for the implementation of the specific recommendations across the six priority areas:

- **Recommendation 0.1:** G20 heads of state should create interagency processes within their respective governments, co-led by the ministry of finance and the central bank/monetary authority (or other relevant entity representing the government in international finance bodies), to explore options for better protecting their domestic as well as the international financial system against cyber threats. Ideally these processes will focus on the six priority areas identified in this report and take into account the report's recommendations. (The co-leadership is designed to avoid disruptions caused by the frequent turnover of politically appointed ministers of finance; including central banks/monetary authorities as co-leads will allow greater continuity of effort.)

    - *Supporting Action 0.1.1:* To help increase trust and confidence, G20 Finance Ministers and Central Bank Governors should consider creating a G20 Finance Track process emulating the confidence-building

measures undertaken by the member states of the Organization for Security and Co-operation in Europe (OSCE), which includes the United States and Russia. (The supplementary background report provides more details about measures the G20 could explore.)

- **Recommendation 0.2:** Financial services firms should expand their engagement and dedicate more resources to strengthening the protection of the sector overall. In particular, firms should support capacity-building efforts for weaker links in the system and become more active in efforts complementary to firms' core focus on resilience, such as advancing international norms, facilitating collective response, and tackling workforce challenges.

- **Recommendation 0.3:** G7 Finance Ministers and Central Bank Governors should renew the mandate of the G7 CEG starting in 2021; the mandate should include expanding the number of participant states and initiating a G7+ process, for example, emulating the one that established the FATF in the early 1990s, or another process for involving members outside its current remit. (In addition to the European Commission, which is already included, this expanded group could include financial centers such as Switzerland and Singapore and other relevant partner countries. Appendix A provides an outline of stakeholders that could be included in such an enlarged process.)

Specific Recommendations for Each Priority Area

Priority #1, "Cyber Resilience": Focus on the Unique Nature of Cyber Threats

Core Pillar #1: *Strengthen operational cyber resilience and collective defense to shield the financial sector against cyber threats.*

The global financial system's operational cyber resilience and collective defense against cyber attacks is the foundation for any comprehensive strategy. This first core pillar provides protection not only against potential cyber attacks but also against accidental failures. National security officials would view such resilience as a means of deterrence by denial. A particular challenge looking ahead will be to ensure that the increasing emphasis on broader operational resilience does not detract attention from the unique aspects of cybersecurity risks—in particular, the risk that nefarious actors will specifically

target financial institutions and the need to create the mechanisms to effectively protect against such threats.

The recommendations focus on (i) ensuring that the shift to a broader conception of operational resilience does not eclipse the need to prepare for the specific risks of malicious cyber attacks; (ii) outlining innovative initiatives that could be emulated; and (iii) highlighting significant issues that demand specific attention.

- **Recommendation 1.1:** Standard-setting bodies—namely the Basel Committee on Banking Supervision (BCBS), the Committee on Payments and Market Infrastructures (CPMI), the International Organization of Securities Commissions (IOSCO), and the International Association of Insurance Supervisors (IAIS)—should continue to support initiatives to improve and align regulatory oversight efforts for the cybersecurity and operational resilience of financial services. This will contribute to higher quality security practices among financial firms by reducing regulatory transaction costs and freeing up bandwidth among firms' cybersecurity staff.

    - *Supporting Action 1.1.1:* The G20 should task the FSB with developing a baseline framework for the supervision of cyber risk management at financial institutions. This framework should leverage common risk management frameworks, such as those advanced by the Financial Stability Institute and the Financial Services Sector Cybersecurity Profile, as well as internationally accepted standards for technology and risk controls.

- **Recommendation 1.2:** Governments (starting with the G7 and G20 Finance Ministers and Central Bank Governors) and industry should expand and strengthen the international ecosystem of financial sector-focused computer emergency response teams (CERTs) or similar entities to stimulate public-private collaboration and strengthen sector-specific security.

    - *Supporting Action 1.2.1:* Governments should create a FinCERT, either as a substructure of an already established national CSIRT (computer security incident response team) emulating the Israeli FinCERT or as a stand-alone entity, to strengthen the protection of the financial sector, which is often at the forefront of regular and novel malicious cyber activity.

    - *Supporting Action 1.2.2:* The Forum of Incident Response and Security Teams (FIRST) should consider creating a stand-alone track or side

event at the annual FIRST conference to deepen this community of experts, including government FinCERTs, staff of national CSIRTs focusing on the financial sector, and related private sector entities. Two or more members of FIRST should also propose a FinCERT "Special Interest Group" to the FIRST board to create a community of interest in addition to the annual side event. (This would be similar to the national CSIRT side event that takes place alongside the annual FIRST conference. Appendix B provides an overview of existing FinCERTs worldwide.)

- **Recommendation 1.3:** Financial authorities should prioritize increasing the financial sector's resilience against attacks targeting the integrity of data and algorithms. Unlike incidents affecting availability or confidentiality, few technical mitigation solutions exist today to mitigate the risks associated with the manipulation of the integrity of data and algorithms. The second-order risk of undermining trust and confidence is significant.

    - *Supporting Action 1.3.1:* Financial authorities should encourage industry to join or emulate data vaulting initiatives, such as Sheltered Harbor, to advance common standards, to better protect against data integrity attacks such as ransomware, and to test data vaulting solutions' effectiveness during a crisis.

    - *Supporting Action 1.3.2:* Considering the limitations of current technical solutions, governments and financial authorities should lead whole-of-society exercises, including industry, that specifically simulate cyber attacks involving the manipulation of the integrity of data and algorithms. Such exercises should be used to identify weaknesses, such as divergence between decision-making timelines in financial markets versus the national security community, and to develop action plans to better protect against such attacks.

- **Recommendation 1.4:** Governments and industry should put additional emphasis on the resilience of financial market infrastructures (FMIs)—critically important institutions responsible for payment systems, central counterparties, central securities depositories, or securities settlement systems—and other service providers deemed critical for the functioning of the financial sector, such as stock exchanges,[25] as successful disruptions against these entities can pose a systemic risk and undermine confidence in the financial system.

    - *Supporting Action 1.4.1:* Governments should use the unique capabilities of their national security communities to help protect FMIs and

critical trading systems, including sharing information about impending threats.

- *Supporting Action 1.4.2:* Industry groups, such as the World Federation of Exchanges (WFE), which is a global industry association for exchanges and clearing houses, should dedicate more resources to capacity-building efforts designed to help smaller and less mature FMIs and other important service providers increase their cybersecurity level.

- **Recommendation 1.5:** Financial authorities, or a designated lead governmental agency, should (i) assess the benefits and risks of using cloud service providers to strengthen the cybersecurity of financial institutions that lack the capacity to effectively protect themselves and (ii) take steps to minimize the risks associated with a migration to the cloud, including potential concentration risk.

  - *Supporting Action 1.5.1:* Financial authorities, or a designated lead governmental agency, should assess which financial institutions, especially small and medium-sized organizations, would become more resilient against cyber attacks by migrating to appropriately secured public or hybrid cloud service providers.

  - *Supporting Action 1.5.2:* To better assess and address growing concerns about concentration risks, governments should work with the major cloud service providers and financial institutions to:

    - Organize annual joint exercises simulating different scenarios to (a) identify internally who would lead their firms during a global cyber disruption; (b) increase cooperation among cloud service providers in building international response and recovery capabilities; and (c) strengthen the resilience of the cloud service infrastructure, as disruption of one provider could lead to service disruptions and reputational damage for all providers in a worst-case scenario.[26]

    - Assess systemic risks, as well as existing and potential mitigations, and share information about key vulnerabilities and threats. The goal is to provide coordinated analysis and identify potential systemic risks for critical functions shared by cloud service providers and to create a playbook for when an incident occurs.[27]

Although the activities listed above have been piloted in other industries in line with anti-trust provisions, governments should express their support and provide guidance by issuing public statements clarifying their position.[28]

- *Supporting Action 1.5.3:* Financial authorities should monitor whether the market, through cloud service providers and third-party consulting firms, is providing financial services firms with sufficient resources to assist with the migration to public or hybrid cloud service providers; this information will allow them to minimize the transitory risk and otherwise take supplementary actions. Publishing these findings will improve market information and allow potential cloud customers to assess benefits and costs more accurately.

- *Supporting Action 1.5.4:* National security agencies should consult critical cloud service providers to determine how intelligence collection could be used to help identify and monitor potential significant threat actors and develop a mechanism to share information about imminent threats with cloud service providers.

- **Recommendation 1.6:** G20 Finance Ministers and Central Bank Governors should highlight, ideally in their 2021 communiqué, the necessity of cybersecurity threat information sharing—including being clear about what information should be shared, why, with whom, how, and when—in order to protect the global financial system.

  - *Supporting Action 1.6.1:* Data protection regulators (for example, the European Data Protection Board), together with financial authorities, should assess the impact of data protection regulation on different cyber threat information-sharing initiatives and clarify, where necessary, that such sharing arrangements serve the public interest and that they comply with the General Data Protection Regulation (GDPR) or other relevant regulations.[29]

  - *Supporting Action 1.6.2:* Governments should assess the potential negative impact of broader data localization requirements on the ability to protect against cyber threats and consider actions to balance these different policy objectives.

- **Recommendation 1.7:** Financial authorities and industry should ensure they are properly prepared for influence operations and hybrid attacks that combine influence operations with malicious hacking activity;[30] they should integrate such attacks into tabletop exercises (such as the G7

exercise) and apply lessons learned from influence operations targeting electoral processes to potential attacks on financial institutions.

- *Supporting Action 1.7.1:* Major financial services firms, central banks, and other financial supervisory authorities should identify a single point of contact within each organization to engage with social media platforms for crisis management. Quick coordination with social media platforms is necessary to organize content takedowns. Social media platforms will be more responsive to a single collective point of contact than to ad hoc communication with many financial institutions.

- *Supporting Action 1.7.2:* Financial authorities, financial services firms, and tech companies should develop a clear communications and response plan focused on being able to react swiftly. A quick response can effectively dampen the effect of an incident, but conventional communication channels are often insufficient to fill the information vacuum in such an event. Given the speed of social media content sharing, limiting the number of people required to review and approve a response is essential for a swift response. Financial institutions should ensure potential influence operations are part of their cyber-related communications planning and be familiar with the rules on platforms relating to key areas, including impersonation accounts and hacked materials.

- *Supporting Action 1.7.3:* In the event of a crisis, social media companies should swiftly amplify communications by central banks, such as corrective statements that debunk fake information and calm the markets. Central banks and social media platforms should work together to determine what severity of crisis would necessitate amplified communication and develop escalation paths similar to those developed in the wake of past election interference, as seen in the United States and Europe.

- *Supporting Action 1.7.4:* Financial authorities and financial services firms should review their current threat monitoring systems to ensure that they include and actively try to identify and detect potential influence operations.

Priority #2, "International Norms": Reinforce and Implement International Norms

Core Pillar #2: *Reinforce international norms at the United Nations and through other relevant processes to clarify what is considered inappropriate behavior—that is, when malicious activity has crossed a line—and hold actors accountable for violations to avoid norms being eroded by impunity.*

Diplomatic agreements on international norms can further reduce risk by clarifying unacceptable behaviors and by helping shape the actions of states and nonstate actors. For example, norms can make clear that undermining the integrity of the financial system would cross a line and lead the international community to swiftly condemn the action and potentially impose consequences. As attribution capabilities improve, this advances deterrence through normative taboos.[31] Norms can also outline standards for positive state behavior, such as providing assistance or investigating alleged malicious activity. At present, such international norms remain weak and will require senior leadership support and reinforcement to have a lasting impact.

The following recommendations are designed to address the uncertainty regarding how international law applies to cyberspace and malicious cyber activity targeting financial institutions, and to build and reinforce existing efforts to advance international norms.

- **Recommendation 2.1:** Heads of state should ensure that their state organs (continue to) exercise restraint when using offensive cyber capabilities to target financial institutions. This will strengthen the nascent state practice that has emerged over the past few decades.

- **Recommendation 2.2:** Individual governments should clarify how they interpret existing international law to apply to cyberspace, specifically with respect to malicious cyber activity involving financial institutions. Governments could do this through ministerial statements or speeches, letters to parliament/legislatures, submissions to the United Nations (UN) emulating existing examples, or other appropriate mechanisms. (Such clarification should follow and ideally go beyond the Australian, British, and Dutch examples and focus on the set of questions highlighted in the complementary report to this strategy.)

    - *Supporting Action 2.2.1:* The North Atlantic Treaty Organization (NATO), the Shanghai Cooperation Organisation (SCO), and other relevant security organizations should clarify how they interpret existing international law to apply to cyberspace, specifically with

respect to malicious cyber activity involving financial institutions; at a minimum, they should initiate processes for member states to discuss this question.

- *Supporting Action 2.2.2:* The International Committee of the Red Cross, through its mission to build respect for international legal obligations,[32] should build on and clarify its existing publications to provide a recommendation to the international community for how existing international humanitarian law should apply to cyberspace specifically with respect to malicious cyber activity involving financial institutions.[33]

- **Recommendation 2.3:** UN member states should strengthen and support the operationalization and implementation of the voluntary norms they agreed to through the UN, namely the norm focused on protecting critical infrastructure.

  - *Supporting Action 2.3.1:* The G20 Finance Ministers and Central Bank Governors should adopt a communiqué, building on previous communiqués, urging restraint per recommendation 2.1, and adding specific declaratory language. The G20 heads of state should then endorse the language adopted by the G20 Finance Ministers and Central Bank Governors.

  - *Supporting Action 2.3.2:* In a future process convened through the UN General Assembly and succeeding the UN Open-Ended Working Group (OEWG) and the UN Group of Governmental Experts (GGE), UN member states should:

    - Make explicit reference to the financial services sector as critical infrastructure for all UN member states for the purposes of norms (f) and (g) of the 2015 UN GGE report, which focus on critical infrastructure.

    - Highlight that financial institutions have been a primary target for malicious actors and face growing criminal and state-sponsored threats that require stronger cooperation among states to protect the global financial system.

    - Call on states to adhere to the positive norms of cooperating in the investigation of transnational cyber crimes and denying the use of their territories for malicious activity.

- *Supporting Action 2.3.3:* Financial authorities and industry should use the systems developed for resilience purposes (for example, to identify and detect potential incidents in order to defend against and recover from them) for the detection and attribution of norm violations. Sharing such information is necessary to more effectively hold malicious actors accountable.

- *Supporting Action 2.3.4:* The UN Security Council should continue to monitor North Korea's activities, considering that North Korea's actions have impacted at least thirty-eight UN member states from 2015 to 2020 alone.[34] The UN Security Council should use all its instruments, ranging from monitoring latest developments through regular reports (such as the 2019 "Report of the Panel of Experts Established Pursuant to Resolution 1874"[35]) to the imposition of sanctions, to deter future malicious activity.

- **Recommendation 2.4:** Financial services firms and related trade associations, such as the Institute of International Finance (IIF), the Global Financial Markets Association (GFMA), the Bank Policy Institute (BPI), the Geneva Association, the American Bankers Association (ABA), the European Banking Federation (EBF), the Pan-European Insurance Forum, the Association of Banks in Singapore (ABS), and others should call for stronger international norms to protect the financial system and should prioritize this as a talking point in their engagement with governments.

  - *Supporting Action 2.4.1:* CEOs of financial services firms should collectively call on governments, for example via a joint letter, to strengthen international norms to protect the global financial system and for the G7 and the G20 to issue such a commitment.

  - *Supporting Action 2.4.2:* Financial services firms should commit to sharing information about threat actors' behavior and potential norm violations to assist in the monitoring of compliance. Not sharing this information could embolden malicious actors to continue their activity with impunity.

  - *Supporting Action 2.4.3:* If governments publicly commit to protecting the integrity of the financial system, financial services firms should provide financial support to advance the implementation and strengthening of international norms, for example, to expand capacity-building activities.

Priority #3, "Collective Response": Disrupt and Deter Attackers More Effectively

Core Pillar #3: *Facilitate collective response to disrupt malicious actors and more effectively deter future attacks.*

The third strategic priority—collective response through law enforcement action or other instruments of statecraft, including multilateral or collective response with industry—is enabled by strong resilience and a clear normative framework. Considering the escalating threat landscape, there is growing concern that a lack of more robust and continuous reactions to malicious activity is further emboldening attackers. The current levels of theft and disruptive and destructive activities therefore require not just resilience but a response. Especially during the coronavirus pandemic, cyber heists cannot be ignored when societies worldwide need every penny to assist people in need and can ill afford to have those resources land in the pockets of cyber criminals.

A response may include sanctions, arrests, asset seizures, or other actions. For such actions to be justified, there must be a mutual understanding that a line has been crossed; in addition, since sanctions and other actions to hold actors accountable may provoke an escalatory response, financial actors will need to have a minimum level of resilience so that they can withstand such responses.

The following recommendations outline specific steps that governments and industry can take to facilitate a collective response to an incident in order to deter malicious actors from future cyber attacks. Such a response may include law enforcement action, and it may well require strengthening the financial sector's ties to other parts of the national security community, considering the growth of state-sponsored threats.

- **Recommendation 3.1:** Governments and the financial industry should consider establishing entities to bolster their ability to assess systemic risk and threats as well as to coordinate mitigating actions. Existing examples of such entities include the United States' Financial Systemic Analysis and Resilience Center (FSARC) and the United Kingdom's Financial Sector Cyber Collaboration Centre (FSCCC).

- **Recommendation 3.2:** Governments should ensure their intelligence collection priorities include a focus on threats that could pose a risk to the financial system.In addition to nation-state and state-sponsored threat actors, sophisticated criminal actors could deliberately or (more likely)

accidentally pose a risk, or they could provide the tools and services for others' disruptive and destructive attacks.

- **Recommendation 3.3:** Governments should consider sharing intelligence about threats that pose a risk to the financial system with other allied, partnered, or like-minded countries.
    - *Supporting Action 3.3.1:* To facilitate such information sharing, governments should consider finding ways—from downgrading classification of intelligence to broadening the pool of security clearance issuance (for example to relevant industry professionals)—to facilitate the sharing of threat intelligence.
- **Recommendation 3.4:** Financial services firms should consider joining transnational networks like the Financial Services Information Sharing and Analysis Center (FS-ISAC) and/or emulating the region-based Cyber Defence Alliance (CDA) model to create a collective space for the financial industry to share information and prioritize responses to malicious cyber incidents.
- **Recommendation 3.5:** Governments should not only focus on state-sponsored actors but also make the fight against cyber crime a renewed priority, focusing less on time-consuming negotiations of a new cyber crime treaty and more on direct cooperation. This is especially important given the impact of the pandemic. For example, governments could support the WEF's Partnership Against Cybercrime and Third Way's Cyber Enforcement Initiative.
    - *Supporting Action 3.5.1:* Governments should build a framework to strengthen and further institutionalize public-private cooperation to tackle cyber crime more effectively at the national, regional, and global levels. The World Economic Forum's Partnership Against Cybercrime is a promising initiative to further advance this on the international level, and Third Way's Cyber Enforcement Initiative is an innovative effort to develop new public policy approaches aimed at strengthening public-public and public-private cooperation to address this problem.
    - *Supporting Action 3.5.2:* The financial industry should throw its weight behind efforts to tackle cyber crime more effectively, for example by increasing its participation in law enforcement efforts and better integrating its financial crimes, fraud, and cybersecurity systems in order to capture latest developments.

- *Supporting Action 3.5.3:* Governments should prioritize and develop law enforcement capabilities to address cyber crimes that violate international norms, namely those targeting financial institutions.

- **Recommendation 3.6:** National and multilateral law enforcement agencies should help coordinate and provide negotiation expertise for financial institutions that have been infected with malware and are being held for ransom by threat actors.

- **Recommendation 3.7:** The FATF should explore how the existing regime to detect and counter money-laundering as well as terrorist and proliferation financing could be leveraged to fight cyber attacks more effectively.

Priority #4, "Workforce": Expand Effective Models

Crosscutting Issue #1: *Build the cybersecurity workforce required to turn ambitions into actions by assessing and expanding effective models for addressing workforce challenges including limited pipelines and a lack of diversity.*

The fourth strategic priority—overcoming cybersecurity workforce challenges—is crosscutting in nature given that a strong cybersecurity workforce is needed by all actors, ranging from industry actors to central banks and governmental organizations, to effectively implement strategies and policies in each of the preceding areas. Financial authorities' increased activity over the past five years may have created an unintended consequence in that financial firms now hire more of the limited cybersecurity talent, thereby exacerbating the workforce shortage in other sectors that are unable to compete with salaries offered in the financial industry.

The recommendations in this section can be grouped into two main categories considering the slightly different sets of challenges each sector is facing: (i) cybersecurity workforce challenges in the private sector and (ii) cybersecurity workforce challenges in the public sector.

- **Recommendation 4.1:** Financial services firms should prioritize their efforts to address cybersecurity workforce challenges, ranging from the limited talent pipeline to the lack of diversity in the workforce. The high rate of unemployment in the wake of the coronavirus pandemic represents an important opportunity to retrain and hire talent.

    - *Supporting Action 4.1.1:* Large financial services firms should form a dedicated working group to collect, compare, and assess data about their own current workforce and related initiatives with the goal of

assessing those initiatives' effectiveness and scalability and addressing the broader cybersecurity workforce challenges faced by individual firms, the sector, and countries.

- *Supporting Action 4.1.2:* Following an assessment of the effectiveness and scalability of existing models, the dedicated working group should share best practices and lessons learned and issue recommendations for how the financial services sector can better address cybersecurity workforce challenges.

- *Supporting Action 4.1.3:* Financial authorities, central banks, and ministries of finance should explore how they could help expand effective cybersecurity workforce initiatives. This would help alleviate the unintended consequence of financial services firms hiring more talent to comply with recently increased regulatory expectations, which exacerbates the workforce shortage for other sectors that cannot compete with financial sector salaries.

- **Recommendation 4.2:** Financial services firms should provide financial and other resources to help augment effective cybersecurity workforce initiatives, especially those focusing on building and widening the cybersecurity professional pipeline, including high school, apprenticeship, and university programs.

- **Recommendation 4.3:** Government agencies and financial authorities should identify, improve, and better promote their employment proposition to cybersecurity professionals, including: (i) exposure to and responsibility for a broad range of technical issues, (ii) access to cutting-edge information and authorities, (iii) providing a market-wide perspective valued by the private sector, (iv) job security, and (v) a service mission to the public.

  - *Supporting Action 4.3.1:* Leaders of financial authorities, and lawmakers when needed, should create mechanisms that give hiring managers greater flexibility, for example allowing them to offer salaries to cybersecurity professionals that are competitive with those offered by industry.

  - *Supporting Action 4.3.2:* Financial authorities should design their workforce plans based on the assumption that staff will leave their positions after a few years rather than stay for the medium or long term. This provides the opportunity to think of such staff as a resource that will build capacity for the sector more broadly and to minimize risk

resulting from staff turnover. This action will likely require organizations to maintain additional headcount on the assumption that some number of positions will be routinely vacant until replacements are hired.

- *Supporting Action 4.3.3:* Financial authorities should establish secondment mechanisms with government agencies that employ staff with cybersecurity expertise. Financial authorities may be able to attract and retain cybersecurity professionals more effectively by offering opportunities to work on cybersecurity challenges in other government agencies, or with private sector companies. At the same time, other government agencies tend to have limited situational awareness of the financial infrastructure and processes and could benefit from the expertise of seconded cyber supervisors and regulators.

- *Supporting Action 4.3.4:* Financial authorities should establish secondment mechanisms with the financial services and technology sectors. This will offer opportunities for increased knowledge transfer and cybersecurity capability adoption by both public and private sectors. Both sectors could benefit from exposure to alternative cybersecurity risk and operational perspectives, as well as initiatives and technologies that may be brought back to their home organizations for implementation.

Priority #5, "Capacity-Building": Align Limited Resources to Maximize Impact

Crosscutting Issue #2: *Align and expand capacity-building efforts across all three core pillars for those seeking assistance.*

The fifth strategic priority—capacity-building—centers on providing assistance to those in need and is also crosscutting. Countries around the world have been seeking assistance from more mature actors in government, industry, and the central bank community on how to strengthen their financial sector's cybersecurity. For example, the IMF and other international organizations received many requests for cybersecurity assistance from member states, especially in the wake of the 2016 Bangladesh incident, in which a cyber attack resulted in unauthorized large fund transfers. Such capacity-building efforts cut across all three core pillars but are still relatively undeveloped with respect to operational cyber resilience and collective defense within the financial services sector (Core Pillar #1).

For this reason, the following recommendations focus on the still nascent capacity-building efforts relating to operational cyber resilience and collective defense. Some of these recommendations also reinforce other, related ongoing capacity-building efforts to help tackle cyber crime and to strengthen international norms.

- **Recommendation 5.1:** The G20 Finance Ministers and Central Bank Governors should adopt a communiqué creating a mechanism to operationalize a coherent approach to cybersecurity capacity-building for the financial sector. Such an approach could emulate and build on the lessons learned from the Global Infrastructure Hub launched during Australia's G20 presidency or the Global Partnership for Financial Inclusion (GPFI) launched during South Korea's G20 presidency.[36]

    - *Supporting Action 5.1.1:* To clarify roles and responsibilities, the G20 Finance Ministers and Central Bank Governors' communiqué should declare that one of the international financial institutions (ideally the IMF, as the sector-specific multilateral organization) will be the lead coordinating agency for this mechanism, which would also include the World Bank, the Consultative Group to Assist the Poor (CGAP), the Alliance for Financial Inclusion (AFI), and other relevant stakeholders.

    - *Supporting Action 5.1.2:* Considering ongoing capacity-building efforts by the private sector—for example, the Customer Security Program advanced by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)—and the public sector's limited financial resources in the wake of the pandemic, the G20 Finance Ministers and Central Bank Governors should invite private sector firms and other relevant stakeholders to participate in and support such capacity-building initiatives, as is the practice in a number of states today.

    - *Supporting Action 5.1.3:* The G20 Finance Ministers and Central Bank Governors should welcome and encourage the use of the "Cyber Resilience Capacity-building Tool Box for Financial Organizations," developed by the Carnegie Endowment for International Peace and launched in partnership with the IMF, SWIFT, FS-ISAC, and other organizations.

- **Recommendation 5.2:** The member states of the Development Assistance Committee of the Organisation for Economic Co-operation and Development (OECD) should integrate cybersecurity capacity-building into official development assistance (ODA) budgets and significantly increase assistance to countries in need. Even with technical cooperation

mechanisms, international financial institutions such as the IMF and World Bank currently do not have the capacity to respond to the disruptions to critical financial services or the hundreds of millions of dollars stolen in countries around the world.

- **Recommendation 5.3:** To further expand and strengthen ongoing capacity-building around international cyber norms and to advance the objectives outlined in this report, the UN Institute for Disarmament Research (UNIDIR) and the UN Office for Disarmament Affairs (UNODA) should integrate a specific module focusing on the financial sector into their capacity-building material.

- **Recommendation 5.4:** To further expand and strengthen ongoing capacity-building efforts with respect to tackling cyber crime more effectively, state and industry stakeholders should support the efforts by the Council of Europe, Europol, INTERPOL, the UN Office on Drugs and Crime (UNODC), and the World Bank to strengthen capabilities to address cyber crime.

Priority #6, "Digital Transformation": Safeguard Financial Inclusion

Crosscutting Issue #3: *Safeguard financial inclusion and the G20's achievements of the past decade in this area.*

The sixth strategic priority focuses on the massive digital transformation currently reshaping the financial system. One area where this transformation has been most pronounced is in the tremendous effort by the G20 and other stakeholders to expand financial inclusion around the world and increase access to financial services for hundreds of millions of people. Many financial inclusion efforts rely on leapfrogging to digital financial services (DFS) and are changing the level and type of interdependencies of the financial system and tech companies.[37] Safeguarding financial inclusion achievements against growing cyber threats is therefore an urgent challenge.

The following recommendations focus on establishing a consolidated foundation to advance cybersecurity in the context of financial inclusion and to safeguard the achievements made in that area over the past decade. This includes clarifying roles and responsibilities of key stakeholders, considering a dedicatedregional focus on Africa to complement the focus on Latin America already provided through the Organization of American States (OAS), and exploring how financial inclusion initiatives could be leveraged to raise awareness about basic cybersecurity principles.

- **Recommendation 6.1:** The G20 heads of state should strengthen coordination among existing financial inclusion and cybersecurity efforts so as to align limited resources and maximize their impact, especially in the wake of the pandemic. They should also initiate an annual conference to assess latest developments and coordinate next steps; the convening should include major donors, the World Bank, IMF, AFI, CGAP, and other relevant stakeholders.

    - *Supporting Action 6.1.1:* The G20 should clarify the role of international financial institutions like the World Bank, CGAP, and the IMF with respect to cybersecurity and financial inclusion. They should also emphasize the need to coordinate on issues that overlap across these institutions.

    - *Supporting Action 6.1.2:* The GPFI should deepen the connections between financial inclusion initiatives and the cybersecurity community. As DFS continue to be expanded, especially in the wake of the pandemic, it is critical to develop greater collaboration between the financial inclusion and cybersecurity communities.

    - *Supporting Action 6.1.3:* The GPFI should deepen the connections between financial inclusion actors and the law enforcement community. As more people gain access to financial services, the platforms they use will become increasingly attractive targets for cyber criminals. By strengthening the relationship between the financial inclusion community and the law enforcement community, stakeholders can more effectively address cyber crime that targets products and services used for financial inclusion.

- **Recommendation 6.2:** A network of experts should be created to focus specifically on cybersecurity and financial inclusion in Africa to complement other existing regional initiatives. The fifty-four countries in Africa are experiencing a significant transformation of their financial sectors as they extend financial inclusion and leapfrog to DFS. At the same time, this transformation makes African countries a prime target for cyber criminals who exploit soft targets and financial institutions with limited capacity to effectively protect themselves. Cybersecurity expertise across the African continent remains limited and scattered.

- **Recommendation 6.3:** The G20 should highlight that cybersecurity must be designed into technologies used to advance financial inclusion from the start rather than included as an afterthought. An example of such a foundational expectation is the reference in the GPFI's "G20 Action Plan

on SME Financing" to a strong credit infrastructure as a fundamental requirement for small- and medium-sized enterprises to have access to loans and other credit. By looking ahead and mapping initiatives that will come online in the coming years, GPFI can help ensure that cybersecurity will ideally no longer be an afterthought but be incorporated in future financial inclusion developments beyond payment systems.

- **Recommendation 6.4:** The GPFI, main funders, and DFS platforms should explore how financial inclusion efforts could be leveraged to increase general awareness of basic cybersecurity principles. Raising awareness of best cybersecurity practices is critical, especially among users in developing countries, who recently gained access to financial services and the internet, often via a mobile phone. Financial inclusion platforms could be leveraged to offer basic cybersecurity resources for the individuals and businesses using them.

PART II BACKGROUND REPORT: ANALYSIS AND CONTEXT

The unique nature of cyber threats and the actions necessary to better protect the global financial system against them require strengthening the connections between different actors and initiatives. However, many public and private actors remain unaware of the full range of efforts in this domain. The fact that this report is the most comprehensive analysis to date of the efforts underway to protect the global financial system against cyber threats is a telling example of the disconnect.

This background report therefore complements the strategy outlined in Part I and aims to raise readers' awareness of processes taking place in other communities. The following sections outline the analysis and context for each recommendation in the strategy and its supporting actions. Each section offers an overview of the challenges specific to the priority area as well as a mapping of ongoing initiatives and relevant stakeholders in government, industry, and the financial supervisory community. We hope that readers will focus not on the sections they are most familiar with, but on those discussing less familiar issues.

For example, for central bank officials who are already very familiar with ongoing efforts to increase the sector's resilience, the sections on international norms and collective response will offer new information about how the recommendations focusing on diplomatic initiatives and the national security community can help support their resilience-focused efforts. Similarly, for

diplomats focused on advancing international norms, the section on cyber resilience will point to opportunities for implementing these norms. And the challenges with respect to workforce and capacity-building are often neglected but essential to strengthen the system's weakest links.

The main challenge, outlined in the overarching recommendations, is how best to organize the protection of the financial system against cyber threats. These overarching recommendations therefore focus on strengthening international mechanisms for coordination, placing the G20 and the G7 at the center and pairing them with more active industry engagement.

- **Recommendation 0.1:** G20 heads of state should create interagency processes within their respective governments, co-led by the ministry of finance and the central bank/monetary authority (or other relevant entity representing the government in international finance bodies), to explore options for better protecting their domestic as well as the international financial system against cyber threats. Ideally these processes will focus on the six priority areas identified in this report and take into account the report's recommendations. (The co-leadership is designed to avoid disruptions caused by the frequent turnover of politically appointed ministers of finance; including central banks/monetary authorities as co-leads will allow greater continuity of effort.)

    - *Supporting Action 0.1.1:* To help increase trust and confidence, G20 Finance Ministers and Central Bank Governors should consider creating a G20 Finance Track process emulating the confidence-building measures undertaken by the member states of the Organization for Security and Co-operation in Europe (OSCE), which includes the United States and Russia.

Although the G20 member states tend to emphasize their shared interest—the stability of the global financial system—that shared interest has not been sufficient to overcome a profound lack of trust, which has hampered coordination and cooperation among the G20 member states. To develop more trust when discussing cybersecurity in the context of the financial system, G20 member states could consider emulating the process at the OSCE. Given that the OSCE's fifty-seven participating states, including the United States and Russia, were able to agree on confidence-building measures in 2013 and 2016, this seems a promising model to emulate in the G20 Finance Track.

Established during the Cold War, the OSCE was created to help build trust and increase confidence between the United States and the Soviet Union. In 2012, the OSCE's member states decided to launch a new work stream specifically

designed to reduce mistrust in the area of cybersecurity and conflict. They launched a working group focusing on developing "confidence-building measures (CBMs) to enhance interstate cooperation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs [information and communications technologies]." A first set of CBMs was adopted in 2013, followed by an expanded set adopted in 2016.

Similar actions could be taken through the G20 Finance Track, considering that a major cyber incident involving the financial system is likely to require international cooperation at a global level. As a starting point, G20 member states could assess which of these measures are already in place, whether through the FSB's actions initiated in 2017 or other relevant entities such as the BIS. The following table lays out possible CBMs for the G20 modeled after the set created by OSGE.

Table 2: Possible Measures to Build Confidence Among the G20

G20 member states will **nominate a 24/7 contact point** to facilitate pertinent communications on cyber incidents with respect to the financial sector. G20 member states will update contact information annually and share any changes with other members no later than thirty days after a change has occurred.
G20 member states will voluntarily **provide contact information for existing official national structures** that manage ICT-related incidents relevant to the financial sector; member states will also coordinate responses to enable direct dialogue and facilitate interaction among responsible national bodies and experts.
G20 member states will voluntarily **establish measures to ensure rapid communication at policy levels of authority.**
G20 member states will voluntarily **provide their national views on various aspects of national and transnational cyber threats targeting the financial system.** The extent of such information will be determined by the member states.
G20 member states will voluntarily **facilitate cooperation among the competent national bodies** as well as exchange of information relevant to protecting the financial sector against cyber threats.
G20 member states will, on a voluntary basis and at the appropriate level, **hold consultations** in order to protect the integrity of the global financial system.
G20 member states will voluntarily **share information on measures that they have taken to protect the integrity of the global financial system.**
G20 member states will **use the FSB as a platform for dialogue, exchange of best practices, awareness-raising, and information on capacity-building** regarding cybersecurity in the financial sector. The participating states will explore further developing the FSB role in this regard.
G20 member states are encouraged to have in place **modern and effective frameworks and policies** to facilitate voluntary bilateral cooperation and effective, time-sensitive information exchange among competent authorities of the participating member states, including law enforcement agencies, in order to respond to malicious cyber activity.

Table 2: Possible Measures to Build Confidence Among the G20 (continued)

G20 member states will voluntarily **share information on their national organization, strategies, policies, and programs** (including those involving cooperation between the public and the private sector) relevant to cybersecurity in the financial sector; the extent of this information sharing will be determined by the providing member states.
G20 member states will, on a voluntary basis, **share information and facilitate inter-state exchanges** in different formats, including workshops, seminars, and roundtables; these exchanges are aimed at allowing member states to investigate the spectrum of cooperative measures as well as other processes and mechanisms that could enable them to better protect the global financial system against cyber threats.
G20 member states will, on a voluntary basis and consistent with national legislation, **promote public-private partnerships and develop mechanisms to exchange best practices** of responses to common cybersecurity challenges in the financial sector.
G20 member states will, on a voluntary basis, **encourage responsible reporting of vulnerabilities** affecting cybersecurity in the financial sector with the goal of increasing cooperation and transparency among G20 member states.
G20 member states will, at the level of **designated national experts, meet at least three times each year**, to discuss information exchanged and explore appropriate development of these measures.

*Certain steps taken at the OSCE have already occurred in the G20 Finance Track. For example, the cyber lexicon developed by the FSB mirrors a similar effort at the OSCE.

Source: OSCE, "Confidence-Building Measures to Reduce the Risks of Conflict Stemming From the Use of Information and Communication Technologies," OSCE Permanent Council Decision No. 1202, March 10, 2016, https://www.osce.org/pc/227281.

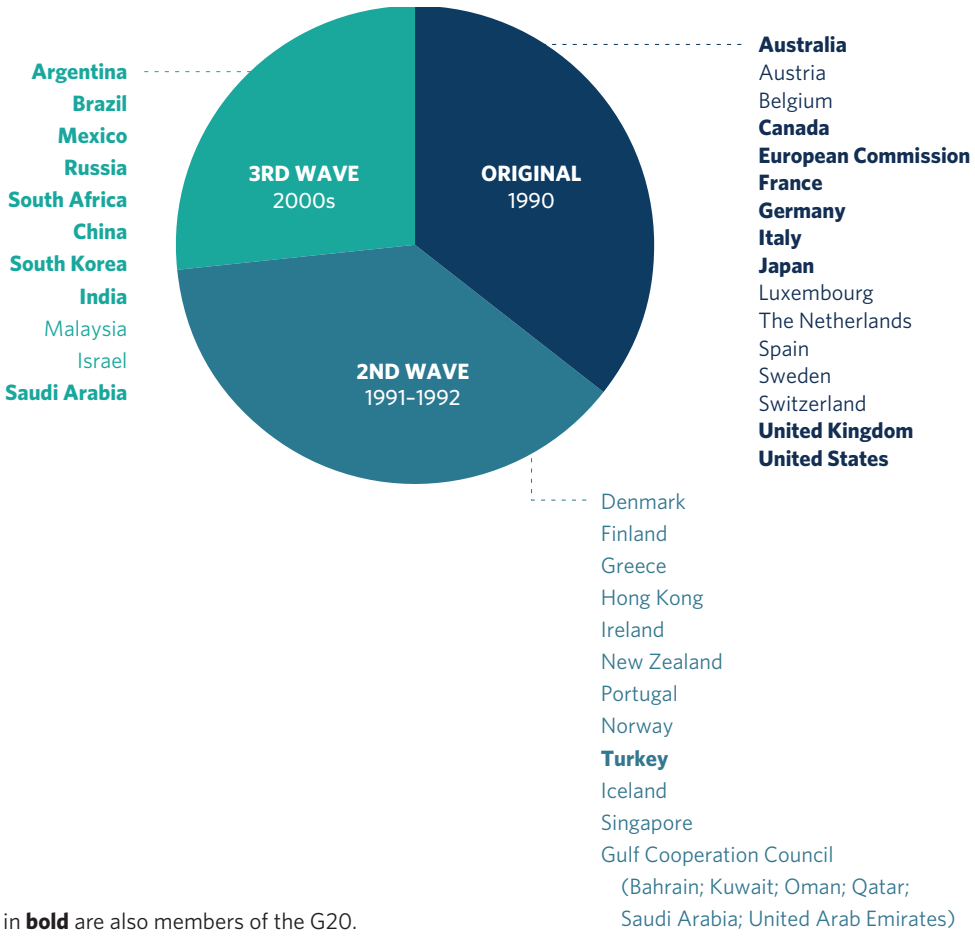
- **Recommendation 0.2:** Financial services firms should expand their engagement and dedicate more resources to strengthening the protection of the sector overall. In particular, firms should support capacity-building efforts for weaker links in the system and become more active in efforts complementary to firms' core focus on resilience, such as advancing international norms, facilitating collective response, and tackling workforce challenges.

- **Recommendation 0.3:** G7 Finance Ministers and Central Bank Governors should renew the mandate of the G7 CEG starting in 2021; the mandate should include expanding the number of participant states and initiating a G7+ process, for example, emulating the one that established the FATF in the early 1990s, or another process for involving members outside its current remit. (In addition to the European Commission, which is already included, this expanded group could include financial centers such as Switzerland and Singapore and other relevant partner countries. Appendix A provides an outline of stakeholders that could be included in such an enlarged process.)

The creation of the FATF provides useful insight into how to expand the important work that the G7 CEG commenced in 2016. A similar G7+ enlarged group could include other major financial centers such as Switzerland and Singapore. Rather than creating a formalized membership like that of the FATF, this new group could issue standing invitations to a small number of countries, similar to those extended by the G20 presiding member state each year.

Figure 3 shows the three phases of expansion for FATF's membership, as the organization shifted over time from its original open membership model to one that invited additional countries to join based on a consensus-driven process. Membership of a group focusing on cybersecurity in the context of the financial system would likely differ from FATF's original membership. Appendix A outlines which countries may be most relevant to include and which financial institutions would be particularly important to consult for such an effort.

Figure 3: Phases of FATF Expansion

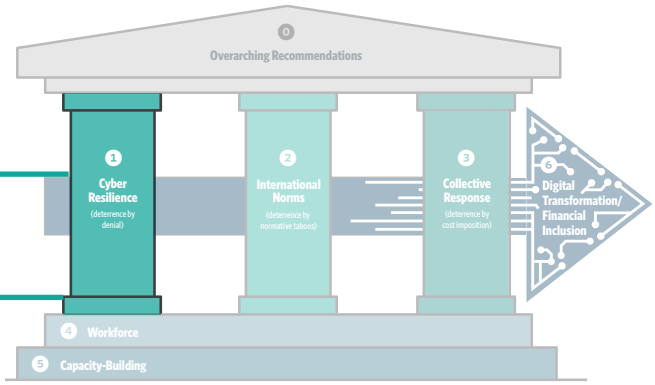


Countries in **bold** are also members of the G20.

Note: Saudi Arabia has participated in the FATF vis-à-vis the Gulf Cooperation Council since 1992 but became a full member of the FATF in 2019.

CHAPTER 1

PRIORITY #1: CYBER RESILIENCE



Core Pillar #1: *Strengthen operational cyber resilience and collective defense to shield the financial sector against cyber threats.*

Problem Statement: Preparing for the Next Crisis

In March 2017, G20 Finance Ministers and Central Bank Governors warned for the first time that "the malicious use of Information and Communication Technologies could . . . undermine security and confidence and endanger financial stability."[38] Consequently, the G20 tasked the FSB with taking stock of approaches on cybersecurity and the financial system; that FSB report was published in October 2017.[39] A year later, the FSB also published a cyber lexicon to promote a common language in the industry.[40]

In the meantime, many individual jurisdictions have been developing approaches to address the risk of cyber incidents. Cyber incidents (attacks or system failures) are inevitable, especially when financial institutions are increasingly digitally interconnected. Firms must be ready to withstand them and maintain operations.[41] While operational risk has been a fundamental tenet of financial risk management for more than a decade, the term *operational resilience*—"the ability of firms and financial market infrastructures (FMIs) and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions"[42]—is still emerging as a foundational principle of financial risk management. Central to operational resilience is cyber resilience.

There is broad agreement that the financial sector should embrace operational resilience in order to withstand and recover from nonfinancial shocks and to protect financial stability. In February 2020, Christine Lagarde, the former managing director of the IMF and now head of the ECB, warned that a cyber attack had the potential to trigger a liquidity crisis.[43] Just *how* operational resilience should be implemented and achieved remains unclear.

Managing cyber risk is still a challenge for regulatory and supervisory authorities. According to Arthur Lindo, a senior official from the U.S. Federal Reserve Board and chair of the BCBS Operational Resilience Group, "traditional regulatory approaches will not be adequate for meeting the challenges of this new environment. [Cyber risk] is requiring [a] regulatory approach that is significantly different from those we use for capital, liquidity and other major risk stripes."[44]

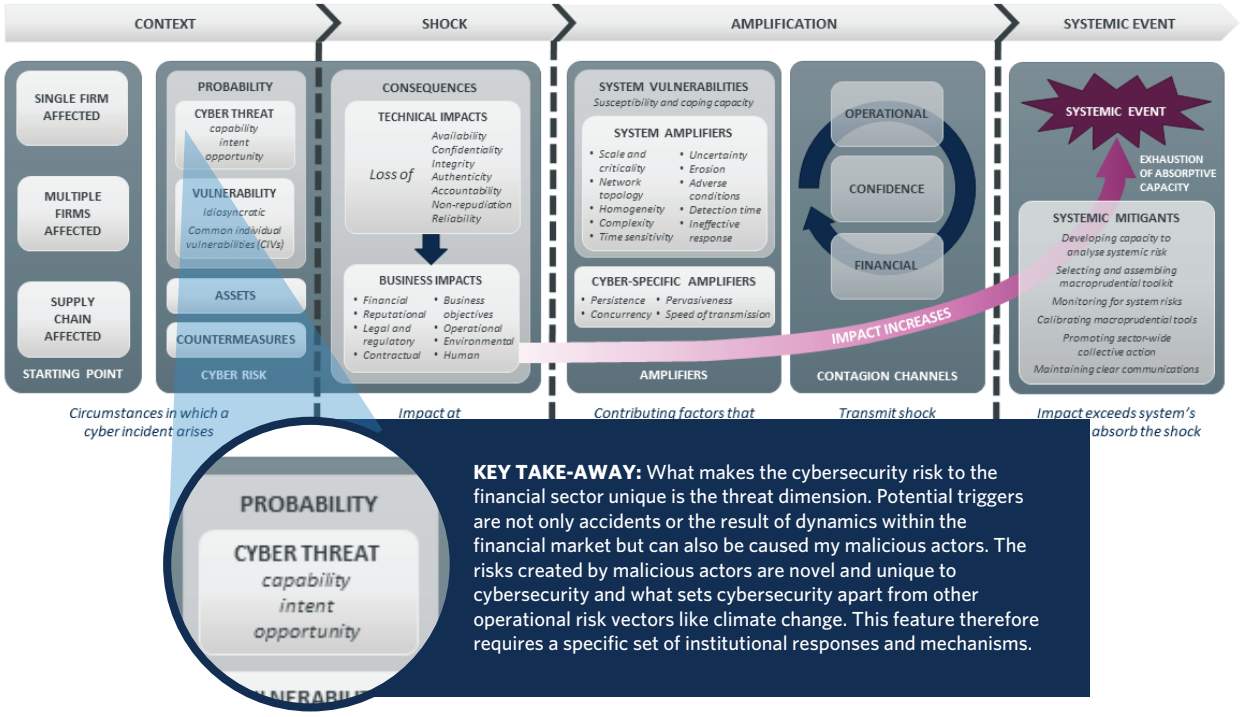
Activities of the G7 Finance Track CEG

- "Fundamental Elements of Cyber Security for the Financial Sector" (2016)[45]
- "Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector" (2017)[46]
- "Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector" (2018)[47]
- "Fundamental Elements for Threat-led Penetration Testing" (2018)[48]
- "Cybersecurity: Coordinating Efforts to Protect the Financial Sector in the Global Economy" (May 2019)[49]
- G7-wide simulation exercise (2019)[50]

The financial community is currently debating how regulators should create new tools and expectations to ensure operational resilience across jurisdictions. Both financial institutions and regulators have incentives to effectively mitigate risks from cyber incidents,[51] but there is debate about what is required of firms. Achieving operational resilience requires a comprehensive approach to prevention, adaptation, response, recovery, and learning. Consequently, operational resilience has many subcomponents, including impact tolerances, penetration-testing, third-party risk management, incident response and crisis management, information sharing, incident reporting, governance, and a common lexicon, to name a few.

Figure 4 illustrates how the thinking about cyber risks in the context of the financial system has evolved.

Figure 4: Overview of How to Conceptualize Systemic Cyber Risk With Respect to the Financial System



Source: European Systemic Risk Board, "Systemic Cyber Risk," February 25, 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

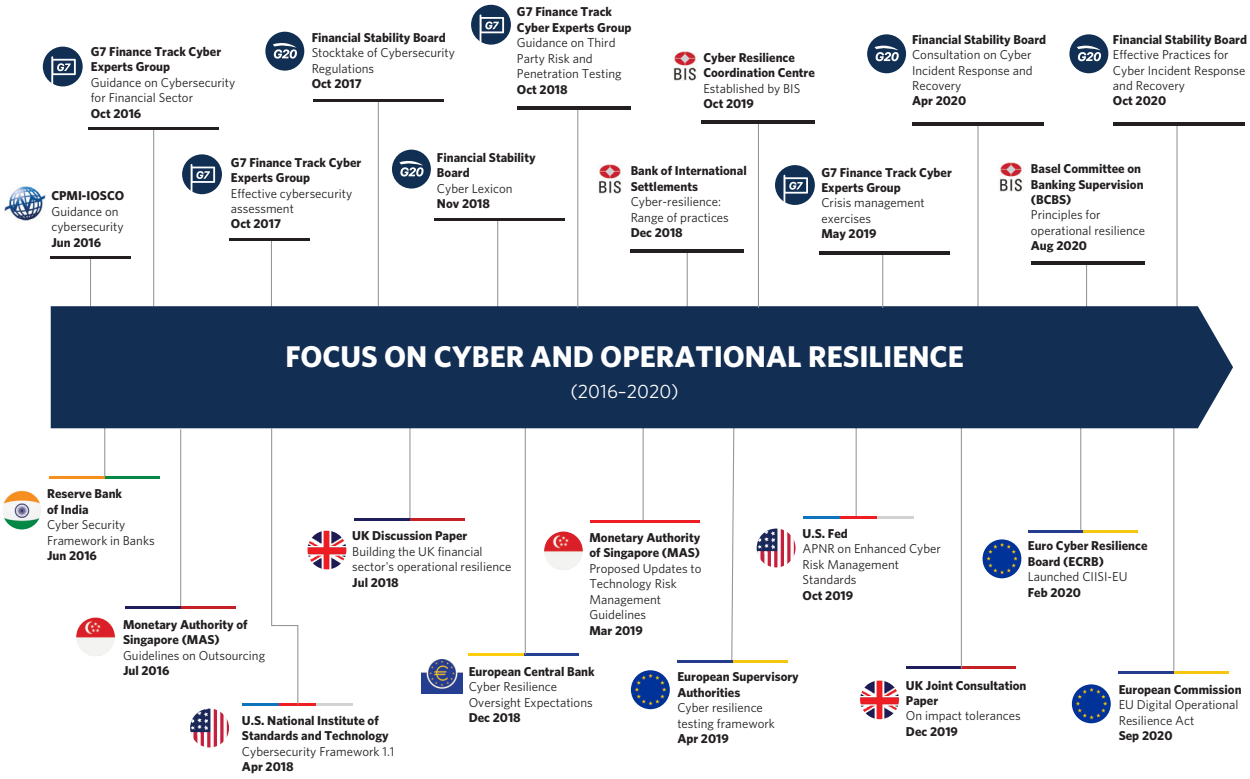
Industry has raised concerns about financial authorities' divergent and inconsistent approaches and has called for an "international common approach."[52] Harmonizing regulation internationally, they argue, will reduce the costs of complying with multiple regimes and free up resources for operational activities.

Mapping the Status Quo: Current Approaches and Specific Areas of Focus

National Approaches Trump International Cooperation

The concept of "operational resilience" emerged as a key focus among national supervisory and regulatory authorities in 2016, as highlighted in Figure 5.[53]

Figure 5: A Timeline of Regulation Focusing on Operational Resilience



Source: Marc Saidenberg, John Liver, and Eugene Goyne, "2020 Global Bank Regulatory Outlook: Four Major Themes Dominating the Regulatory Landscape in 2020" (EY, January 20, 2020), https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-global-regulatory-outlook-four-major-themes-dominating-the-regulatory-landscape-in-2020_v2.pdf.

The United Kingdom's 2018 discussion papers cemented the term across the sector, and authorities in the United States, Singapore, and the EU also developed their own perspectives on the topic.

This section summarizes and analyzes the approaches of five key jurisdictions—the United Kingdom, the EU, Singapore, the United States, and India—chosen for their centrality and thought leadership in the global financial system.

United Kingdom

The Bank of England (BoE), the Prudential Regulation Authority, and the Financial Conduct Authority (FCA), here referred to in the aggregate as the United Kingdom Financial Service Authorities (UK FSAs), were among the first financial authorities to advance the concept of operational resilience.

Starting in July 2018, the UK FSAs published a series of discussion papers, "Building the UK Financial Sector's Operational Resilience," that drew focus away from firms' ability to prevent disruptions and refocused attention on ensuring that individual firms and the financial sector had the ability to withstand disruptions, or "shocks."[54] In December 2019, the UK FSAs proposed an operational resilience framework based on industry feedback that called upon financial institutions and FMIs to set impact tolerances for key business services by "quantifying the acceptable level of disruption through severe . . . but plausible scenarios."[55] Importantly, the UK FSAs noted that they would refine their framework based on emerging international standards.[56]

The United Kingdom has a number of other important initiatives related to operational resilience. To support sector-wide penetration testing, the BoE developed CBEST, a framework for penetration testing of systemically critical organizations.[57] According to the BoE, "The implementation of CBEST will help the boards of financial firms, infrastructure providers and regulators to improve their understanding of the types of cyber-attacks that could undermine financial stability in the U.K."[58]

The United Kingdom also hosted and takes part in a number of cybersecurity exercises. For example, UK FSAs hosted the Waking Shark I and II exercises in 2011 and 2013, and the 2018 SIMEX18 exercise also focused on a prolonged and broad cyber attack.[59] In 2015, the United Kingdom and the United States held a joint exercise testing the stability of the financial system in a cyber incident.[60] Many UK firms participate in the regular Quantum Dawn exercises, hosted by the Securities Industry and Financial Markets Association (SIFMA).[61] Relatedly, to support information sharing, the United Kingdom has the Cyber Security Information Sharing Partnership, a joint industry/government initiative led by the National Cyber Security Centre (NCSC) that provides threat intelligence to key financial institutions.[62]

Public-private mechanisms like the Cross Market Operational Resilience Group (CMORG) or FSCCC enable cooperation on exercises and information-sharing in the UK financial sector. For example, CMORG is a platform for senior public and private sector executives to rehearse how to respond to a major crisis event to establish what the Bank of England calls "common reflexes."[63] The group is jointly chaired by Lyndon Nelson of the Bank of England and Stephen Jones, CEO of UK Finance, the London-based financial services industry association.[64] A subgroup of CMORG, the Sector Exercising Group, manages the sector's annual exercise regime, including simulations of major cyber incidents like SIMEX18.[65]

In short, the UK FSAs are key thought leaders on operational resilience and the outcome of the consultation process will likely shape the international dialogue around this issue.

The European Union

The EC, the European Central Bank and other European supervisory authorities (ESAs), and individual EU member states have explored, tested, and implemented new approaches to strengthen the cyber and operational resilience of the financial system. Nonetheless, according to a September 2020 assessment by the EC, "Overall, the financial sector stability and integrity are not guaranteed and the single market for financial services remains fragmented."[66] The new "Digital Finance Strategy for the EU" therefore puts harmonizing operational resilience approaches front and center in the EC's legislative agenda, which will likely lead to greater convergence among national approaches in the coming years.

Activity by the European Commission

In March 2018, the EC's FinTech Action Plan called for the ESAs to issue ICT risk management requirements for the EU financial sector.[67] The ESAs published the "Joint Advice of the European Supervisory Authorities,"[68] which noted that "efforts should be made toward greater harmonization" and toward improved third-party risk management. In late 2019, the European Banking Authority (EBA) published its "Guidelines on ICT and Security Risk Management," which entered into force on June 30, 2020.[69] Among other things, these guidelines call for firms to conduct "business impact analysis by analyzing their exposure to severe business disruptions."[70] The EBA also published their outsourcing guidelines.[71]

In 2019, the EC focused on updating its regulations for Europe's financial sector. In December 2019, the EC launched a consultation initiative, "Digital Operational Resilience Framework for Financial Services: Making the EU Financial Sector More Secure."[72] Aware of the financial service industry's concerns around harmonization, the consultation noted: "It is essential that financial supervisors' efforts work in a harmonised and convergent framework."[73] The EBF, the EU's largest financial trade organization, welcomed the EC's consultation: "The interconnectedness of all actors within the financial ecosystem, incl. [sic] third party providers, and the evolution of ICT risks highlight the need for a common minimum security for the financial sector as a whole, based on international coordination."[74]

In September 2020, the EC released a new digital finance strategy for the EU in conjunction with a "digital finance package" of legislative proposals. The

new strategy warns that coronavirus has "increased reliance on digital and remote technologies," which has only increased the urgency of action: "The EU cannot afford to have the operational resilience and security of its digital financial infrastructure and services called into question."[75]

The legislative package includes the Digital Operational Resilience Act (DORA) for the financial sector, which was prompted by an observed "minimum harmonization [that left] room for national interpretation and fragmentation."[76] DORA aims to strengthen firms' management of ICT risks, increase the capacity of supervisors, improve testing of financial systems, and upgrade oversight of third-party ICT providers.[77] DORA reinforces that EU authorities are particularly concerned with third-party risk, especially that posed by cloud service providers. Most importantly, the legislation addresses the ESAs' 2019 call to create "an appropriate oversight framework for monitoring critical service providers";[78] DORA proposes a framework that would enable "continuous monitoring of the activities of ICT third-party service providers that are critical providers to financial entities."[79]

Activity by the European Central Bank

The ECB has also played a central role in advancing initiatives on cyber resilience across the EU. In 2017, the ECB Executive Board voted to establish the Euro Cyber Resilience Board (ECRB) for pan-European Financial Infrastructures, a forum for senior officials to advance cyber resilience policy. In 2019, the ECB published a set of "cyber resilience oversight expectations" (CROE) to provide guidance to FMIs and supervisors. The ECB also hosts UNITAS, a cybersecurity exercise that tests the resilience of crisis communications between supervisors and firms.

Since its launch in 2018, the ECRB has focused on tackling effective cross-border information sharing between financial infrastructures. In February 2020, the ECRB launched the Cyber Information and Intelligence Sharing Initiative (CIISI-EU), which brings together a range of public and private stakeholders: pan-European financial infrastructures, operational teams within central banks, critical service providers, the European Union Agency for Cybersecurity (ENISA), and Europol.[80] CIISI-EU provides a technical platform for public-private information sharing, notably including strategic intelligence regarding nation state activity. To prevent mistrust between private companies and authorities from chilling the exchange of information, all content is siloed outside the purview of the supervisory functions of participating public authorities.[81]

Additionally, in 2018, the ECB published the Framework for Threat Intelligence-Based Ethical Red Teaming (TIBER-EU), based on the original Dutch TIBER-NL

framework. The TIBER-EU framework provides central banks and financial authorities guidance in collaborating with financial institutions to carry out penetration testing of live systems. TIBER-EU aims to overcome barriers of mistrust by generating practical results for financial institutions, and by fostering community and collaboration from the bottom up. To this end, the ECB chairs a TIBER-EU Knowledge Centre where participants convene, share experiences, and plan mutual cross-border tests. To date, TIBER-EU has been adopted by twelve EU member states and adoption continues to grow.[82]

Individual EU Member States

EU member states have developed national approaches to operational resilience that mostly complement the EU's work over the last two years. Key guidance and regulations from G7 states include: guidance on cloud computing from France's Prudential Supervision and Resolution Authority (ACPR), the Bank of Italy's guidance on outsourcing risk management, and governance expectations from Germany's Federal Financial Supervisory Authority (BaFin).

One particular concern is how operational resilience will be implemented at a supra-national level, within the EU's single market, given the national security implications of financial (in)stability. This concern was expressed during a meeting of the EU's Economic and Financial Affairs Council in September 2019: "The designation of financial services as critical infrastructure might lead Member States to increasingly declare financial regulation a matter of national security, thus undermining internal market objectives. . . . An approach reconciling security and internal market objectives is therefore needed."[83] CIISI-EU and TIBER-EU can be seen as first attempts to balance these competing equities, and DORA is a signal that the European financial system is moving toward a coordinated approach to operational resilience. However, overcoming barriers of trust will require persistent and practical collaboration that clearly demonstrates value to member states.

Singapore

Singapore is another key thought leader in the cybersecurity domain. The Cyber Security Agency of Singapore (CSA) is responsible for cybersecurity nation-wide and works closely with the MAS on cyber security and resilience in the financial sector. Singapore's Cybersecurity Act, which entered into force in March 2018, establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore. Its key objectives are to strengthen critical information infrastructure against cyber attacks; authorize the CSA to prevent and respond to cybersecurity threats and incidents;

establish a framework for sharing cybersecurity information; and establish a light-touch licensing framework for cybersecurity service providers.[84]

With respect to cybersecurity and operational resilience in the financial sector, the MAS, through its Technology and Cyber Risk Supervision Department, has issued a number of innovative regulatory cyber risk management approaches over the last decade. In June 2013, the MAS issued a "Notice on Technology Risk Management" to establish legally binding requirements for the availability and recoverability of critical systems, recovery time, and incident reporting.[85] The MAS is currently revising these guidelines to reflect a more principles-based approach.[86]

In March 2019, the MAS proposed changes to their Technology Risk Management Guidelines and Business Continuity Management (BCM) guidelines, citing concerns about the increase in the scale and frequency of cyber attacks.[87] The proposed revisions in the BCM guidelines intend to raise the standards for financial institutions to better account for interdependencies across their operational units and linkages with external service providers in their business continuity plans. The draft's initial reference to "minimum performance levels"—not too dissimilar from the UK's concept of "impact tolerances"—is being reviewed following the public consultation process.

Additionally, the MAS has been particularly focused on third-party risk management because they oversee many financial institutions with global footprints and operate in a small jurisdiction with relatively few local service providers. In 2016, the MAS "Guidelines on Outsourcing" stated "these Guidelines provide guidance on sound practices on risk management of outsourcing arrangements. . . . An institution should ensure that outsourced services (whether provided by a service provider or its subcontractor) continue to be managed as if the services were still managed by the institution." In interviews, MAS staff expressed concern about the systemic risk to the financial system posed by cloud computing, a danger that stems from the fact that there are very few cloud service providers and the prospect of concentration risks if more financial institutions migrate their mission critical workload to the few available cloud platforms. A disruption of a major cloud service platform due to a cyber attack or operational incident could impact the financial sector. MAS staff also emphasized that financial institutions need to reevaluate third-party risks in light of lessons learned from the coronavirus pandemic.

In short, the MAS has become an international thought leader in building cyber resilience. For example, the MAS served as co-chair in developing the CPMI-IOSCO cyber guidance, one of the earliest international efforts focused

on operational resilience.[88] The MAS also partnered with the FS-ISAC to establish the Asia Pacific Regional Analysis Centre and an information-sharing group for central banks, regulators, and supervisory entities—the Central Banks, Regulators, and Supervisory Entities or CERES Forum—to combat cyber threats more effectively.[89] Furthermore, Singapore has expanded its international cooperation through cybersecurity exercises such as the September 2019 Exercise Cyber Star and the November 2019 Exercise Raffles.[90]

The United States

In the United States, the Board of Governors of the U.S. Federal Reserve System (the Fed), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) issued an advance notice of proposed rulemaking around "enhanced cyber risk management standards" in 2016. These rules were to be issued in 2017 but were then deprioritized.[91] Two years later, the *Financial Times* reported that U.S. regulators were working on a "cross-agency approach to testing banks against attacks that could crash global payments networks, expose customer data or otherwise threaten the integrity of an industry."[92] The Fed had reopened the consultation process for the proposed "Enhanced Cyber Risk Management Standards," suggesting that resilience is once again becoming a priority.[93]

There are indications that the United States is more sympathetic than other jurisdictions to industry concerns about regulatory harmonization. For example, in 2018, Randal Quarles, then vice chairman for supervision at the Fed, stated in a speech to the Financial Services Roundtable: "We support industry efforts to improve harmonization across the sector, which are complementary to achieving our regulatory safety and soundness goals."[94] He concluded that the Federal Reserve's approach to cybersecurity "may not have fast results" but was focused on "getting it right."[95] A year later, during testimony before the U.S. House Committee on Financial Services, JPMorgan Chase CEO Jamie Dimon reiterated industry's complaint about the conflicting cybersecurity regulations they were facing. The *Financial Times* reported that Dimon and other financial CEOs went on to meet with U.S. Treasury Secretary Steven Mnuchin to discuss improving harmonization of cybersecurity requirements.[96]

In short, the United States is embracing operational resilience but moving more slowly, prioritizing regulatory harmonization and private sector input over speed. Arthur Lindo, deputy director of supervision and regulation at the Fed, explained the reasoning behind the U.S. approach: "We have changed [the Fed's] focus from developing operational resiliency expectations that are primarily regulatory driven to developing expectations that are harmonized to

leading industry standards and best practices and reflect significantly more input from firms before we establish specific resiliency tolerances."[97]

Even with this more deliberate approach, cyber resilience remains a priority for U.S. financial supervisory authorities. In its 2020–2023 strategic plan, the Fed committed to "evolve policy and supervisory capabilities to keep pace with financial technology innovation and operational vulnerabilities, including cyber security."[98] During the January 2020 meeting of the Fed's Federal Open Market Committee, some participants raised concerns "that cyber-attacks could affect the U.S. financial system," marking concern about the issue among senior leadership.[99]

In addition to the Fed, individual states, specifically New York, have outsized influence on the financial sector's resilience efforts. This is in part because the U.S. financial sector is heavily clustered around New York, and the New York State Department of Financial Services (NYDFS) has led a significant portion of the cyber risk supervision. In 2016, NYDFS published "Cybersecurity Requirements for Financial Service Companies," a major revision to existing cybersecurity supervision requirements that focused less on prevention and more on recovery from cyber incidents.[100]

India

India's approach to cyber resilience and operational resilience is mainly driven by its central bank, the Reserve Bank of India (RBI). In 2016, the RBI published a circular calling for a cyber security framework for Indian banks; this document warned that "banks should immediately put in place a cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats." The framework also called for banks to establish security operations centers as soon as possible.

India's other financial authorities have also been proactive in addressing cyber risks over the last five years. In 2015, the Securities and Exchange Board of India published a framework on cyber security and cyber resilience for FMIs, specifying that "cyber security frameworks include measures, tools and processes that are intended to prevent cyber attacks and improve cyber resilience."[101] In 2018, the Insurance Regulatory and Development Authority of India issued a circular outlining guidance on cybersecurity risk for India's insurance companies, including requirements on a cyber security assurance program, a gap analysis report, and a cyber crisis management plan.[102] Other key actors in India like the National Cyber Security Coordinator and the National Critical Information Infrastructure Protection Centre also play an active role in promoting cyber resilience across the financial sector.

Created by the RBI in 1996, the Institute for Development and Research in Banking Technology (IDRBT) incubated the Indian Banks–Center for Analysis of Risks and Threats (IB-CART) in 2014; IB-CART is modeled after FS-ISAC and the RBI Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds. Today, IB-CART facilitates information sharing across India's financial sector. It was the first such sector-specific center in India and, according to IDRBT, has since "become a model of other critical sectors."[103] According to IDRBT's website, "The IB-CART now has more than ninety users from over sixty public, private and foreign banks in India. The IB-CART advisory council has nine members with representation from public and private sector banks and CERT-IN."[104] IDRBT also led the development of a 2016 cyber security checklist for supervised entities within India's financial sector. The checklist aims to "help banks in identifying any gaps in cybersecurity systems" and "help board level subcommittees on risk management and information security on monitoring the cyber defence preparedness of banks."

In 2019, to address this evolving threat landscape, the RBI centralized all regulatory and supervisory functions related to cyber risks within its Cyber Security and IT Risk Group, located in a newly created Department of Supervision. In addition, the RBI, together with CERT-In, hosts cybersecurity exercises within the financial sector; as of July 2020, thirteen exercises have been held.[105]

In response to coronavirus, the RBI has begun taking further action to address heightened cyber risk to India's financial sector, in particular its payments markets. The rise in cyber threats also prompted the RBI to work in close coordination with CERT-In to combat cyber-enabled fraud.[106] CERT-In began tracking cyber threats, analyzing threat intelligence, and helping the RBI issue advisories to financial sector chief information security officers (CISOs).[107] The RBI has been working proactively with the Economic Offenses Division of India's Central Bureau of Investigation, which leads investigations of cyber crimes related to banking and financial services.[108] However, the degree of cyber threats in India's financial sector has revived calls for a national Indian FinCERT.[109]

Impact Tolerances

In 2018, UK authorities introduced the concept of *impact tolerances* through a series of discussion papers that have since become the BoE website's most downloaded document. Impact tolerances are defined as "the maximum tolerable level of disruption to an important business service, including the maximum tolerable duration of a disruption."[110]

There are signs that authorities from other jurisdictions are planning to take similar approaches to operational resilience. In the EU, the EBA's "Guidelines on ICT and Security Risk Management" instruct financial institutions to conduct "business impact analysis by analyzing their exposure to severe business disruptions."[111] In Asia, the MAS's proposed revisions to the BCM guidelines call for financial institutions to map critical business functions and determine recovery times and minimum performance levels for each.[112] In the United States, Arthur Lindo has discussed the Fed's process for establishing "specific resiliency tolerances."[113]

The private sector has acknowledged that impact tolerances will be a component of sector-wide operational resilience, but there is disagreement about supervisory expectations. For example, in their response to the 2018 UK discussion papers, the GFMA agreed that "asking firms to set 'impact tolerances' for their most important business services could be helpful to mature operational resilience across the industry"; however, they also maintained that such a request "should remain aspirational rather than to meet supervisory expectations."[114] The financial sector's coordinated response to the UK FSA's consultation process will be the next major iteration in the public-private dialogues around establishing expectations for impact tolerances.

Requirements that banks map, set, and share their impact tolerances raise two main concerns. The first concern arises if financial authorities ask for impact tolerances without first developing a standardized, cross-jurisdictional framework, thereby forcing banks to produce multiple assessments to fit each jurisdiction's requirements. For example, supervisors of Country A may require impact tolerances from a bank not only for its operations in Country A but also for its operations in Country B because operations in Country B could impact the financial stability of Country A.

The second concern is that consolidating tolerances from systemically important financial institutions into a single repository—essentially, a map of what business function disruptions would cripple a bank—creates a high-value target for sophisticated malicious actors. Financial authorities would need to securely store tolerance data.

Both concerns raise questions about what information is reasonable for a supervisor to request related to firms' business outside of the supervisor's jurisdiction. Namely, what are reasonable roles and responsibilities of the *home* regulator versus the *host* regulator?

International Financial Institutions' Approach to Operational Resilience

This section summarizes and analyzes approaches to operational resilience on the part of key international financial institutions; the following section examines the approaches adopted by industry.

Committee on Payments and Market Infrastructures & the International Organization of Securities Commission

The CPMI, a committee within the BIS, is a global standard setter for payment, clearing, and settlement in the financial system; it is also a forum for central bank cooperation on such functions. IOSCO is an international body for financial authorities that regulate securities and futures markets. The CPMI and IOSCO have overlapping mandates and often collaborate on cybersecurity issues, "to enhance coordination of standard and policy development and implementation, regarding clearing, settlement and reporting arrangements including financial market infrastructures (FMI) worldwide."[115]

In June 2016, CPMI-IOSCO released their joint report, "Guidance on Cyber Resilience for Financial Market Infrastructures."[116] It is regarded as the first internationally agreed upon guidance on cybersecurity for FMIs and highlights the growing attention this issue has been receiving in recent years. The goal of the report is to increase the ability of FMIs to pre-empt, rapidly respond to, and recover from cyber attacks, as well as to set resiliency standards from country to country.[117]

It should be noted that both organizations tackle cybersecurity individually as well as collaboratively. For example, IOSCO's Cyber Task Force tracks cybersecurity regulations from IOSCO member jurisdictions. In 2019, the task force published a report finding that member jurisdictions consider cyber "to be at least one of the most important risks faced by regulated firms."[118] In May 2018, the CPMI published a guidance document, "Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security."[119]

Financial Stability Board

The FSB, established by the G20 in 2009 and hosted by the BIS, began its work on cyber resilience in 2017, after being tasked by the G20 with taking stock of approaches on cybersecurity and the financial system.[120] In October 2017, the FSB published its "Stocktake and Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices." It

found that many jurisdictions were still actively developing regulation and guidance and pointed to a fragmentation between approaches among surveyed jurisdictions.[121]

The FSB also published a cyber lexicon to promote a common language in the industry; this lexicon is currently being updated and is scheduled to be released in November 2020.[122] The FSB also developed a toolkit, "Effective Practices for Cyber Incident Response and Recovery,"[123] based on a range of practices from different jurisdictions; the toolkit will be presented at the G20 meeting in November 2020.

Basel Committee on Banking Supervision

The BCBS, the main international body of banking supervisory authorities guided by the central bank governors of the G10 countries, has traditionally advanced cyber resilience and operational resilience through coordination and surveys across its memberships, and most recently through a set of principles for operational resilience. The BCBS works closely with the BIS and other international financial standard-setting bodies, and its focus on operational resilience and cyber risk builds on the work of its counterparts. For example, in 2019, the BCBS published "Cyber-resilience: Range of Practices," which builds upon a 2017 survey from the FSB and compares how financial authorities approach cyber resilience across jurisdictions.[124]

In August 2020, the BCBS published a consultative document, "Principles for Operational Resilience,"[125] which builds on its 2011 "Principles for the Sound Management of Operational Risk." The new consultation notably broadens the focus beyond cyber incidents to include risks from pandemics, accidents, natural disasters, and technology failures.[126] The consultation period is set to end by November 2020.

Bank for International Settlements

The BIS helps its members manage cyber risk and build resilience through key regulator stocktakes,[127] convenings,[128] consultations, and guidance.[129] In 2018, the BIS hosted two events on cyber resilience: a cybersecurity seminar attended by fifty central banks and monetary authorities and a five-day cyber range exercise in which cybersecurity professionals from fifteen central banks defended against attacks on simulated networks. From these events, the BIS learned that "to be truly effective against the common threat of cyber attack, central banks must work together."[130] Shortly afterwards, the BIS created the CRCC to facilitate such collaboration.

The BIS's CRCC is part of its Innovation BIS 2025 strategy, designed to facilitate collaboration on cyber resilience within the central bank community. According the BIS's annual report, the CRCC will "offer cyber security seminars, technical training with hands-on cyber ranges similar to the one described above, and a secure platform to help build collaboration within the central bank community." In a 2019 speech to regulators, the general manager of BIS, Agustín Carstens, explained that the CRCC will leverage its "trusted position within the central bank community" to provide four core services:

- Developing a cyber resilience self-assessment framework for central bank cyber security benchmarking
- Providing cyber range capability to provide hands-on cyber security training via scenarios that are fully customized for the financial sector
- Providing a secure collaboration platform for multilateral cyber threat information exchange, virtual access to cyber security personnel in other central banks, information technology investment discussions, and best practices in information sharing
- Collaborating closely with the Financial Stability Institute to assist in its delivery of cyber resilience publications and training as well as providing cyber security expertise in relation to emerging financial technology trends[131]

The Financial Stability Institute, established jointly by the BIS and the BCBS, advances research through policy briefs, crisis exercises, and papers on effective cybersecurity and operational resilience practices, along with other financial policy topics.[132] The institute drives capacity-building for supervisors and regulators through four channels:

- Raising awareness around key developments in cyber resilience through a global series of high-level meetings
- Facilitating regional exchanges of experiences and best practices on cyber resilience and cyber risk between supervisors and regulators through regional expert meetings
- Developing online products and tutorials on the work of the international financial standard-setting bodies—the BCBS, IAIS, and CPMI-IOSCO—on cyber resilience
- Publishing research, policy briefs, and environmental scans on supervisory and regulatory developments in cybersecurity and cyber resilience in the financial sector

Because of their cost-effectiveness and scalability, online tutorials will be the focus for future efforts.[133]

Industry's Approach to Operational Resilience

The financial industry generally supports establishing a minimum level of operational resilience across the sector but wants to be involved in developing a regulatory approach that does not overly burden business. Because financial institutions do not view cybersecurity or operational resilience as competitive issues, the industry has developed a consensus-preferred approach: regulations that are simple, internationally harmonized, principles-based, and risk-based and that maximize resilience while minimizing risk. Industry has also launched its own initiatives, mostly in the United States, to advance operational resilience.

The financial industry primarily advocates for regulatory development and reform, including around operational resilience, through trade associations. Some trade associations, like the EBF, align closely with specific regional markets, whereas other trade associations, like the IIF and the GFMA, represent institutions from all over the world. On major issues, like operational resilience, trade associations coordinate to speak to regulators with a unified voice.

Industry has two primary concerns about the global regulatory approach to operational resilience. First, there is significant concern about regulatory fragmentation. In 2016, just as regulators had begun to explore operational resilience, a group of trade associations warned that "fragmentation would not only impede the flow of global capital and its contribution to economic growth, but also exacerbate the very risks regulators are trying to mitigate."[134] In the United States, industry built the "Financial Sector Cybersecurity Profile" to help simplify compliance requirements.[135] According to the FSSCC website, "The Profile is a financial services sector-specific extension of the NIST Cybersecurity Framework (NIST CSF)—and other key guidance documents such as [those created by the International Organization for Standardization (ISO)] and CPMI-IOSCO—to better address the sector's regulatory environment."[136] In Europe, the EBF has warned that "harmonization of regulatory requirements is a standing request of the European banking sector so as to facilitate compliance and avoid duplication and overlapping."[137]

To counter fragmentation, industry wants leadership from international financial organizations. For example, in response to the MAS's proposed BCM guideline revisions, the Asia Securities Industry and Financial Markets Association (ASIFMA) recommended that regulatory requirements be driven by "G20, FSB and the Basel Committee."[138] Industry's desire for harmonization

also explains their advocacy of a common taxonomy and their support for the FSB's cyber lexicon.

Second, industry is concerned about prescriptive requirements and maintains instead that regulators should adopt risk- and principles-based approaches. Trade associations argue that there is no "one-size-fits-all" approach and that regulations need to be proportional to the maturity and systemic importance of the firm. They consider risk- and principles-based approaches to be more future-proof, whereas prescriptive requirements may become irrelevant as technology changes.

In addition to consultation and advocacy with regulators, industry has established sector-led initiatives focused on operational resilience, primarily in the United States. Examples include FSARC and its UK counterpart FSCCC, Sheltered Harbor (a subsidiary of FS-ISAC focused on consumer banking), the Financial Sector Profile, and Quantum Dawn, a series of global sector-led cybersecurity exercises. These initiatives not only improve firms' resilience but also signal to regulators that private sector interests align with those of the public and that future regulatory requirements need not be heavy-handed.

The Growing Popularity of Exercises

Cybersecurity exercises are important for preparedness and resilience because they help institutions think through responses to hypothetical scenarios. Exercises about cyber incidents affecting the financial system help supervisors and banks consider possible repercussions for core bank functions, identify gaps in current response plans, and practice crisis communication and coordination. These exercises may vary from tabletop simulations to penetration tests. Leading financial institutions make these exercises routine to strengthen coordination among government agencies, supervisors, and the private sector. Some of the major exercises include:

- **Quantum Dawn:** The Quantum Dawn exercise series hosted by SIFMA dates back to 2011. Over the course of the five exercises held since then, participation has grown from a small group of U.S. institutions to more than 180 global financial institutions as of 2019. Each exercise has simulated a different set of cyber incidents, but the post-event lessons from every exercise have consistently called for better communication among participants. Quantum Dawn V, held in 2019, simulated a targeted ransomware attack with impacts on major banks across the globe, starting in the United States and moving

across Asia and the UK; the exercise boasted over 600 participants from 180 financial institutions.[139] The exercise tested coordination between SIFMA, the Association for Financial Markets in Europe (AFME), and ASIFMA.

- **Cyber-attack Against Payment Systems (CAPS):** FS-ISAC regularly hosts CAPS, a series of tabletop exercises, with its membership institutions. The exercise aims to help participants prepare for attacks against their systems and processes.[140]
- **Exercise Cyber Star:** Led by Singapore's CSA, Exercise Cyber Star is a periodic crisis exercise that tests the cybersecurity readiness and response capabilities of stakeholders across Singapore's eleven critical information infrastructure sectors, including banking and finance.
- **Exercise Raffles:** Jointly organized by the MAS and the ABS, this financial sector exercise tests financial institutions' business continuity and crisis management against operational disruption scenarios. The three most recent iterations of the exercise (in 2014, 2017, and 2019) focused on cyber attack scenarios, with the most recent exercise being held over two days and covering banking and payment service disruptions, trading disorders, data theft, and the spreading of rumors and falsehoods on social media.
- **Waking Shark:** The Waking Shark exercises I and II simulated cyber attacks on the UK's financial sector in 2011 and 2013 respectively. Participants represented major financial institutions, financial market infrastructure providers, financial authorities, the UK Treasury, and other government agencies.[141]
- **SIMEX18:** In 2018, as part of the SIMEX series, UK financial authorities simulated a significant multiday cyber attack on the UK's financial sector with participation from "29 of the most systemically important firms and financial market infrastructures."[142] The exercise prompted a review of the sector response framework and the integration of the FSCCC into the response framework.
- **Hamilton Series:** The Hamilton Series consists of exercises led by the U.S. Department of the Treasury to improve U.S. response to cyber threats within the financial sector. The exercises include participants from both the public and the private sector to stress test and improve public-private response strategies.[143] U.S. government agencies, including the Department of Homeland Security, regulators led by the Financial and Banking Information Infrastructure Committee, and law enforcement participate alongside industry partners like the Financial Services Sector Coordinating Council (FSSCC) and FS-ISAC.[144]
- **Resilient Shield:** In 2015, the British and U.S. governments conducted one of the first international exercises with the private sector to strengthen coordination and response planning.[145]

- **UNITAS:** In June 2018, the ECB hosted a market-wide crisis communication exercise, known as UNITAS, to simulate an attack on a major financial market infrastructure. According to the ECB, the aim was to: "(i) raise awareness of data integrity issues and the implications for financial infrastructures; (ii) discuss how impacted financial infrastructures could cooperate and collaborate with each other and other relevant stakeholders on a pan-European basis; and (iii) assess the need for developing external public communication strategies."[146]
- **G7 cybersecurity exercise:** In June 2019, twenty-four financial authorities from G7 countries participated in a "major cross-border cyber-security attack on the financial sector."[147] Some G7 countries invited private financial institutions from their jurisdictions to participate, while others limited participation to government agencies.[148]

In 2019, the UK NCSC even published "Exercise-in-a-Box," a free and simple online tool that helps organizations practice responding to a cyber attack.[149] The tool uses a basic profile of the participants' institution and provides a tailored scenario based on the institution's level of cybersecurity maturity. After the exercise is completed, participants receive a summary report with key takeaways and recommendations to improve their institution's cyber resilience. This could become an effective tool for cybersecurity capacity-building enabling participants to live and think through the implications of a cyber incident in a controlled setting.

Recommendation 1.1: Standard-setting bodies—namely the Basel Committee on Banking Supervision (BCBS), the Committee on Payments and Market Infrastructures (CPMI), the International Organization of Securities Commissions (IOSCO), and the International Association of Insurance Supervisors (IAIS)—should continue to support initiatives to improve and align regulatory oversight efforts for the cybersecurity and operational resilience of financial services. This will contribute to higher quality security practices among financial firms by reducing regulatory transaction costs and freeing up bandwidth among firms' cybersecurity staff.

- *Supporting Action 1.1.1*: The G20 should task the FSB with developing a baseline framework for the supervision of cyber risk management at financial institutions. This framework should leverage common risk management frameworks, such as those advanced by the Financial Stability Institute and the Financial Services Sector Cybersecurity Profile, as well as internationally accepted standards for technology and risk controls.

Specific Issues Worth Highlighting: Promising Opportunities, Urgent Topics, and Low-Hanging Fruit

FinCERTs

The ability to respond quickly and effectively to a cyber incident is fundamental to recovery and operational resilience. CERTS and CSIRTs specialize in response; they have been described as "digital fire brigades."[150]

Over the last twenty years, an ecosystem of CERTs that specialize in responding to incidents in the financial system has emerged—some of which are explicitly called "FinCERTs."[151] FinCERTs specialize in responding to cyber incidents in financial networks, core banking systems, and payment systems. Most FinCERTs are operated by large banks to respond to incidents on their internal networks. Recently, financial regulators have begun establishing their own FinCERTs to respond to incidents within their jurisdiction. Figure 6 shows their existence around the globe.

In addition, many national CERTs and cybersecurity agencies operate substructures that specialize in financial sector cybersecurity. While the national-level CERTs and cybersecurity agencies are officially sector-agnostic, these substructures often fulfill the same function as that of a standalone FinCERT: facilitating information sharing, responding to cyber incidents, and building public-private trust.

However, the ecosystem of FinCERTs and national substructures is fragmented, and cooperation occurs on an ad hoc basis. There is no sector-wide coordinating body that connects FinCERTs across jurisdictions or bridges the public-private divide. (FS-ISAC is not a CERT since it does not perform incident response functions.[152]) Connecting the emerging system of FinCERTs will likely improve global responses to rising cyber threats to the financial system.

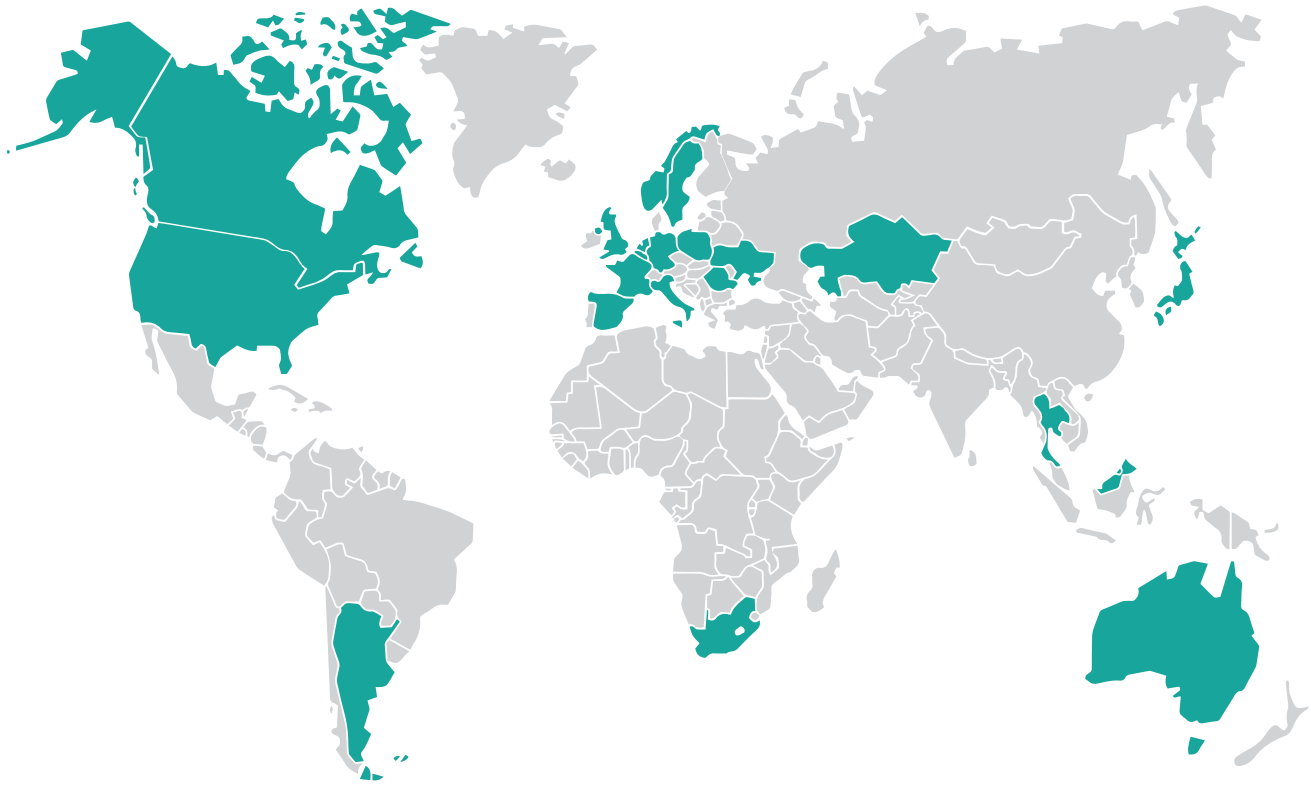
Mapping the FinCERT Ecosystem

While there is no sector-wide coordinating body for FinCERTs, two organizations—FIRST and the Task Force on Computer Security Incident Response Teams (TF-CSIRT)—provide global platforms with the "aim of sharing information among CSIRTs and assisting coordination during network-wide incidents."[153] Neither have operational functions, but most FinCERTs are members of one or both platforms.

Most FinCERTs can be categorized as either (1) CERTs operated by financial institution CERTs, or (2) CERTs operated by public financial authorities.

A survey of the directories of FIRST and TF-CSIRT shows that there are at least sixty-eight FinCERTs operating today: thirteen are public, and fifty-five are private.

Figure 6: Countries With Public Sector FinCERTs



Source: For a full list of FinCERTs, see: Forum of Incident Response and Security Teams, "FIRST Teams," accessed September 30, 2020, https://www.first.org/members/teams/; Trusted Introducer Service, "Directory," Task Force on Computer Security Incident Response Teams, accessed September 30, 2020, https://www.trusted-introducer.org/directory/index.html.

Public Sector FinCERTs

Governments have long been operating CERTs at the national level to respond to incidents that occur on government or commercial networks, including networks operated by the financial industry. The EU's NIS Directive requires member states to establish national CSIRTs and supervise critical sectors like the financial sector.[154] What is new is that central banks and ministries of finance are establishing their own FinCERTs to create specialized response and recovery capabilities for the financial sector. One advantage of housing a

FinCERT within a financial regulatory body is increased authority to request information and data sharing from private financial institutions.[155] Many, like Sri Lanka's FinCERT, were established in collaboration with private financial institutions and trade associations.

Another example of a public-private FinCERT is the Italian CERTFin, which is led jointly by the Bank of Italy and the Italian Banking Association. Participation in CERTFin is open and any financial institution or service provider operating in Italy's financial sector can opt in.

According to its mission statement, CERTFin's main goals are:

- "To provide prompt information regarding potential cyber-threats that could damage banks and insurance organizations;
- To act as Point of Contact between financial operators and other relevant public institutions as far as cyber protection;
- To facilitate the response to large-scale security incidents;
- To support crisis management process in case of cyber incidents;
- To cooperate with national and international institutions and other actors, from both public and private sector, which are involved in cyber security, by promoting the cooperation among them; and,
- To improve cyber-security awareness and culture."[156]

CERTFin coordinates incident response and acts primarily as an information gathering center for affected constituents. In the event of a major cyber incident, CERTFin also functions as a conduit between cybersecurity operators in the financial sector and the Italian national CERT through a dedicated escalation process. CERTFin also prioritizes operational cooperation and information sharing with other CERTs, considering such activity "of paramount importance."[157]

Europe has established the majority of FinCERTs. One standout example of multilateral cooperation is the Nordic Financial CERT, operated jointly by Sweden, Norway, Iceland, Denmark, and Finland. Efforts by the ENISA and TF-CSIRT to coordinate CERTs and CSIRTs across Europe may contribute to the culture of collaboration in the European CERT community.[158] Additionally, the fact that the ECB has its established CSIRT-ECB may encourage national central banks to create their own.

Israel's FinCERT: The Cyber and Finance Continuity Center (FC3)

Israel's national FinCERT, FC3, is worth highlighting. FC3 provides specialized cybersecurity capabilities focusing specifically on the financial ecosystem and its needs.[159] It also provides a set of services to its customers, including information sharing, incident handling, and situational reports.

FC3 was established after a cybersecurity exercise with the country's financial leadership revealed "a need for integration and 'translation' between the financial language, the cyber and technology language and the risk management needs."[160] It is co-owned and co-managed by the Israeli Ministry of Finance and the Israeli National Cyber Directorate, which provide expertise in the financial ecosystem and in cyber and technology, respectively. This coordination has allowed FC3 to comprehensively map Israel's financial sector processes, systems, and functions to improve resilience. Additional synergies are realized because FC3 is headquartered on the same campus as university experts and Israel Defense Forces cybersecurity experts.

Israel's experience establishing a national FinCERT may be instructive for other countries. According to FC3's leadership, the following process led to the creation of the FinCERT:

1. A government directive that promoted government regulation and leadership in developing cybersecurity protection.

2. Drills for the leaders of the financial ecosystem and security agencies in identifying gaps; these drills were also used to catalyze improved cybersecurity protection.

3. A government committee that drove deeper internal processes; this committee was led by the Ministry of Finance and brought together all of the country's financial regulators, the central bank, and cyber authority.

4. Identification of the financial ecosystem players and mapping of the protection layers.

5. Definition and mapping of end-to-end financial processes.

After several months of consultation and resource mapping, the government committee decided to disband and move directly into creating the financial CERT.[161]

The Israeli government took away valuable lessons from the process. Notably, FC3 was "the first sectorial CERT that was created and is now part of several sectorial CERTs—each one focuses in a different sector, and utilizes capabilities, knowledge and tools that are provided by the national CERT."[162] According to FC3 leadership, key lessons include:

- Create a workforce with experts from financial institutions, technology experts, and managers who have experience working with the financial regulators.
- Develop additional channels for collaboration with the private sector, such as a steering committee, conferences, and internships for financial CERT employees in private financial institutions and vice versa.
- Quickly begin using online tools for institutions to receive information and share data.
- Work incrementally: all of the financial institutions were connected voluntarily to the financial CERT, allowing trust, value, and cooperation to emerge.
- Create an ongoing process that allows growth and empowerment in technology, people, processes, and intelligence across financial sectors in the national and international arenas.[163]

Recommendation 1.2: Governments (starting with the G7 and G20 Finance Ministers and Central Bank Governors) and industry should expand and strengthen the international ecosystem of financial sector-focused computer emergency response teams (CERTs) or similar entities to stimulate public-private collaboration and strengthen sector-specific security.

- *Supporting Action 1.2.1:* Governments should create a FinCERT, either as a substructure of an already established national CSIRT (computer security incident response team) emulating the Israeli FinCERT or as a stand-alone entity, to strengthen the protection of the financial sector, which is often at the forefront of regular and novel malicious cyber activity.

- *Supporting Action 1.2.2:* The Forum of Incident Response and Security Teams (FIRST) should consider creating a stand-alone track or side event at the annual FIRST conference to deepen this community of experts, including government FinCERTs, staff of national CSIRTs focusing on the financial sector, and related private sector entities. Two or more members of FIRST should also propose a FinCERT "Special Interest Group" to the FIRST board to create a community of interest in addition to the annual side event. (This would be similar to the national CSIRT side event that takes place alongside the annual FIRST conference. Appendix B provides an overview of existing FinCERTs worldwide.)

Sheltered Harbor

Sheltered Harbor is designed to improve the resilience of and preserve public confidence in the U.S. financial system, specifically with respect to the integrity of financial data. It functions as a fail-safe to restore financial data for banks and customers in the event of a major disruption. The main idea is that should a financial institution be unable to recover quickly from a cyber incident, other financial firms could jump in and continue to provide service to affected customers by accessing the struggling firm's standardized, backed-up account data through the Sheltered Harbor data vault.[164]

Sheltered Harbor was conceptualized after the 2015 Hamilton Series showed financial institutions how damaging a major data loss or disruption would be to financial stability.[165] A group of thirty-four financial institutions, clearing houses, core processors, and industry associations came together in 2016 to create the initiative.[166] As of October 2018, Sheltered Harbor holds the data for 70 percent of U.S. deposit accounts and 55 percent of U.S. retail brokerage client assets.[167]

Participation in Sheltered Harbor is voluntary; member institutions must pay minor dues and meet certain standards. In a public letter sent to financial CEOs in May 2019, six U.S. financial trade associations called for all financial institutions to join Sheltered Harbor, arguing that "implementing the Sheltered Harbor standard prepares institutions to provide customers timely access to balances and funds in such a worst-case scenario."[168]

An excerpt from that public letter explains how Sheltered Harbor works:

> Financial institutions back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own secure data vault or using a participating service provider. The data vault is owned and managed by your institution, is unchangeable, and is completely separated from your institution's infrastructure, including all backups. When your institution completes the requirements for data vaulting, you will be awarded Sheltered Harbor certification. This designation and accompanying seal communicate to key audiences, such as customers, industry peers, and regulatory agencies, that your critical customer account data [are] protected.[169]

Regulators have received the private sector–led initiative well. For example, two U.S. regulators, the OCC and the FDIC, promoted Sheltered Harbor to

financial institutions in a "Joint Statement on Heightened Cybersecurity Risk" following the U.S. killing of Iranian general Qasem Soleimani.[170] Additionally, the U.S. Federal Financial Institutions Examination Council included Sheltered Harbor in their 2019 "IT Examination Handbook" and 2018 "Cybersecurity Resource Guide for Financial Institutions."[171]

Recommendation 1.3: Financial authorities should prioritize increasing the financial sector's resilience against attacks targeting the integrity of data and algorithms. Unlike incidents affecting availability or confidentiality, few technical mitigation solutions exist today to mitigate the risks associated with the manipulation of the integrity of data and algorithms. The second-order risk of undermining trust and confidence is significant.

- *Supporting Action 1.3.1:* Financial authorities should encourage industry to join or emulate data vaulting initiatives, such as Sheltered Harbor, to advance common standards, to better protect against data integrity attacks such as ransomware, and to test data vaulting solutions' effectiveness during a crisis.

- *Supporting Action 1.3.2:* Considering the limitations of current technical solutions, governments and financial authorities should lead whole-of-society exercises, including industry, that specifically simulate cyber attacks involving the manipulation of the integrity of data and algorithms. Such exercises should be used to identify weaknesses, such as divergence between decision-making timelines in financial markets versus the national security community, and to develop action plans to better protect against such attacks.

Exchanges and Other Financial Infrastructures

> "Banks tend to have the loudest voice but governments need to focus more on exchanges."
> —Expert at Carnegie's FinCyber Brainstorming Workshop in May 2020.

Financial infrastructures include FMIs (that is, payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories), credit rating agencies, stock exchanges, securities settlement platforms, and any other service providers deemed critical

for the functioning of the financial sector.[172] Their systemic importance in the financial system demands a high standard of resilience. For example, the first internationally agreed upon guidance on cyber resilience was about FMIs, published by CPMI-IOSCO in 2016. In 2019, the ECB published the CROE, which provides guidance to FMIs and supervisors regarding cyber resilience expectations.[173]

Financial infrastructure operators do have unique concerns about operational resilience. For example, in comments to CPMI-IOSCO, the WFE raised concerns about a prescriptive recovery time of two hours. As Darrell Duffie and Joshua Younger explained, "the CPMI standard for the cyber resilience of financial market infrastructure is a two-hour recovery time, or '2hRTO,' but this standard remains aspirational."[174] There are also concerns about independent assurance of data integrity in the event of an incident: in order to independently assure data integrity, an FMI would need to establish a point of reliability loss, invalidate transactions submitted after that point, and return to the previous checkpoint. This also raises questions about whether and to what extent legal provisions around settlement finality may need to be updated.

Nevertheless, financial infrastructure operators seem broadly supportive of a regulatory approach based on operational resilience, and the interests of financial infrastructure operators typically align with those of other financial institutions. Resistant to prescriptive supervision and regulation, they advocate for proportionality, and they are concerned about the international harmonization of cybersecurity regulatory approaches. In a March 2020 response to the EC's consultation, the WFE affirmed support for policymakers' efforts "to enhance operational resilience," but urged them to align new rules with existing ones, as this "would be helpful in quickly realising and implementing those common principles across an interconnected, global financial services industry."[175] Financial infrastructures are built on consumer trust, so establishing a resilient financial system is also broadly in their interest. This is especially true given the evolving threat landscape in which financial infrastructures operate.

Threat Landscape for Exchanges and Clearing Houses

A 2013 survey by the WFE and IOSCO found that 53 percent of exchanges surveyed reported experiencing a cyber attack in the previous year and that 89 percent of respondents considered cyber crime in securities markets to be a systemic risk. The survey also found that attacks against exchanges tend to be disruptive rather than profit-driven.[176] This clearly differentiates exchanges from banks and other financial institutions: exchanges are focused on traders

and corporate clients and do not hold personal accounts that can be targeted, as happens, for example, in carding. Instead, a DDoS campaign against the New Zealand Stock Exchange in August 2020 led to multiday disruptions of its operations and was a powerful reminder of the continued threat to, and importance of, exchanges for a country's financial sector.[177]

A string of successful profit-driven attacks—including one via the SWIFT network against the Bangladesh Bank in 2016; one against Mexico's interbank payment network, SPEI, in 2018; and one against Banco de Chile in 2018 via international payment systems—have also focused attention on attacks against participants within financial payments systems.[178] In 2018, SWIFT and BAE Systems examined potential threats to foreign exchange markets, securities markets, and trade finance markets. They found that:

> The cyber threat is highest in the securities markets, particularly to its Participants. This is due to the large numbers of Participants and infrastructures in that market, the complexities of their interactions, and inherent characteristics such as long chains of custody, unstructured communications and trusted practices—all of which combine to provide opportunities for [Advanced Persistent Threat] groups to exploit.[179]

Profit-driven attackers usually target low-hanging fruit in emerging financial markets, but this could change. As BAE analysts point out, attackers "might choose to attack foreign exchange markets, trade finance, securities and other areas, looking to make large gains in single intrusions or use persistent access to play the market over longer periods."[180] Successful attacks against systemically important exchanges or clearing houses would be highly complex but highly profitable for malicious actors.

Politically motivated attacks that aim to disrupt exchanges and clearing houses may also pose a systemic risk to the financial system and could create market volatility, settlement issues, and trade inconsistencies. Disruptions to a systemically important exchange or clearing house could have cascading consequences for the larger financial system. Attacks that call into question the integrity of an exchange's transactions or data could undermine trust in the financial system and require a great deal of time, effort, and funds to resolve.

Past examples of politically motivated disruptions include 2012 DDoS attacks against U.S. exchanges; a 2014 data breach involving the Warsaw Stock Exchange, reportedly carried out by a group affiliated with the self-proclaimed Islamic State; and 2019 DDoS attacks against Hong Kong Exchanges and Clearing Limited.[181]

Recommendation 1.4: Governments and industry should put additional emphasis on the resilience of financial market infrastructures (FMIs)—critically important institutions responsible for payment systems, central counterparties, central securities depositories, or securities settlement systems—and other service providers deemed critical for the functioning of the financial sector, such as stock exchanges, as successful disruptions against these entities can pose a systemic risk and undermine confidence in the financial system.

- *Supporting Action 1.4.1:* Governments should use the unique capabilities of their national security communities to help protect FMIs and critical trading systems, including sharing information about impending threats.

- *Supporting Action 1.4.2:* Industry groups, such as the World Federation of Exchanges (WFE), which is a global industry association for exchanges and clearing houses, should dedicate more resources to capacity-building efforts designed to help smaller and less mature FMIs and other important service providers increase their cybersecurity level.

Third-Party Risk

Financial services firms increasingly rely on services and a complex digital supply chain provided by third parties. This trend has accelerated further during the coronavirus global pandemic as the financial sector transitioned to remote work and expanded digital services. Third-party risk, or outsourcing risk, is not a new concept to financial authorities and institutions. What is new is the degree of interdependent risk, the increasing complexity of that interdependence, and the number of actors involved in managing the risk. This growing interdependence can be exploited by malicious actors who, for example, may choose to target vulnerable third-party service providers with ransomware because the leverage gained by disrupting not only the service provider but also its dependent customers can make extortion more successful.

Financial authorities have traditionally managed third-party risk in the system by setting outsourcing requirements for financial institutions. However, concerns are growing that financial authorities do not have enough visibility or authority over certain third-party service providers, and that financial institutions are expected to manage risks in oligopolistic markets where they have less leverage to set the terms of service level agreements.

New regulation and guidance reflect these growing concerns. The MAS's 2019 updates to its BCM guidelines raise the standards for financial institutions developing business continuity plans so that those plans better account for linkages with external service providers.[182] The BCBS has proposed "third party dependent management" as one of its core "principles for operational resilience." Such approaches provide financial institutions with flexibility, and responsibility, to manage these outsourcing relationships. The EU may be going one step further with DORA, which proposes a framework that would enable "continuous monitoring of the activities of ICT third-party service providers that are critical providers to financial entities."[183]

The Cloud

The increasing reliance on cloud services has been highlighted during the coronavirus pandemic. According to a March 2020 Business Insider article, "projections of moving 55% of workloads to the cloud by 2022 (from 33% now) look conservative as these targets could be reached a full year ahead of expectations given this pace."[184] Nasdaq, for example, has further accelerated its planned migration to the public cloud.[185] Cloud infrastructure also plays an important role for innovation as many start-ups, including in fintech, are "cloud native," using cloud service providers from the start to avoid having to build (and pay for) their own IT infrastructure.

> "A quarter of major banks' activities and almost a third of all UK payments activity are already hosted on the Cloud, and there are considerable opportunities for even more intense usage." Remarks by Mark Carney, Governor of the Bank of England, in June 2019.[186]

When thinking about the risk implications of the cloud for the financial system, two different public policy problems are relevant: an *existing* public policy problem and an *emerging* one. The existing public policy problem is the rising cost of cyber attacks and the fact that most organizations—governments and companies—cannot effectively protect themselves. Very few organizations can rival the security teams of the large cloud service providers and they are therefore better off entrusting their security to teams at cloud service providers or other third-party service providers.[187] The emerging public policy problem is the concentration risk associated with such a centralized approach.

Lawmakers and financial supervisory authorities have grown increasingly concerned about the emerging risk associated with the growth of the cloud. In 2019, two members of the U.S. Congress urged the U.S. Department of

SPOTLIGHT

For more background information about the cloud, security, and public policy, see the Carnegie paper "Cloud Security: A Primer for Policymakers," co-authored by Tim Maurer and Garrett Hinck (August 2020): https://carnegieendowment.org/2020/08/31/cloud-security-primer-for-policymakers-pub-82597

the Treasury to designate the leading cloud service providers to the financial industry as systemically important.[188] Financial authorities outside the United States increasingly lament their inability to assess risks associated with cloud service providers that are primarily located in the United States or China.

The current geopolitical landscape makes a multilaterally coordinated governance approach to cloud service providers highly unlikely. While such an arrangement would not be unprecedented (consider, for example, the SWIFT governance model), it is much more likely that a fragmented regulatory approach will emerge. This fragmentation will be characterized along two dimensions. In the first, fragmentation will emerge among jurisdictions as individual countries and small groups of like-minded countries create their own regulatory frameworks. In the second, fragmentation will emerge across sectors as individual sectors start to impose regulations affecting cloud service providers through, for example, third-party provisions.

Given the current climate, it is also difficult to envision a scenario where the United States or China would agree to a multilateral governance arrangement without being in the driver's seat. After all, nearly all major cloud service providers are located in the United States and China. Although other countries will try to extend their own regulatory authority to cloud service providers, either reaching beyond their borders or forcing companies to store and process data locally, cloud service providers will likely behave like other firms have in the past. Depending on the market, they will either (a) comply with the regulation only for the largest and most important markets such as the United States, (b) communicate that they comply with other countries' individual regulations de jure while de facto only using a few jurisdictions internally as benchmarks, or (c) decide to leave markets with overly onerous regulatory burdens or not to enter them in the first place.

In short, it is unlikely that a regulatory approach will effectively address the growing security concerns about cloud service providers in the near to medium term. The regulatory trend is overwhelmingly toward fragmentation and away from coherence, and this state of affairs is likely to continue for years. This raises the question: What can realistically be done to improve the security and resilience of cloud service providers within the next five years? The recommendations in this report focus on a few actionable measures that could help mitigate the risk independent of the broader governance questions.

Recommendation 1.5: Financial authorities, or a designated lead governmental agency, should (i) assess the benefits and risks of using cloud service providers to strengthen the cybersecurity of financial institutions that lack the capacity to effectively protect themselves and (ii) take steps to minimize the risks associated with a migration to the cloud, including potential concentration risk.

- *Supporting Action 1.5.1:* Financial authorities, or a designated lead governmental agency, should assess which financial institutions, especially small and medium-sized organizations, would become more resilient against cyber attacks by migrating to appropriately secured public or hybrid cloud service providers.

- *Supporting Action 1.5.2:* To better assess and address growing concerns about concentration risks, governments should work with the major cloud service providers and financial institutions to:

    - Organize annual joint exercises simulating different scenarios to (a) identify internally who would lead their firms during a global cyber disruption; (b) increase cooperation among cloud service providers in building international response and recovery capabilities; and (c) strengthen the resilience of the cloud service infrastructure, as disruption of one provider could lead to service disruptions and reputational damage for all providers in a worst-case scenario.

    - Assess systemic risks, as well as existing and potential mitigations, and share information about key vulnerabilities and threats. The goal is to provide coordinated analysis and identify potential systemic risks for critical functions shared by cloud service providers and to create a playbook for when an incident occurs.

    - Although the activities listed above have been piloted in other industries in line with anti-trust provisions, governments should express their support and provide guidance by issuing public statements clarifying their position.

- *Supporting Action 1.5.3:* Financial authorities should monitor whether the market, through cloud service providers and third-party consulting firms, is providing financial services firms with

sufficient resources to assist with the migration to public or hybrid cloud service providers; this information will allow them to minimize the transitory risk and otherwise take supplementary actions. Publishing these findings will improve market information and allow potential cloud customers to assess benefits and costs more accurately.

- *Supporting Action 1.5.4:* National security agencies should consult critical cloud service providers to determine how intelligence collection could be used to help identify and monitor potential significant threat actors and develop a mechanism to share information about imminent threats with cloud service providers.

Data Privacy, the GDPR, and Challenges to Information Sharing

Ensuring data privacy is fundamental to the operation of the financial ecosystem and the financial institutions therein. However, "data privacy" (the proper protection and handling of personal data) and "data security" (the protection of data from unauthorized access) are not the same. There has been some confusion as to whether recent data privacy regulation, in particular the EU's GDPR, may have unintended consequences for cybersecurity in the financial system. Specifically, some are concerned that the GDPR's protections of personal data could hamper cybersecurity threat information sharing.

For example, one legal assessment, produced in 2018 on behalf of FS-ISAC, concluded:

> The exact impact of GDPR on international threat information sharing appears not fully understood. There should be no misunderstanding: threat information sharing, undertaken in a proper and controlled manner, is a lawful enterprise under GDPR. Article 6(1)(f) holds as lawful the processing of personal data that "is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject", requiring protection of the personal data. The processing of personal data in threat information by FS-ISAC and its Members, as well as other ISACs, member organizations, and governmental entities meets this criteria.[189]

Feedback from regulators and industry experts suggests that governments and regulators may need to provide further clarification so as to remove any doubt among financial institution's legal counsels (including data protection officers) that could potentially undermine cybersecurity efforts. Confusion seems to exist specifically with respect to the sharing of potentially personal data (for example, IP addresses, email addresses, and related metadata), which are often linked to business email compromise, as well as with sharing profiles of malicious actors and anonymized tactics, techniques, and procedures.[190]

This uncertainty and reluctance are not in the public interest as they can degrade a financial institution's ability to protect against and respond to cyber attacks targeting systems and data under their care (including attacks on personal data, the protection of which is the key justification for the GDPR). Specifically, if financial institutions limit their information-sharing arrangements because of a perceived risk of incurring GDPR-related fines (and the subsequent reputational impact), it could undermine the cybersecurity not only of the institutions themselves but of the entire financial system. In Europe, initiatives like CIISI-EU have had to overcome such hurdles, often caused by participants' legal counsels having a very narrow interpretation of the GDPR's applicability in such cybersecurity arrangements.[191]

Data protection regulations usually include specific reasons that can justify cybersecurity threat information sharing within the financial system. For example, GPDR justifies information sharing in cases of national security and the public interest.[192] However, without further clarification from governments that these justifications apply to cybersecurity threats, industry will opt to avoid risk more often than not.

EU member countries may choose to interpret the cybersecurity of their financial system as a national security issue under Part 2, Chapter 3 of the Data Protection Act 2018.[193] However, this measure is geared toward national cybersecurity and law enforcement authorities; embracing such an interpretation would run counter to the international and interdependent nature of the financial system. Treating financial cybersecurity as a national security issue may inhibit cross-border information sharing and undermine the cybersecurity of the EU's digital single market and of the international financial system more broadly. Cybersecurity threat information sharing in the financial system may more appropriately fall under the public interest justification as outlined in Article 6 (1)(e) of the GDPR.[194] The public interest justification may not face the same potential barriers to cross-border sharing that face the national security justification.

Ultimately, it would be ironic if confusion about data protection regimes led the financial industry to reduce cybersecurity threat information sharing and resulted in weaker protections for personal data held in the purview of financial institutions. Since the GDPR is seen internationally as a leading model in data privacy and is used as a template for data protection regulations around the world, Europe has an opportunity to clarify this important issue and set an example that would help countries beyond Europe's borders avoid this conflict in their own privacy frameworks.

Recommendation 1.6: G20 Finance Ministers and Central Bank Governors should highlight, ideally in their 2021 communiqué, the necessity of cybersecurity threat information sharing—including being clear about what information should be shared, why, with whom, how, and when—in order to protect the global financial system.

- *Supporting Action 1.6.1:* Data protection regulators (for example, the European Data Protection Board), together with financial authorities, should assess the impact of data protection regulation on different cyber threat information-sharing initiatives and clarify, where necessary, that such sharing arrangements serve the public interest and that they comply with the General Data Protection Regulation (GDPR) or other relevant regulations.

- *Supporting Action 1.6.2:* Governments should assess the potential negative impact of broader data localization requirements on the ability to protect against cyber threats and consider actions to balance these different policy objectives.

Influence Operations and Deepfakes in the Context of the Financial System

Financial markets are shaped by their information environments. The internet has transformed how information flows through financial markets. This creates new ways for actors to manipulate information in financial markets for malign purposes—for example, through influence operations. The FSB's consultative document "Effective Practices for Cyber Incident Response and Recovery" highlights the "sector-wide implications of a cyber incident, including any market confidence issues arising through, for example, social media, news media, and market reactions."[195]

Influence operations are the organized attempt to achieve a specific effect among a target audience.[196] They employ a variety of tactics, techniques, and messaging, including disinformation (the deliberate spreading of misleading or false information), astroturfing (creating the illusion of a grassroots movement), hack-and-leaks, and other cyber attacks.

Recent attention paid to influence operations has focused on the threat to political processes, especially elections, but little attention has been paid to how influence operations affect financial markets. Influence operations targeting financial markets are not new, and innovating technologies continue to empower their speed, scale, and scope. It is therefore prudent to examine whether and how modern influence operations could pose a threat to the financial system.

Influence operations that might threaten the financial sector can be broadly split into two categories based on target and aim: (1) operations that target a specific business, brand, or institution (mostly led by criminals and competition); and, (2) operations aimed at overall markets or a country (mostly led by nation-states and terrorist groups).

The first category of influence operations, those targeting individual firms, is generally profit-driven and carried out by individuals, criminal organizations, or lobbyists. Organized actors will spread fraudulent rumors to manipulate stock prices and generate profit based on how much the price of the stock was artificially moved. Firms and lobbyists use astroturfing campaigns, which create a false appearance of grassroots support, to tarnish the value of a competing brand or attempt to sway policymaking decisions by abusing calls for online public comments. Fortunately, while these operations might cause short-term financial harm, because they are precise in their targeting, they pose little systemic risk to the financial system.

The second category of influence operations, those aimed at the overall market, is rare and more challenging to carry out but may pose systemic risk, at least temporarily. Attacks in this category are likely to be carried out by a politically motivated actor like a terrorist group or even a nation-state. This type of influence operation may directly target the financial system to manipulate markets, for example, by spreading rumors about market-moving decisions by central banks. Alternatively, influence operations may aim to spread false information that does not directly reference financial markets but that causes financial markets to react. For example, the state-sponsored Syrian Electronic Army caused the U.S. stock market to briefly lose $136 billion in value by disseminating false news on Twitter in 2013 (see Figure 7).[197]

Figure 7: Fake Tweet via Associated Press Twitter Account Impacts Stock Market

Source: Shawn Langlois, "This Day in History: Hacked AP Tweet About White House Explosions Triggers Panic," *MarketWatch*, April 23, 2018, https://www.marketwatch.com/story/this-day-in-history-hacked-ap-tweet-about-white-house-explosions-triggers-panic-2018-04-23.

It is important to note that not every part of an influence operation is malign. Operations may make use of a mix of social media and online advertising that then crosses over to mainstream media with the goal of spreading disinformation across these various platforms. In addition, the accidental spread of false or misleading information, even if not connected to an influence operation, should also be a concern.

On May 13, 2019, a false rumor circulating on WhatsApp led to a minor run on Metro Bank, a commercial bank in London. One posting read: "Urgent . . . You need to empty as soon as possible. The bank is facing lot of financial difficulties [sic]."[198] The false information was made more credible due to a mistake Metro Bank had made months earlier when it failed to hold sufficient capital to meet UK regulatory requirements.[199] While minor, the incident illustrates how misinformation can affect financial institutions.

The problem is that while organizations tend to be good at having playbooks, they are bad at organizing how to respond. A good indicator of an organization's ability to respond quickly is the number of people required to review and sign off on a statement or tweet in response to an incident: an organization that needs clearance from multiple people will inevitably be less nimble. Another indicator is whether a playbook envisions a response only as a press statement or includes plans to respond across platforms; social media in particular requires repeated and persistent messaging to quickly counter any potential influence operation.

Recommendation 1.7: Financial authorities and industry should ensure they are properly prepared for influence operations and hybrid attacks that combine influence operations with malicious hacking activity; they should integrate such attacks into tabletop exercises (such as the G7 exercise) and apply lessons learned from influence operations targeting electoral processes to potential attacks on financial institutions.

- *Supporting Action 1.7.1:* Major financial services firms, central banks, and other financial supervisory authorities should identify a single point of contact within each organization to engage with social media platforms for crisis management. Quick coordination with social media platforms is necessary to organize content takedowns. Social media platforms will be more responsive to a single collective point of contact than to ad hoc communication with many financial institutions.

SPOTLIGHT

Rapid advances in artificial intelligence (AI) are enabling novel forms of deception. AI algorithms can produce realistic deepfake video and audio clips—which show people saying and doing things they never said or did—as well as fake photos and writing. Collectively called synthetic media, these tools have already been documented in multiple financial crimes.

Synthetic media are unlikely to pose a serious threat to the stability of the global financial system or national markets in mature, healthy economies. But they do present risks to emerging markets and to developed countries experiencing financial crises, and they can harm individually targeted people, businesses, and government regulators. Technically savvy bad actors who favor tailored schemes are more likely to incorporate synthetic media, although many others will continue to rely on older, simpler techniques.

Three malicious techniques (further described in the paper cited below) are particularly worrisome and should be prioritized in any response: deepfake voice phishing (or "vishing"), fabricated private remarks, and synthetic social botnets. The latter two are "broadcast" attacks that spread widely via social and traditional media, much like politically themed deepfakes. But deepfake vishing is a novel "narrowcast" threat, tailored and delivered directly to a small audience. This threat is more distinctive to the financial sector and presents an opportunity for policy leadership.

The financial system should take an incremental approach to synthetic media: start with small steps to stay ahead of this emerging challenge without diverting too many resources from larger, already extant threats. This will require a range of actors, both inside and outside the financial sector, to collaborate on technological solutions, organizational practices, and broad public awareness.

To learn more, including about the ten specific scenarios explored as part of this research, see the Carnegie FinCyber working paper "Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios," by Jon Bateman (July 2020): https://carnegieendowment.org/specialprojects/fincyber/workingpapers/

- *Supporting Action 1.7.2:* Financial authorities, financial services firms, and tech companies should develop a clear communications and response plan focused on being able to react swiftly. A quick response can effectively dampen the effect of an incident, but conventional communication channels are often insufficient to fill the information vacuum in such an event. Given the speed of social media content sharing, limiting the number of people required to review and approve a response is essential for a swift response. Financial institutions should ensure potential influence operations are part of their cyber-related communications planning and be familiar with the rules on platforms relating to key areas, including impersonation accounts and hacked materials.

- *Supporting Action 1.7.3:* In the event of a crisis, social media companies should swiftly amplify communications by central banks, such as corrective statements that debunk fake information and calm the markets. Central banks and social media platforms should work together to determine what severity of crisis would necessitate amplified communication and develop escalation paths similar to those developed in the wake of past election interference, as seen in the United States and Europe.

- *Supporting Action 1.7.4:* Financial authorities and financial services firms should review their current threat monitoring systems to ensure that they include and actively try to identify and detect potential influence operations.

SPOTLIGHT

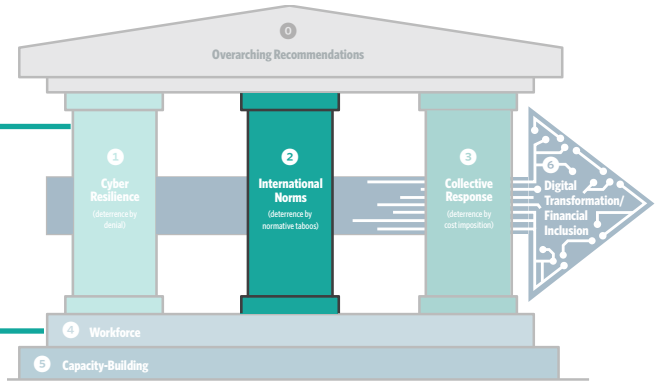
Cyber insurance is a potential complement to existing efforts aimed at addressing cybersecurity risk in the financial sector. The cyber insurance market is growing rapidly, with both established insurance companies and start-ups hoping to develop sustainable models to assess and price cyber risk. So far, the full potential of cyber insurance remains unrealized as limited data and a quickly evolving security environment complicate the emergence of a more mature marketplace.

The financial sector may have a unique vantage point from which to develop innovative approaches to cyber insurance and unlock its potential. The financial services industry plays a dual role in the cyber insurance market as both buyer and seller, while financial regulators are familiar with the governance of risk.

To learn more about cyber insurance, see Carnegie's publications "Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance," by Ariel E. Levite, Scott Kannry, and Wyatt Hoffman (2018), and "War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions," by Jon Bateman (2020).[200]

CHAPTER 2

PRIORITY #2: INTERNATIONAL NORMS



Core Pillar #2: *Reinforce international norms at the United Nations and through other relevant processes to clarify what is considered inappropriate behavior—that is, when malicious activity has crossed a line—and hold actors accountable for violations to avoid norms being eroded by impunity.*

Problem Statement: Weak International Norms in Need of Implementation

International norms make clear what behavior is considered appropriate and when a line has been crossed.[201] They provide the legitimacy for actions to hold those who violate such norms accountable. If every country unilaterally did what it wanted, the world would be even more of a Wild West. That is why the international community has clarified norms of shared interest around issues ranging from biological and chemical weapons, to human rights, international trade, and cyberspace. The past few years have also highlighted what happens when these norms erode and weaken over time.

Operationalizing and implementing the still nascent norms for cyberspace must be a top priority in the coming years. The financial sector provides an opportunity to advance this effort and to cement words and diplomatic consensus into action and state behavior.

The international community shares a strong common interest in financial stability. Great powers share an interest in preserving the integrity of the financial system. In the United States, "it's the economy, stupid" wins elections.[202] In China, the Communist Party has no interest in seeing a run on banks that could fuel further social unrest. The Russian elite wants to safeguard its money and has an interest in setting certain limits on cyber criminals

like the Carbanak group that become too aggressive.[203] And most of the world is tiring of attacks by North Korean hackers that continue to steal millions from countries all around the globe.[204] Amounts that may seem like peanuts for rich countries matter greatly to countries that need every penny for the effort to lift people out of poverty.

States can help protect the integrity of the financial system by committing to advance certain norms governing their behavior. Currently, the process for establishing international norms for cyberspace comes from two directions. The first is the top-down process driven by UN diplomats who have agreed on a catalogue of aspirational, voluntary norms that they hope will ultimately reflect how states actually behave. The second is the bottom-up process of emerging state practice that is beginning to shed light on areas of state restraint that could eventually be explicitly codified as norms.

Table 3: Key Economic Functions of the Financial System

Deposit taking and savings	Retail current accounts
	Small- and medium-sized enterprise (SME) current accounts
	Retail savings accounts/time accounts
	SME savings accounts
	Corporate deposits
Lending and loan servicing	Retail mortgages
	Retail lending (secured/unsecured)
	Retail credit cards
	SME lending (secured)
	Corporate lending
	Trade finance
	Infrastructure lending
	Credit card merchant services
Capital markets and investment	Derivatives
	Trading portfolio
	Asset management
	General insurance
	Life insurance, pensions, investment, and annuities
Wholesale funding markets	Securities financing
	Securities lending
Payments, clearing, custody, and settlement	Payment services
	Settlement services
	Cash services
	Custody services
	Third-party operational services

Source: European Systemic Risk Board, "Systemic Cyber Risk," February 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

The bad news is that neither of these two driving forces currently provides clarity on how international norms apply to the financial system specifically. The good news is that both offer useful starting points for clarifying and strengthening norms to protect the financial system. In addition, the work carried out by financial supervisory authorities on systemic risk can help operationalize and implement the diplomatic norms agenda. For example, the European Systemic Risk Board released a report in February 2020 identifying key economic functions of the financial system that, if disrupted, could pose a systemic risk.[205] Table 3 details these functions.

Industry also has an important role to play in strengthening international norms. The value to industry in pursuing cyber norms for the financial system is twofold. Most obviously, norms that increase the stability and security of cyberspace will reduce operational and systemic risk. In addition, public advocacy for norms allows financial institutions to enhance their brand and improve customer trust in their products. There are five main approaches that the financial industry can use to support the construction of cyber norms protecting the global financial system: (1) political signaling and agenda setting, (2) coalition building, (3) partnerships and financial support, (4) public commitments, and (5) monitoring compliance and collective response.

Mapping the Status Quo: A Shaky Foundation in Need of Reinforcement

Emerging State Practice

In addition to the diplomat-led, top-down processes, a growing number of experts with ties to the national security community are focusing on how states actually behave in cyberspace and what their use of offensive tools reveals about emerging norms.[206]

A comprehensive review of significant cyber incidents targeting financial institutions between 2011 and 2020 reveals that states have already demonstrated significant restraint in using cyber means against the integrity of the financial system. For example, it is noteworthy that there are no public data implicating states in any of the incidents involving the manipulation of the integrity of financial data; this suggests states have been exercising restraint so far. (The only exceptions over the past two decades have been North Korea's disk-wiping attacks against financial institutions in South Korea and Chile.)[207]

Upon reflection, such restraint makes sense. Global interdependence makes the financial sector more vulnerable than other critical infrastructure, but states share a common interest in refraining from putting financial stability at risk.[208] The damaging effects of an intrusion targeting the electrical grid or the oil and gas sector will mostly be limited to a single country's territory or its immediate neighbors. The effects of an incident targeting the integrity of financial data, however, are not necessarily bound by geography—they would be very difficult to understand and, therefore, hard to tailor and to predict.[209] An operation targeting a payment processing system could have the direct impact of corrupting the transactions running through it. Indirectly, however, it could lead to an institution's bankruptcy that sends shock waves throughout the international system. The 2008 collapse of Lehman Brothers highlighted the unanticipated contagion effect caused by the bankruptcy of even a single institution. The 1997 Asian financial crisis was similarly triggered by the collapse of the Thai currency and the unanticipated cascading effects that occurred throughout the region. Such second-order effects are difficult to anticipate, and they may not be factored into the attacker's battle damage assessments.[210]

Major powers, notwithstanding their fundamental differences, have recognized this in principle and in practice. The U.S. government reportedly refrained from using offensive cyber operations against Saddam Hussein's financial system.[211] Russia's 2011 "Draft Convention on International Information Security" explicitly suggests that "each State Party will take the measures necessary to ensure that the activity of international information systems for the management of the flow of . . . finance . . . continues without interference."[212] China also has a vested interest in the system, reflected, in part, by its successful effort to make the renminbi part of the IMF's global reserve currency basket.[213]

Recommendation 2.1: Heads of state should ensure that their state organs (continue to) exercise restraint when using offensive cyber capabilities to target financial institutions. This will strengthen the nascent state practice that has emerged over the past few decades.

Existing International Law

The international community has clarified through the UN that existing international law applies in cyberspace.[214] However, at present, there is so much uncertainty about how international law applies during both times of peace and war, at least in respect to data, that international law is simply not up to the task of safeguarding interdependent domestic, regional, and global financial systems. Because cyber attacks against the financial sector do not result in deaths or physical damage, it is difficult to analogize their effects, particularly of attacks against the integrity of financial data. The following discussion is based on an analysis that Michael Schmitt, one of the world's leading international lawyers on cyber operations, co-authored with Tim Maurer, one of the authors of this strategy document.[215]

International law has instituted a set of prohibitions that can be used to determine what sorts of operations are acceptable and unacceptable. During peacetime, the three prohibitions most likely to be implicated by cyber operations are those involving sovereignty, coercive intervention, and the use of force:

1. It is unclear whether cyber operations against data that do not cause damage to another state's cyber infrastructure qualify as violations of sovereignty. Efforts to manipulate the integrity of financial data are unlikely to result in physical damage or loss of functionality of cyber infrastructure (although they could cause a loss of confidence in financial institutions and be highly destabilizing); thus, they exist in a legal gray zone. Similarly, the line between financial activities that amount to inherently governmental acts and those that do not is indistinct. Financial data associated with a state's taxation system, for instance, would be clearly encompassed in the protection; however, data residing in the servers of state-owned banks might not be.

2. The second prohibition forbids a state's unlawful intervention in the internal or external affairs of another state. . . . The paradigmatic case of a prohibited cyber intervention is manipulation of election returns. In the context of financial data, an operation targeting the integrity of financial data upon which the state pension or welfare system relied in order to compel the target to adopt a particular domestic policy would exemplify prohibited cyber intervention.

3. The debate continues over whether non-physically destructive cyber operations can nevertheless qualify as prohibited uses of force. In particular, there is a strong argument to be made that the nature of the consequences (destructive or not) matters far less than their severity. From

this perspective, a cyber operation targeting financial data that results in severe financial instability and widespread economic disruption might amount to a prohibited use of force. But the approach is far from universally embraced, and the threshold above which a cyber operation would be considered sufficiently severe remains unsettled even among this perspective's proponents.

There are three factors that obscure how international law applies to cyber operations during wartime:

1. First, it is not clear that a cyber operation undermining the integrity of financial data, but not affecting the associated cyber infrastructure, would qualify as an attack and therefore be subject to the prohibition on attacking civilian objects.

2. There is also lack of agreement as to whether data constitute an "object," such that the prohibition on attacking civilian objects applies at all. . . . The interpretive distinction is critical, for if civilian financial and other data do not qualify as an object, they may be targeted, subject to some narrow exceptions, without violating international humanitarian law.

3. Finally, assuming solely for the sake of analysis that data *are* an "object" that is capable of being "attacked" as a matter of law, the question arises as to which data qualify as a "military objective" legally susceptible to attack. However, a long-standing debate surrounds so-called "war-sustaining" objects and how far the definition of a legitimate target can be stretched. The issue has direct relevance in the data context because cyber operations against an enemy's financial system could directly impede its ability to sustain the conflict.

Since this article was published in 2017, only three governments have publicly clarified aspects of how they interpret international law with respect to cyber operations involving financial institutions:

- In 2018, the UK attorney general stated in a speech that:

> The precise boundaries of [the international law prohibition on intervention in the internal affairs of other states] are the subject of ongoing debate between states, and not just in the context of cyberspace. But the practical application of the principle in this context would be the use by a hostile state of cyber operations to [sic] . . . intervention . . . in the stability of our financial system. Such acts must surely be

a breach of the prohibition on intervention in the domestic affairs of states.[216] (Emphasis added.)

- In 2019, the Australian government stated in a letter to the UN that:

  Harmful conduct in cyberspace that does not constitute a use of force may still constitute a breach of the duty not to intervene in the internal or external affairs of another state. . . . Accordingly, as former UK Attorney-General Jeremy Wright outlined in 2018, the use by a hostile State of cyber operations to [sic] . . . intervention . . . in the stability of States' financial systems would constitute a violation of the principle of non-intervention.[217] (Emphasis added.)

- In 2019, the Dutch minister of foreign affairs outlined in a letter on the international legal order in cyberspace to the House of Representatives of the Netherlands that

  International law does not provide a clear definition of "use of force." The government endorses the generally accepted position that each case must be examined individually to establish whether the "scale and effects" are such that an operation may be deemed a violation of the prohibition of use of force. . . . In the view of the government, at this time it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as the use of force.

  . . .

  Necessity is a ground justifying an act which, under certain strict conditions, offers justification for an act that would otherwise be deemed internationally wrongful, such as deploying offensive cyber capabilities against another state. . . . [T]he damage does not already have to have taken place, but must be imminent and objectively verifiable. . . . The damage caused or threatened does not necessarily have to be physical: situations in which virtually the entire internet is rendered inaccessible or where there are severe shocks to the financial markets could be classified as circumstances in which invoking necessity may be justified.[218] (Emphasis added.)

Recommendation 2.2: Individual governments should clarify how they interpret existing international law to apply to cyberspace, specifically with respect to malicious cyber activity involving financial institutions. Governments could do this through ministerial statements or speeches, letters to parliament/legislatures, submissions to the United Nations (UN) emulating existing examples, or other appropriate mechanisms. (Such clarification should follow and ideally go beyond the Australian, British, and Dutch examples and focus on the set of questions highlighted in the complementary report to this strategy.)

- *Supporting Action 2.2.1*: The North Atlantic Treaty Organization (NATO), the Shanghai Cooperation Organisation (SCO), and other relevant security organizations should clarify how they interpret existing international law to apply to cyberspace, specifically with respect to malicious cyber activity involving financial institutions; at a minimum, they should initiate processes for member states to discuss this question.

- *Supporting Action 2.2.2*: The International Committee of the Red Cross, through its mission to build respect for international legal obligations, should build on and clarify its existing publications to provide a recommendation to the international community for how existing international humanitarian law should apply to cyberspace specifically with respect to malicious cyber activity involving financial institutions.

Voluntary Norms

As international lawyers debate how existing international law and its provisions apply to cyberspace, diplomats have been busy developing a set of complementary, voluntary norms for peacetime. Outlined in a set of consensus reports agreed to by the UN GGE and endorsed by the UN General Assembly and the G20, these norms are aspirational in nature and outline how states will ideally behave in the future.

The most relevant norm with respect to the financial system is the following paragraph from the 2015 UN GGE report:

> A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that

> intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.[219]

This statement articulates a laudable goal, but effective operationalization faces several challenges. First, states have different definitions of what constitutes critical infrastructure. Second, the limitation to "intentional" damage does not take into account potential unintended effects like those witnessed in the WannaCry and NotPetya incidents. This was part of the reason several governments issued statements specifically condemning such attacks.[220]

To address this shortcoming, the discussion among UN member states in 2019 and 2020 led to a "pre-draft" report from the UN OEWG, which noted that:

> While States observed that critical infrastructure is defined differently in accordance with national prerogatives and priorities, they emphasized the severity of threats to particular categories of infrastructure, including for instance the health and financial sectors and electoral infrastructure. Transborder and transnational critical infrastructure was highlighted as at risk as was supranational critical information infrastructure, notably those global systems upon which public or financial services rely. In this regard, States underscored that attacks on critical infrastructure pose not only a threat to security, but also to economic development and people's livelihoods.[221] (Emphasis added.)

As part of this discussion, some states suggested "an 'upgrading' as well as further elaboration of norms," such as "highlight[ing] that supranational critical information infrastructure could be considered a special category of critical infrastructure, and that its protection was the shared responsibility of all States."[222] Singapore, one of the world's four largest global financial hubs,[223] specifically argued that.

> More cooperation is necessary to protect and deal with threats to supranational critical information infrastructure (CII), which are owned by private companies, operate across national borders, and are not under any particular State's jurisdiction. . . . Singapore also supports the further elaboration of norms where needed, for example, in respect of supranational CIIs which could be considered a special category of critical infrastructure, whose protection is the shared responsibility of all Member States.[224]

And the French government recommended that "More space could be dedicated to fields of vital importance such as healthcare, finance, transport, and electoral infrastructures."[225] (Emphasis added.)

In the United States, the congressionally mandated Cyberspace Solarium Commission issued a similar recommendation to "take a sector-by-sector approach to norms implementation: Prioritize norms against malicious cyber activity targeting elements of critical infrastructure that underpin shared global stability, such as the financial services sector, building on the existing norm against attacking critical infrastructure (CI)."[226] (Emphasis added.)

The U.S. government has already started taking action in line with this recommendation, issuing specific statements focusing on election infrastructure and the health sector (see Appendix C for more details). With respect to the financial sector, it is worth mentioning the bipartisan joint letter sent by the chairman of the U.S. House Committee on Foreign Affairs, then congressman Edward Royce, and the co-chair of the Congressional Cybersecurity Caucus, Congressman Jim Langevin, to Treasury Secretary Steven Mnuchin and State Secretary Mike Pompeo on November 5, 2018.[227] (See Appendix D for the text of the letters.) The representatives proposed that the two secretaries work with their counterparts in other countries to issue a statement at an upcoming G20 Finance Ministers and Central Bank Governors' meeting that would declare a commitment to protecting the financial system in the face of growing cyber threats. They recommended that such a statement condemn malicious cyber activity targeting financial institutions and call for partner governments and private sector institutions to facilitate better international cooperation on this issue. Two weeks later, on November 19, 2018, private industry speaking through the FSSCC also sent a letter to Mnuchin with the same request to pursue a statement through G20 and G7 channels.[228]

Why focus on the G20 for such a statement? The G20 is uniquely positioned to serve as the anchor for such a declaratory statement for several reasons:

- **Impact:** The G20 convenes the world's major economies, all of which have a shared interest in protecting the integrity of the global financial system, despite other existing political differences and tensions.
- **Mandate:** The G20 was established specifically in the wake of the global financial crisis to focus on financial stability and is primarily focused on economic issues and the financial system.

- **Type of agreement:** The G20 adopts not legally binding agreements but political ones. These are nonetheless effective because it is senior officials—either heads of state or top ministers—that agree to them. This important characteristic of the G20 has allowed its members to elegantly circumvent the contentious debate between Russia and China on the one hand, which have been promoting the idea of a legally binding information security treaty, and Western nations on the other, which have been focusing instead on existing international law and voluntary norms.
- **Process:** The G20's most established track is the G20 Finance Track, which precedes even the G20 heads of state convenings, thereby providing a well-established and well-oiled mechanism.

Recommendation 2.3: UN member states should strengthen and support the operationalization and implementation of the voluntary norms they agreed to through the UN, namely the norm focused on protecting critical infrastructure.

- *Supporting Action 2.3.1:* The G20 Finance Ministers and Central Bank Governors should adopt a communiqué, building on previous communiqués, urging restraint per recommendation 2.1, and adding specific declaratory language. The G20 heads of state should then endorse the language adopted by the G20 Finance Ministers and Central Bank Governors.

- *Supporting Action 2.3.2:* In a future process convened through the UN General Assembly and succeeding the UN Open-Ended Working Group (OEWG) and the UN Group of Governmental Experts (GGE), UN member states should:

    - Make explicit reference to the financial services sector as critical infrastructure for all UN member states for the purposes of norms (f) and (g) of the 2015 UN GGE report, which focus on critical infrastructure.

    - Highlight that financial institutions have been a primary target for malicious actors and face growing criminal and state-sponsored threats that require stronger cooperation among states to protect the global financial system.

- Call on states to adhere to the positive norms of cooperating in the investigation of transnational cyber crimes and denying the use of their territories for malicious activity.

- *Supporting Action 2.3.3:* Financial authorities and industry should use the systems developed for resilience purposes (for example, to identify and detect potential incidents in order to defend against and recover from them) for the detection and attribution of norm violations. Sharing such information is necessary to more effectively hold malicious actors accountable.

- *Supporting Action 2.3.4:* The UN Security Council should continue to monitor North Korea's activities, considering that North Korea's actions have impacted at least thirty-eight UN member states from 2015 to 2020 alone. The UN Security Council should use all its instruments, ranging from monitoring latest developments through regular reports (such as the 2019 "Report of the Panel of Experts Established Pursuant to Resolution 1874") to the imposition of sanctions, to deter future malicious activity.

- *Supporting Action 2.3.2*: UN member states in a future process convened through the UN General Assembly and succeeding the UN OEWG and UNGGE should

  - make explicit reference to the financial services sector as critical infrastructure for all UN member states for the purposes of norms (f) and (g) of the 2015 UNGGE report, focusing on critical infrastructure;

  - highlight that financial institutions have been a primary target for malicious actors and face growing criminal and state-sponsored threats that require stronger cooperation among states to protect the global financial system; and

  - call on states to adhere to the positive norm of cooperating in the investigation of transitional cyber crimes and to deny the use of their territories for malicious activity.

- *Supporting Action 2.3.3*: Financial authorities and industry should use the systems developed for resilience purposes, e.g. to identify and to detect potential incidents in order to defend against and to recover from them, also for the detection and attribution

of norm violations. Sharing such information is necessary to hold malicious actors accountable more effectively.

- *Supporting Action 2.3.4*: The UN Security Council should continue to monitor North Korea's activities considering that North Korea's actions have impacted at least 38 UN member states across continents from 2015–2020 alone. The UN Security Council should use all its instruments ranging from monitoring latest developments through regular reports, such as the 2019 Report of the Panel of Experts established pursuant to resolution 1874, to the potential imposition of sanctions to deter future malicious activity.

North Korea is one of the most threatening actors targeting financial institutions. Over the past decade, North Korea has used cyber attacks to steal some $2 billion, more than three times the amount of money it was able to generate through counterfeit activity over the four decades prior.[229]

A More Ambitious Proposal

States could also be more ambitious and consider establishing a specific regime designed to protect the integrity of the financial system as outlined below. Such a regime would have three connected and mutually reinforcing elements.[230]

- First, a state must not conduct or knowingly support any activity that intentionally manipulates the integrity of financial institutions' data and algorithms where they are stored or when they are in transit (for example, by sharing information about a vulnerability with other actors who then conduct the malicious action or by turning a blind eye to a nonstate actor's activity).

- Second, to the extent permitted by law, a state must respond promptly to appropriate requests from another state to mitigate activities manipulating the integrity of financial institutions' data and algorithms when such activities are passing through or emanating from its territory or perpetrated by its citizens. (This element is analogous to Core Pillar #3 on collective response in this strategy document.)

- Third, states would also be expected to implement existing due diligence standards and best practices. (This element is analogous to Core Pillar #1 on operational resilience.)

Linking these three elements would augment the overall effectiveness of this normative regime, as illustrated in Figure 8. The important characteristic of this proposal is that it combines a negative normative commitment (states commit *not to do* something) with a positive normative commitment (states commit *to do* something).[231] Linking the agreement governing state behavior with expectations that states will implement due diligence standards addresses the problem of moral hazard. And states' commitment to provide assistance and information when requested circumvents the attribution problem: rather than the victim of an attack having to prove its source, other states would have to live up to their commitment to respond to and help mitigate that attack, or explain why they do not. States would be expected to comply with these obligations in accordance with the requirements of national and international laws, both of which may require adjustment to reflect the principles described here.[232]

In order to achieve effective reciprocal adherence and be widely accepted among UN member states, this regime should not be limited to only a subset of financial institutions like the Global Systemically Important Banks (as enumerated by the FSB). From the standpoint of international stability—and of winning the support of a large number of states—it may be worth extending protections to all states' financial institutions. Cyber operations that threaten the integrity of any financial institution would create precedents and sow fears that could threaten all states and the financial system writ large.

If G20 member states or a group of states were to find the proposed agreement compelling, they could include the language proposed here (or otherwise improved) in a communiqué and implement and promulgate the agreement with the relevant standard-setting bodies and private sector institutions including CPMI, IOSCO, and the BCBS.[233]

Unlike the actions taken after the 2007–2008 financial crisis, adoption and implementation of an agreement like the one proposed here would require engagement with countries' national security communities and CERTs. No international forum to date exists that allows for such interactions. However, the FSB can act as the convener for such a process, possibly with the support and cooperation of other nongovernmental organizations.

Figure 8: Three Elements for an Effective, Self-Reinforcing Regime

There are clearly limits to the extent to which officials in the national security communities of each country can engage with foreign governments and experts in the financial sector. Given those limits, another approach would be an international agreement through the G20 complemented by a series of unilateral declarations by each government or its military to bolster the G20's statement and contribute to the agreement's effectiveness.[234] Unilateral declarations would also be a simple way for states that are not part of the G20 to state that they join the G20 member states in their commitment.

The existing regime against counterfeiting currencies is instructive here. For nearly a century, states have adhered to and helped enforce the 1929 International Convention for the Suppression of Counterfeiting Currency, because of widespread mutual vulnerability to the effects of counterfeiting. And because this restraint is widely accepted, states violating it are highly likely to face punishment. Nonstate actors, of course, persist in counterfeiting, as do North Korea and a few other states, but the practice is contained enough that it does not threaten the stability of the international financial system.

The Role of the Private Sector: Activating the Financial Industry as a Norm Entrepreneur

To date, the financial industry as a whole has not been very active in discussions of international cyber norms, apart from a few individual firms such as JPMorgan Chase, Bank of America, and Mastercard that have publicly supported international cyber norms.[235] Although multiple major financial institutions have considered becoming more actively involved (for example, when they were asked to join the Paris Call for Trust and Security in Cyberspace), there has not been the right window of opportunity for the sector to throw its full weight behind an initiative. Implementing a more coherent strategic approach such as the one outlined in this report may present such a window for industry to take some of the following actions.

- **Political Signaling and Agenda Setting:** Financial institutions can signal to their customers, the broader public, and their governments that there is a need for norms to constrain malicious cyber activity against the financial system. The impact of such signaling depends on the number of institutions sending a signal, and how loud and public those signals are. Options range from a series of letters sent to relevant government institutions, to public statements or op-eds published by a group of institutions, to public testimony before legislative bodies. Through political signaling, financial institutions can elevate the issue of cyber norms, particularly those to protect the financial system, on the agenda of political and industry leaders. For example, Microsoft's president, Brad Smith, has advocated for his idea of a Digital Geneva Convention at the Munich Security Conference, the WEF Annual Meeting in Davos, and many other high-profile events, and the company is actively engaged in intergovernmental fora.[236]

- **Coalition Building:** The financial industry has a global architecture in place to build and channel coalitions; trade associations at the national, regional, and global levels are potential vehicles for building consensus and advocating for norms. The work of consensus building and advocacy

includes building consensus within the financial industry and developing greater consensus and momentum among the stakeholders in the international community to focus on norms for the global financial system.

For example, at the global level, the financial industry could leverage global trade associations like the IIF and GFMA. Financial industry efforts could also be synchronized with current regional norms processes in organizations like the OAS, the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF), and the OSCE.

It is worth highlighting that in 2018, the OAS issued a detailed 181-page report, "State of Cybersecurity in the Banking Sector in Latin America and the Caribbean," demonstrating how a regional organization could be leveraged effectively and in partnership with industry.[237]

- **Partnerships and Financial Support:** The financial industry can join others' public commitments in support of international cyber norms such as Microsoft's Cybersecurity Tech Accord, Siemens' Charter of Trust, or the Paris Call. Financial support, particularly for resource-constrained nongovernmental organizations involved in advancing the public interest and strong cyber norms, provides another important opportunity for financial institutions to support ongoing norms processes. For example, Mastercard supports the CyberPeace Institute.[238]

- **Public Commitments:** The financial services industry could follow the logic of the Charter of Trust by making and implementing certain public commitments (although the lack of implementation has become a growing criticism of the Charter of Trust). A good illustration of such a corporate action is SWIFT's Customer Security Program. Following the 2016 Bangladesh incident, SWIFT updated its Customer Security Program to include cybersecurity standards for its clients in its contractual relationships. The program's terms and conditions remind clients that:

  > To conduct business over the SWIFT network, users need to have a commercial relationship with other SWIFT users. Users must establish such relationships taking into account multiple criteria. In addition to obvious commercial considerations, these criteria typically relate to KYC and sanctions/AML compliance, operational risk, cyber security, and fraud.

> Cyber-attacks are growing in number, their modus operandi are increasing in sophistication and attackers are focusing more deeply inside banks. Cybersecurity is therefore an important consideration in establishing commercial relationships between SWIFT users. . . . [As] part of the SWIFT Customer Security Programme, SWIFT is acting as a facilitator of standards and transparency regarding the cybersecurity compliance status of the users. Pursuant to the [SWIFT Customer Security Controls Policy], users must self-attest against the security controls set out in the CSCF. While SWIFT reserves the right to report failures to comply therewith, each user remains solely and exclusively responsible for any reliance thereupon and, more generally, any decision to exchange (or stop or suspend exchanging) messages or files with another user, and defining and implementing appropriate supporting controls and other arrangements.[239] (Emphasis added.)

These are now de facto mandatory requirements that SWIFT expects its clients to meet in order to retain access to the global network. This is one example of how private financial institutions can leverage their contractual relationships to strengthen cybersecurity and impose consequences on those who do not meet such requirements.

A related option is for financial services firms to use the power of the purse to nudge other industry actors into changing their behavior. In 2002, for example, Microsoft launched its Trustworthy Computing Initiative after Wall Street joined its growing chorus of critics.

On January 15, 2002, Bill Gates sent a now famous, one-paragraph memo to Microsoft employees, announcing that henceforth security would be Microsoft's number one priority:

> Over the last year it has become clear that ensuring .NET is a platform for Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing—or able—to take advantage of all the other great work we do. Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.[240]

After this memo, Microsoft launched its Trustworthy Computing Initiative and developed its security lifecycle model for Microsoft products.

Microsoft took this action because several of its largest customers, including major financial firms, told the company to improve the security of its software or risk losing some of their business.[241] At the time, financial industry was undergoing the transformative shift to internet banking services—such as the 2001 strategic alliance between Citigroup and Microsoft to offer internet banking services. Reliable infrastructure was essential.[242] Microsoft executives made specific overtures to the financial industry during the roll-out of the Trustworthy Computing Initiative.[243] In an *Economist* op-ed about Microsoft's focus on security, Craig Mundie, the champion of the Trustworthy Computing Initiative, noted that "in online banking, for example, the bank wants robust authentication." In other words, Wall Street used the power of the purse to nudge others to change.

- **Monitoring Compliance and Collective Response:** Industry owns and operates most of the financial system's infrastructure. Without industry, governments would have difficulty assessing when an international norm has been violated. Information sharing between industry and government is therefore required to monitor states' compliance with international norms. If states commit and generally adhere to strong international norms and mechanisms to hold actors accountable, industry will have an incentive to work with government when incidents occur.

  The financial industry is uniquely positioned to work with governments to hold norm violators accountable. States already use the financial sector to implement sanctions for a wide variety of reasons. Usually, financial services firms are reluctant instruments of statecraft. However, there is likely significantly greater appetite among financial services firms for implementing sanctions if these firms were themselves the target of malicious activity. One could also imagine a scenario where a firm could leverage its corporate relationships through contractual provisions, like those of SWIFT's Customer Security Program, to hold its clients accountable for actions enabling or contributing to norm violations.

Recommendation 2.4: Financial services firms and related trade associations, such as the Institute of International Finance (IIF), the Global Financial Markets Association (GFMA), the Bank Policy Institute (BPI), the Geneva Association, the American Bankers Association (ABA), the European Banking Federation (EBF), the Pan-European

Insurance Forum, the Association of Banks in Singapore (ABS), and others should call for stronger international norms to protect the financial system and should prioritize this as a talking point in their engagement with governments.

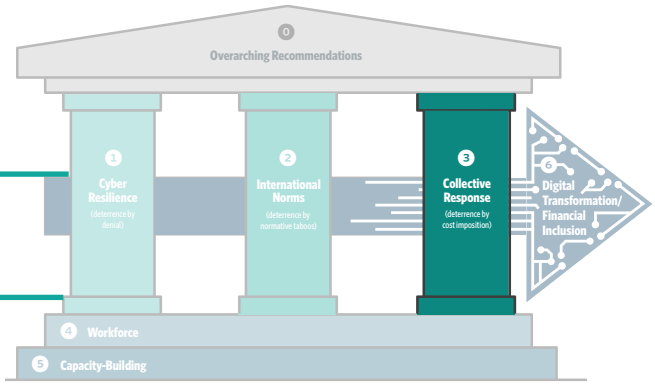
- *Supporting Action 2.4.1:* CEOs of financial services firms should collectively call on governments, for example via a joint letter, to strengthen international norms to protect the global financial system and for the G7 and the G20 to issue such a commitment.

- *Supporting Action 2.4.2:* Financial services firms should commit to sharing information about threat actors' behavior and potential norm violations to assist in the monitoring of compliance. Not sharing this information could embolden malicious actors to continue their activity with impunity.

- *Supporting Action 2.4.3:* If governments publicly commit to protecting the integrity of the financial system, financial services firms should provide financial support to advance the implementation and strengthening of international norms, for example, to expand capacity-building activities.

CHAPTER 3

PRIORITY #3: COLLECTIVE RESPONSE



Core Pillar #3: *Facilitate collective response to disrupt malicious actors and more effectively deter future attacks.*

Problem Statement: A Growing Desire for Justice

Malicious hackers have targeted financial institutions since the early days of the modern internet. In 1994, even before the dot-com boom, cyber criminals stole millions from Citibank.[244] According to the U.S. Federal Bureau of Investigation (FBI), this was a time when the FBI "teamed up with Russian authorities—who provided outstanding cooperation just days after a new FBI legal attaché office had been opened in Moscow—to gather evidence."[245] Over the past quarter century, cyber criminals have remained mostly at large, stealing millions and costing billions to defend against. Over the past decade, the risk has grown as politically motivated malicious actors now operate alongside profit-driven criminals, occasionally joining forces with them. Furthermore, malicious actors rely on the financial system to launder money, purchase offensive capabilities, and convert stolen data into cash.

The escalation of fraudulent activity during the coronavirus pandemic has highlighted the continued threat that malicious actors pose to individual consumers struggling to get by, to companies trying to avoid bankruptcies, even to government agencies doing their best to channel vital resources to those in need. The trend is clearly worrisome. First, attackers are increasingly building advanced capabilities to target core banking systems. Second, attackers are becoming more aggressive in disrupting victims' ability to respond and to recover, and they continue to find ways to collaborate through organized criminal activity that spans multiple geographies. Figure 9 provides a mapping of

the various threat actors targeting financial institutions and Figure 10 details the countries whose payment systems have been attacked from 2016 to 2018.

Figure 9: Mapping the Threat Actors

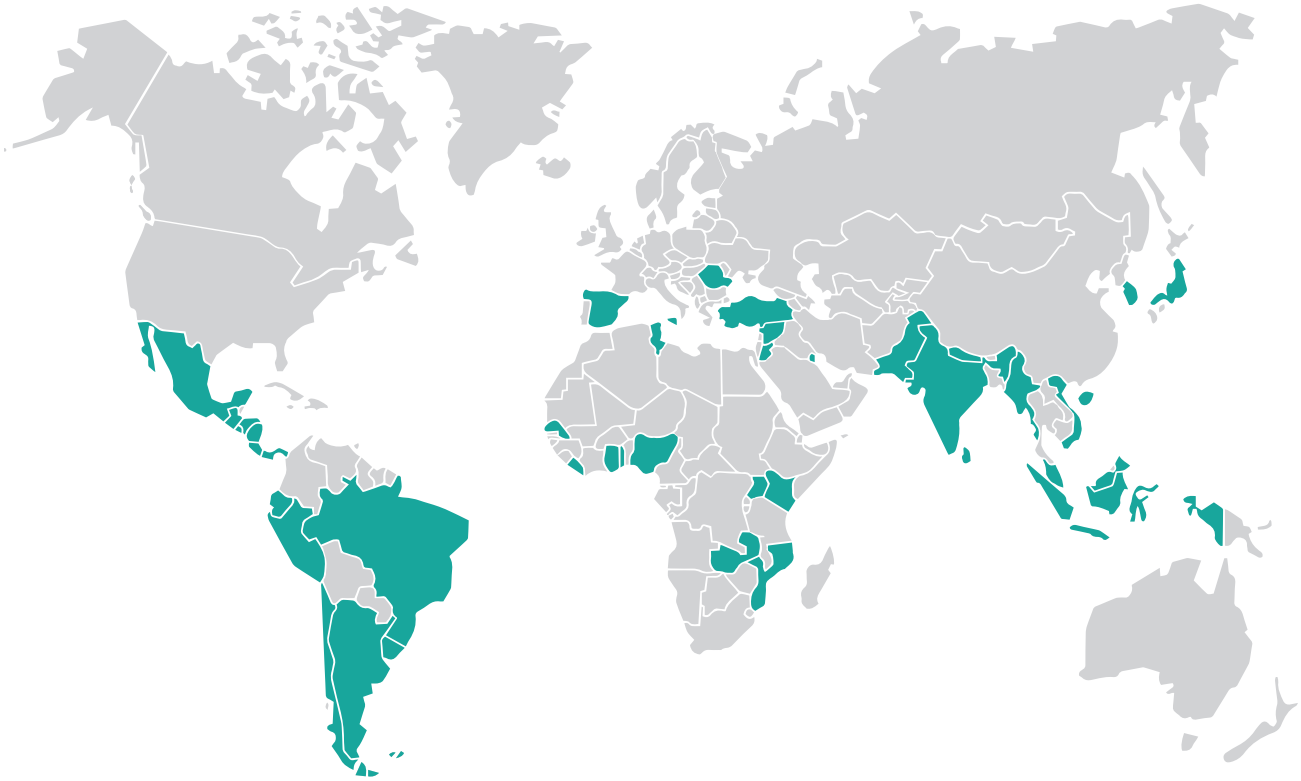
THREAT ACTOR			
 **Nation-states, state-sponsored groups**	**MOTIVATIONS** Geopolitical, ideological	**GOALS** Disruption, destruction, damage, theft, espionage, financial gain	**EXAMPLES** Permanent data corruption Targeted physical damage Power grid disruption Payment system disruption Fraudulent transfers Espionage
 **Cyber criminals**	**MOTIVATIONS** Enrichment	**GOALS** Theft/financial gain	**EXAMPLES** Cash theft Fraudulent transfers Credential theft
 **Terrorist groups, hacktivists insider threats**	**MOTIVATIONS** Ideological, discontent	**GOALS** Disruption	**EXAMPLES** Leaks, defamation Distributed denial-of-service (DDoS) attacks

Source: European Systemic Risk Board, "Systemic Cyber Risk," February 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk-101a09685e.en.pdf.

Cyber resilience is necessary to protect against such attacks, and international laws and norms outline when an actor crosses the line. When the line is crossed, calls for justice grow louder. As the threat escalates, some governments have grown impatient and demonstrated a willingness to take action not only to protect themselves but also to respond to attacks targeting financial institutions.

Governments and the financial industry have a shared interest in countering cyber threats, and this presents an opportunity for collective response and operational collaboration. Each has unique capabilities to bring to the table. Financial institutions maintain a critical vantage point from which to observe threats because it is their technical infrastructure that is often under attack. Governments have instruments of statecraft to deter and disrupt malicious cyber activity as well as the legal authority to act within their respective jurisdictions. However, no individual government or financial institution is equipped to counter cyber threats alone.

Figure 10: Payment Systems Under Attack, 2016–2018



Countries affected include: Argentina, Brazil, Bangladesh, Bosnia and Herzegovina, Bulgaria, Chile, Costa Rica, Ecuador, Ghana, India, Indonesia, Japan, Jordan, Kenya, Kuwait, Malaysia, Malta, Mexico, Mozambique, Nepal, Nicaragua, Nigeria, Pakistan, Panama, Peru, Philippines, Singapore, South Africa, South Korea, Spain, Taiwan, Tanzania, Togo, Turkey, Uganda, Uruguay, Vietnam, Zambia.

Source: U.S. Government Joint Advisory, "Alert (AA20-239A) FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks," August 26, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-239a; Adrian Nish and Saher Naumaan, "The Cyber Threat Landscape: Confronting Challenges to the Financial System" ("Cybersecurity and the Financial System" Working Paper Series, Carnegie Endowment for International Peace, March 2019) https://carnegieendowment.org/specialprojects/fincyber/workingpapers/.

The financial industry is uniquely capable of working with government to counter malicious cyber activity. As Matthew Noyes, Director of Cyber Policy at the U.S. Secret Service, has pointed out, financial institutions recognize "the shared interest of preserving the integrity of financial systems . . . and so when you have crimes that are related to the financial system you have a strong basis of evidence and cooperation globally to go after it."[246] Moreover, financial institutions have a high degree of cybersecurity maturity and have significant resources that can be mobilized to tackle this problem. Finally, international cooperation to combat financial cyber crime is more promising than cooperation around combating other types of cyber crime because there is a stronger international consensus around the definition of "financial crime" than around the definition of "cyber crime."

Taken together, the financial sector plays an important role from at least three angles as governments amplify their responses to malicious cyber activity:

- **As a target of malicious cyber behavior:** The threat landscape has evolved in recent years from criminal nonstate activity to an increasing number of states targeting financial institutions for political purposes (for example, Iranian DDoS attacks occurring from 2011 to 2013[247]), as well as for profit-driven motives (for example, North Korea since at least 2015[248]). One could also imagine financial systems coming under attack for strategic or operational purposes during times of conflict.

- **As an instrument of statecraft to impose costs:** Financial sanctions have become a routine instrument of statecraft. In imposing sanctions, governments are using the financial system to deter actors from engaging in certain types of behavior, ranging from money laundering and terrorist financing, to nuclear proliferation and (most recently) "significant malicious cyber-enabled activities."[249]

- **As a target in response to its use as an instrument of statecraft:** Because financial institutions are used by governments to implement financial sanctions, they may also become a target for those subject to these sanctions. This additional risk may grow as governments increase the number of sanctions and accelerate the use of the financial system as a tool of statecraft.

Mapping Key Trends: Cyber Crimes, Financial Crimes, and Cyber Deterrence

Trend #1: Bridging Finance, Law Enforcement, and National Security

States can improve the systemic resilience of their financial sectors and strengthen their ability to respond to malicious threats by facilitating operational collaboration among the financial services industry, financial authorities, national cybersecurity agencies, and other government authorities. Shifting from simple information sharing to collocated daily collaboration among relevant stakeholders can build the muscle memory necessary for an effective and timely response against malicious cyber threats. This section focuses on specific innovative financial sector models that have sprung up in recent years that could be expanded, replicated, and strengthened as part of this broader push.

Innovative Models

EU Law Enforcement Emergency Response Protocol: In March 2019, in response to WannaCry and NotPetya, the Council of Europe adopted the "EU Law Enforcement Emergency Response Protocol," which clarified roles, responsibilities, and communication procedures for EU law enforcement.[250] In the fall of 2019, ENISA and Europol's European Cybercrime Centre (EC3) organized CyLEEx19, a cyber law enforcement exercise, to test the protocol. The exercise brought together cyber crime investigators and experts from the public and private sectors and simulated a ransomware attack on the EU's financial sector.[251]

Cyber Information and Intelligence Sharing Initiative: In February 2020, the chair of the ECB's Euro Cyber Resilience Board, Fabio Panetta, announced the CIISI-EU, an information-sharing partnership connecting major financial infrastructures, Europol, and ENISA. According to Panetta, CIISI-EU will enable "the most important financial infrastructures to share vital technical information among themselves using an automated platform."[252]

Financial Systemic Analysis & Resilience Center: In the United States, a consortium of the most critical U.S. financial institutions established the FSARC in 2016 with the mission to "proactively identify, analyze, assess and coordinate activities to mitigate systemic risk to the U.S. financial system."[253] The center functions as a mechanism for banks to collaborate with the U.S. national security community, including the Departments of Defense, Homeland Security, and the Treasury, as well as the FBI. FSARC's offices are steps away from the Department of Homeland Security's National Cybersecurity and Communications Integration Center. In 2017, FSARC began providing the U.S. Cyber Command with cyberthreat data in an arrangement called "Project Indigo."[254]

Pathfinder program: This initiative is a partnership between the U.S. military, the U.S. Department of the Treasury, and the financial services sector.[255] It has enabled U.S. Cyber Command to more effectively carry out discovery operations aimed at protecting the financial sector. Lieutenant General Timothy Haugh, then commander of the Cyber National Mission Force, testified that U.S. Cyber Command does not "bring the expertise in what's critical within the financial sector," but by partnering with the Department of Homeland Security, the Treasury, and the financial sector, "as we look overseas . . . we're now focused on the things that are important to that sector."[256]

Financial Sector Cyber Collaboration Centre: UK Finance, a major financial trade association created in 2017, announced the creation of the FSCCC in

2018, modeled after the FSARC in the United States.[257] FSCCC is comprised of twenty large banks and other financial institutions working in collaboration with NCSC, UK FSAs, and the United Kingdom's National Crime Agency.[258] In 2019, the BoE reported that the FSCCC will be integrated into the United Kingdom's financial sector crisis response framework to ensure that the "technical coordination capability [the FSCCC] provides is incorporated into the broader response landscape."[259]

In addition to the models highlighted above, governments have also established national cybersecurity agencies that may function as the primary vehicle to advance systemic resilience and continuity planning.

For instance, the French government's national cybersecurity agency, ANSSI, established cooperation mechanisms with France's two primary financial authorities, ACPR and the Autorité des Marchés Financiers, in 2018.[260] In the United Kingdom, the NCSC and Government Communications Headquarters (GCHQ) worked closely together with the UK Treasury and industry.[261] Jeremy Fleming, head of the GCHQ, recounted an example of cooperation in a 2019 speech to a financial trade association: "Earlier this year we learned of a new and credible threat to the banking sector. We saw an Indian bank lose around £13m in two hours from a coordinated ATM cash scam. Within a very short period of time we pulled together more than fifty UK financial organisations, including many of you here today, to brief them on the threat and advise on specific protective measures."[262]

The most important element of cross-sector collaboration of this kind is to connect the national security agency teams focusing on the financial sector with other financial authorities, companies, partnerships and emerging initiatives. Such partnerships can enable nation-wide systemic resilience as well as an international collective response.

Recommendation 3.1: Governments and the financial industry should consider establishing entities to bolster their ability to assess systemic risk and threats as well as to coordinate mitigating actions. Existing examples of such entities include the United States' Financial Systemic Analysis and Resilience Center (FSARC) and the United Kingdom's Financial Sector Cyber Collaboration Centre (FSCCC).

Recommendation 3.2: Governments should ensure their intelligence collection priorities include a focus on threats that could pose a risk

to the financial system. In addition to nation-state and state-sponsored threat actors, sophisticated criminal actors could deliberately or (more likely) accidentally pose a risk, or they could provide the tools and services for others' disruptive and destructive attacks.

Recommendation 3.3: Governments should consider sharing intelligence about threats that pose a risk to the financial system with other allied, partnered, or like-minded countries.

- *Supporting Action 3.3.1:* To facilitate such information sharing, governments should consider finding ways—from downgrading classification of intelligence to broadening the pool of security clearance issuance (for example to relevant industry professionals)—to facilitate the sharing of threat intelligence.

Recommendation 3.4: Financial services firms should consider joining transnational networks like the Financial Services Information Sharing and Analysis Center (FS-ISAC) and/or emulating the region-based Cyber Defence Alliance (CDA) model to create a collective space for the financial industry to share information and prioritize responses to malicious cyber incidents.

Trend #2: The Growing Importance of Cyber Crime

For the first time in more than a decade, cyber crime is receiving renewed attention among policymakers. After years when cyber warfare and nation-state activities dominated the policy discussion, tackling cyber crime is slowly reemerging as a priority. The WEF is putting in place a new international Partnership Against Cybercrime bringing together government and industry actors.[263] In the United States, the nonpartisan think tank Third Way has popularized the term "cyber enforcement" and has ignited a push to move the fight against cyber crime higher on the agenda.[264] U.S. President Donald Trump's administration hopes to move the U.S. Secret Service and its cyber investigative capabilities away from the Department of Homeland Security and place them back under the Department of the Treasury.[265] And at the UN, Russia obtained enough votes to create a new process advancing a global cyber crime treaty.[266]

Recommendation 3.5: Governments should not only focus on state-sponsored actors but also make the fight against cyber crime a renewed priority, focusing less on time-consuming negotiations of a new cyber crime treaty and more on direct cooperation. This is especially important given the impact of the pandemic. For example, governments could support the WEF's Partnership Against Cybercrime and Third Way's Cyber Enforcement Initiative.

- *Supporting Action 3.5.1:* Governments should build a framework to strengthen and further institutionalize public-private cooperation to tackle cyber crime more effectively at the national, regional, and global levels. The World Economic Forum's Partnership Against Cybercrime is a promising initiative to further advance this on the international level, and Third Way's Cyber Enforcement Initiative is an innovative effort to develop new public policy approaches aimed at strengthening public-public and public-private cooperation to address this problem.

- *Supporting Action 3.5.2:* The financial industry should throw its weight behind efforts to tackle cyber crime more effectively, for example by increasing its participation in law enforcement efforts and better integrating its financial crimes, fraud, and cybersecurity systems in order to capture latest developments.

- *Supporting Action 3.5.3:* Governments should prioritize and develop law enforcement capabilities to address cyber crimes that violate international norms, namely those targeting financial institutions.

Recommendation 3.6: National and multilateral law enforcement agencies should help coordinate and provide negotiation expertise for financial institutions that have been infected with malware and are being held for ransom by threat actors.

> "Two decades ago, a group of enterprising criminals on multiple continents—led by a young computer programmer in St. Petersburg, Russia—hacked into the electronic systems of a major U.S. bank and secretly started stealing money. No mask, no note, no gun—this was bank robbery for the technological age. . . . We teamed up with Russian authorities—who provided outstanding cooperation just days after a new FBI legal attaché office had been opened in Moscow—to gather evidence."[267]
>
> —U.S. Federal Bureau of Investigation, account of a 1994 international cyber crime case.

A growing ecosystem of partnerships, task forces, and tools has emerged to help law enforcement, financial institutions, and other government bodies collectively respond to cyber crime. Many of these initiatives and tools are ripe for further internationalization. This section outlines models that have demonstrated success in combating cyber crime in the financial sector.

Joint Cybercrime Action Taskforce: Launched in 2014 and based at EC3 headquarters, the Joint Cybercrime Action Taskforce (J-CAT) is a standing operational team of cyber liaison officers from eighteen member countries. Having the team work from a single location makes international cooperation function more smoothly. J-CAT focuses on countering transnational cyber crime and has conducted highly effective operations against cyber crime in the financial sector.[268] One highly successful financial sector case was Operation Imperium, in which Bulgarian and Spanish authorities dismantled a highly sophisticated criminal network harvesting financial data from ATMs and point-of-sale terminals. Other examples include the November 2014 Global Airport Action.[269]

Cyber Defence Alliance: The CDA is another model worth highlighting. Established in 2015 by a small number of UK-based financial institutions, the nonprofit works collaboratively with financial industry and law enforcement agencies.[270] CDA members not only collaborate in the UK, where their core banking operations are based, but also extend their work to subsidiary regions, like Asian financial markets. In October 2018, CDA signed a memorandum of understanding with EC3 to formalize information sharing.[271]

Firm-to-firm collaboration enables CDA to act as a single voice when communicating with law enforcement. Firms can work through the organization to build intelligence reports and evidentiary packages that, cumulatively, have a higher chance of resulting in law enforcement action than they would if reported separately. CDA intentionally kept its membership small and local

to leverage the existing trust among member banks that already worked together outside of CDA. This trust allows member institutions to credibly share relevant incidents, threat intelligence, and actionable recommendations on a daily basis and even during an attack on one member.

According to Cheri McGuire, former CISO at Standard Chartered, alliances like CDA "allow [financial institutions] to share information for cybersecurity purposes among financial institutions and then . . . anonymize attribution to a particular institution that can then be shared with government or law enforcement."[272] Alliances that stay small and local may benefit from a preexisting degree of trust and share similar target profiles that make future operational collaboration relevant.

Financial Services Information Sharing and Analysis Center: Established in the late 1990s, FS-ISAC is designed to facilitate information sharing among financial sector entities. Although FS-ISAC has been around since 1999, it recently launched a multiyear strategy to internationalize and broaden its organizational footprint beyond the United States "because today's cybercriminal activities transcend country borders," according to former CEO Bill Nelson.[273]

Over the past two decades, FS-ISAC's membership has grown to nearly 7,000 members in over seventy jurisdictions.[274] It now operates three hubs: the Americas hub in the United States; the Europe, Middle East, and Africa (EMEA) hub in London; and the Asia-Pacific hub in Singapore. FS-ISAC cooperates with national law enforcement and cybersecurity agencies across all of its operational regions, including Singapore's CSA, the UK's NCSC, and Europe's EC3. Other international activities include regional conferences, the Summit of the Americas, the European Summit, and the Asia Pacific Summit; the annual CAPS tabletop exercise with 2,000 participants from around the world; and, hosting the CERES Forum for central banks and financial authorities from ten countries.[275]

Timeline of the FS-ISAC's Expansion

- 2016: FS-ISAC establishes the Asia Pacific Regional Analysis Centre with the MAS.[276]
- 2017: FS-ISAC establishes regional hubs in two of the world's financial centers, Singapore and London.[277]
- 2018: FS-ISAC creates the CERES Forum.[278]
- 2018: FS-ISAC signs a memorandum of understanding with Singapore's CSA.[279]
- 2019: FS-ISAC partners with EC3 to combat cyber crime within the European financial services sector.[280]
- 2020: FS-ISAC plans to host CAPS cybersecurity exercises in the Asia-Pacific region, the Americas, and EMEA.[281]

Trend #3: The Pursuit of Cyber Deterrence

Over the past five years, the U.S. government has tried to strengthen its deterrence posture with respect to malicious cyber activity. In 2018, U.S. Cyber Command announced its new command vision focused on "persistent engagement."[282] The White House's 2018 National Cyber Strategy outlined a new "Cyber Deterrence Initiative," and the U.S. Department of State has released its "Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats."[283] The recommendations outline "the nation's strategic options for deterring adversaries and better protecting the American people from cyber threats."[284] In particular, the recommendations state that

> the desired end states of U.S. deterrence efforts will be (i) a continued absence of cyber attacks that constitute a use of force against the United States, its partners, and allies; and (ii) a significant, long-lasting reduction in destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against U.S. interests that fall below the threshold of the use of force.[285]

To deter bad actors, the recommendations focus on imposing cost together with "likeminded partners":

> The United States should prepare a menu of options for swift, costly, and transparent consequences below the threshold of the use of force that it can impose, consistent with U.S. obligations and commitments, following an incident that merits a strong response that can have downstream deterrent effects. As the United States develops these options, it should assess and seek to minimize the potential risks and costs associated with each of them. . . . The United States will explore new uses of current tools and authorities, identify ways in which existing authorities may need to be amended, and, when necessary, develop legislative proposals for new authorities.[286] (Emphasis added.)

In September 2019, the United States, together with twenty-six like-minded nations, issued a statement coinciding with the annual meeting of the UN General Assembly. The statement's key message was a warning from the signatories: "When necessary, we will work together on a voluntary basis to hold states accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law. There must be consequences for bad behavior in cyberspace."[287] In addition to the United States, the following countries signed on to the statement: Australia, Belgium, Canada, Colombia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, the Netherlands, New Zealand, Norway, Poland, the Republic of Korea, Romania, Slovakia, Spain, Sweden, the United Kingdom.

The Rise of Cyber Sanctions

Sanctions have been a long-standing tool that governments have used to influence other countries' behavior. Governments increasingly rely on "smart" sanctions, which focus on individuals or companies instead of a country's entire economy.[288] The overall trend toward smart sanctions focuses heavily on the more effective use of financial sanctions.[289]

In April 2015, the U.S. government expanded its existing sanctions authorities by adopting U.S. Executive Order 13694 ("Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"). This order paved the way for sanctions to be imposed specifically in response to cyber attacks. For such sanctions to be applied, the order stated, malicious activity must be

> reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign

> policy, or economic health or financial stability of the United States and that have the purpose or effect of:
>
> (A) harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;
>
> (B) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;
>
> (C) causing a significant disruption to the availability of a computer or network of computers; or
>
> (D) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.[290]

These criteria outline a fairly high threshold to be met in terms of significance and malicious intent. At the same time, such sanctions can be imposed against individuals and other entities that are not only directly responsible but may be complicit or have otherwise benefited from the malicious activity.

Past examples of sanctions in response to activity targeting the financial system include:

- sanctions imposed in 2017 against entities and individuals linked to Iran's Islamic Revolutionary Guard Corps responsible for DDoS attacks targeting the U.S. financial system between 2011 and 2013;[291]
- sanctions imposed in 2018 and 2019 against entities and individuals linked to North Korean attacks on financial institutions for the purpose of generating revenue for the country's weapons of mass destruction program;[292] and
- sanctions imposed in 2019 against twenty-one members of Evil Corp, a Russia-based cyber criminal organization responsible for the Dridex malware that targeted financial institutions and generated more than $100 million in stolen funds.[293]

Notably, the 2019 sanctions levied against members of Evil Corp included not only those who facilitated the attacks but also individuals who recruited

and maintained "mule networks" and facilitated money laundering in the United Kingdom and elsewhere. The leader of Evil Corp, Maksim Yakubets, was linked to Russia's security service but many of the other individuals sanctioned were not linked to state entities, potentially suggesting a lower threshold for using sanctions to counter transnational cyber crime.

The EU has also developed a framework to impose sanctions on malicious actors. In 2017, the Council of the European Union adopted the Cyber Diplomacy Toolbox, a framework for responding to malicious cyber activities. Most significantly for the financial sector, this tool box includes the possibility of targeted sanctions against governments, organizations, and individuals.[294] On July 30, 2020, the EU and the United Kingdom exercised this new authority to impose sanctions over malicious cyber activities on a range of Russian, Chinese, and North Korean nationals and entities. In particular, sanctions were imposed on Chosun Expo, an alleged front company for North Korea's Lazarus Group, for facilitating not only the WannaCry attacks but also for "cyber-attacks against the Polish Financial Supervision Authority . . . as well as cyber-theft from the Bangladesh Bank and attempted cyber-theft from the Vietnam Tien Phong Bank."[295]

SPOTLIGHT

Since 2012, the U.S. government has used sanctions—a political tool to freeze the assets and block the transactions of individuals and entities—at least twenty times to punish malicious cyber actors in Iran, North Korea, Russia, China, and Nigeria. In 2019, the European Union finalized its own cyber sanctions framework,[296] and in July 2020, the bloc designated targets for the first time.[297] Actors that have engaged in attacks affecting the integrity of the financial system have been targets of both U.S. and European sanctions.[298]

Though scholars have long debated the utility of targeted financial sanctions at coercing strategic policy change,[299] policymakers continue to use the tool in response to a variety of transnational threats.[300] With respect to malicious cyber activity, proponents of sanctions argue that they can, among other benefits, help publicize attributions of wrongful behavior, satisfy audiences by "doing something" in response to an attack, deny actors the financial rewards of cyber crime, disrupt the financing of cyber operations, provide opportunities for international cooperation, and reinforce norms of responsible behavior.[301]

The U.S. government, in particular, has used sanctions hoping that, cumulatively, the repeated imposition of sanctions in response to malicious cyber attacks can deter future attacks by "increasing effort, raising risk, and reducing rewards" associated with offensive cyber behavior.[302] At the same time, the high threshold for the use of sanctions by the U.S. and the EU reflects concerns that using sanctions excessively may encourage the development of alternative financial architectures that enable sanctions evasion.[303]

The full contours of the European Union's cyber sanctions framework will become more apparent as the bloc expands its use of the new framework, meaning that the impact and value of sanctions as a tool against malicious cyber activity remain uncertain at this point.

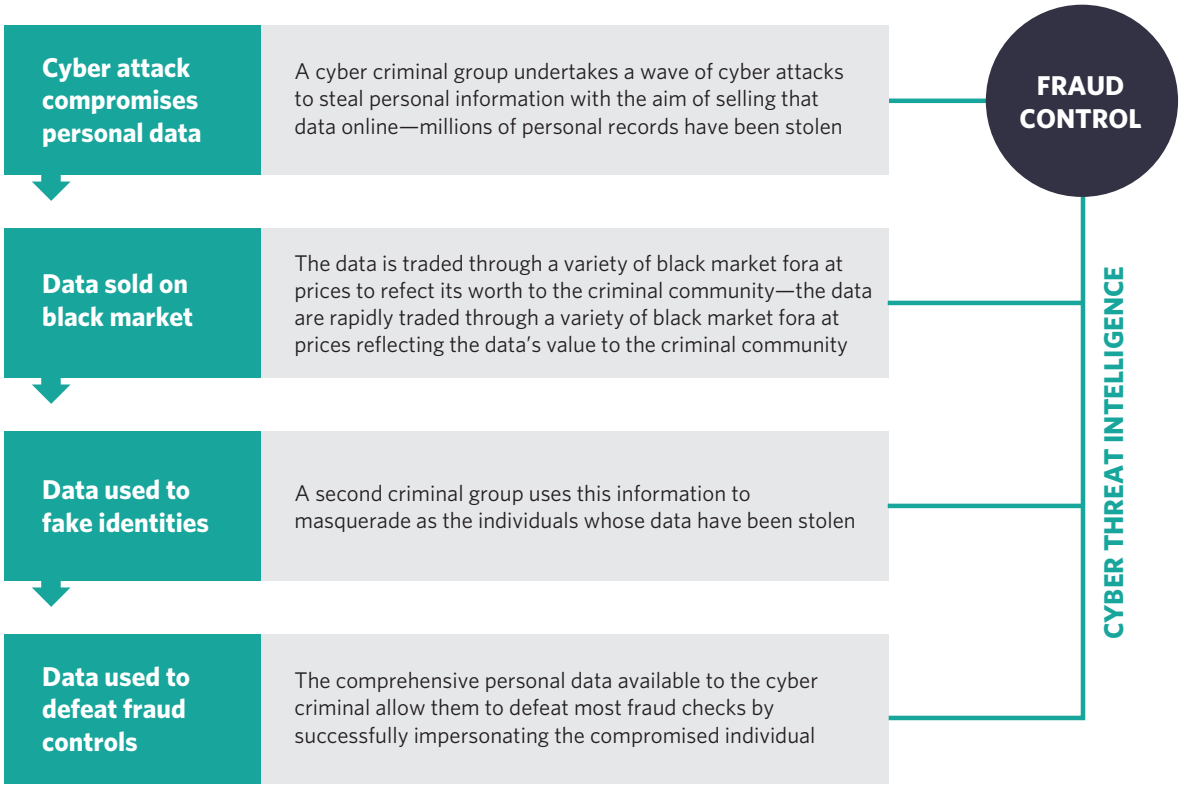
To learn more, see the article "Countering Malicious Cyber Activity: Targeted Financial Sanctions," by Natalie Thompson (forthcoming).

Trend #4: Convergence of Cyber Crimes and Financial Crimes

The financial sector is undergoing a rapid digital transformation. Banks are moving their operations and services online, implementing new financial technologies, and more frequently handling instantaneous transactions and faster risk decisions. One consequence of this changing landscape is that criminals are exploiting DFS to commit fraud and financial crime. Distinctions between cyber crime, fraud, and financial crime are disappearing as criminal activity operates at the intersection of all three. Figure 11 provides an example of such convergence.

The convergence of financial crime, fraud, and cyber crime is new enough that many law enforcement agencies and financial institutions still treat them as separate risks. Teams that were originally designed to counter paper-based fraud and financial crime are siloed from teams countering cyber threats, thereby undermining an organization's situational awareness regarding criminals that use malicious cyber activity to commit fraud or financial crime.

Figure 11: An Example of the Convergence Between Cyber Attacks and Fraud



Source: UK Finance, "Staying Ahead of Cyber Crime," April 2018, https://www.ukfinance.org.uk/system/files/Staying-ahead-of-cyber-crime.pdf.

Recent massive fraud of coronavirus-related unemployment insurance payments and other government payments has underscored the need to address the convergence of cyber and fraud. In May 2020, the U.S. Secret Service warned of a transnational criminal scheme that used stolen personally identifiable information to submit fraudulent claims.[304]

Sophisticated malicious actors can move very quickly from illicitly accessing a system to initiating fraudulent payments and cashing out. A bank's cybersecurity team may be able to detect network intrusions, while the bank's antifraud team may manage transaction controls. However, these teams are often isolated from one another, and the delay in coordinating across silos may give criminals enough time to get in and cash out. The Carbanak attacks, which used malware to target financial institutions and led to the theft of $1 billion, are a good illustration of how criminal groups exploit such gaps.

Fusing Cyber Threat Intelligence and Financial Intelligence

The convergence of financial crime, fraud, and cyber crime also presents new opportunities to disrupt malicious activity by fusing financial intelligence and cyber threat intelligence. Finding ways to leverage these capabilities could also help governments detect and respond to malicious activity targeting the financial sector.[305]

The U.S. Secret Service, one of the largest law enforcement agencies focused on fighting financial cyber crime, reorganized itself in July 2020 to address this convergence. The U.S. Secret Service combined its Electronic Crimes and Financial Crimes task forces into a merged network known as the Cyber Fraud Task Force. "In today's environment, no longer can investigators effectively pursue a financial or cybercrime investigation without understanding both the financial and internet sectors, as well as the technologies and institutions that power each industry," the U.S. Secret Service explained.[306] The U.S. Secret Service also announced plans to expand its Cyber Fraud Task Force network from forty-two offices in the United States and two offices abroad to 160 offices worldwide.[307]

The financial sector is also recognizing the need to fuse these functions. UK Finance has argued that "only by breaking down the barriers between the cyber security, fraud and financial crime disciplines can we really hope to counter cybercrime."[308] Standard Chartered has already joined its fraud, anti-money laundering (AML), and cyber crime teams into a single center which "reduced operating costs by approximately $100 million."[309]

Leveraging Financial Intelligence Units to Address Cyber Threats

In 2019, the U.S. Department of the Treasury restructured the Financial Crimes Enforcement Network (FinCEN) and established the new Cyber and Emergent Issues Section under the Strategic Operations Division.[310] Aligning these intelligence sources will become even more important as financial intelligence units (FIUs) focused on AML and counter terrorist financing improve their capabilities to track and isolate digital currencies, a common money-laundering instrument used by cyber criminals:

- **Australia:** Australia's National Cybersecurity Strategy (2020) pledges that the Australian Transaction Reports and Analysis Centre's "financial intelligence expertise will be harnessed to target the profits of cybercriminals."

- **Canada:** In 2019, FINTRAC, Canada's FIU, expanded its cooperation with the Royal Canadian Mounted Police to counter cyber-enabled fraud.[311]

- **Indonesia:** In 2018, the Indonesian Financial Transaction Reports and Analysis Center leveraged its new cyber crime unit to assist in a card-skimming fraud that used cryptocurrencies.[312]

- **France:** In 2018, France's FIU, Tracfin, established a new investigative division for financial cyber crime to "increase its expertise and expand its investigative capabilities, particularly for analysis of crypto-asset transactions."[313]

- **South Africa:** In 2018, South Africa's FIU, the Financial Intelligence Centre, launched an initiative focused on countering cyber crime and cyber-enabled fraud.[314]

Recent actions taken by the U.S. government against FIN7, a crime ring known for cyber attacks against financial institutions, demonstrate how financial intelligence strengthens law enforcement response to cyber criminals. In addition to U.S.-led indictments and arrests, the U.S. Department of the Treasury sanctioned seventeen members of FIN7 and released "previously unreported indicators of compromise," based on intelligence from FinCEN.[315]

FIUs collect the bulk of their intelligence through suspicious activity reports (SARs) or suspicious transaction reports (STRs), which are submitted by banks when they identify a transaction that raises a red flag. To improve the FIU intelligence collection process, some governments, like those of Japan,[316]

the United States, and the United Kingdom,[317] have started to require that banks include cyber indicators in their SARs/STRs in a standardized format.

Importantly, the convergence of financial crime and cyber crime may be an opportunity for countries to overcome barriers to international cooperation. There is no international consensus on the definition of a "cyber crime"; some governments, like Russia and China, advocate for a broader definition that includes information-related harms, which is challenging to reconcile with Western values of free speech. However, there is a much stronger international consensus around definitions of financial crime, developed in part through the FATF's work on terrorist financing and in part by countries' mutually shared interest in maintaining the integrity of the global financial system. Governments may be more willing to cooperate to combat cyber crime targeting financial institutions if cooperation is framed through the lens of financial crime rather than cyber crime.

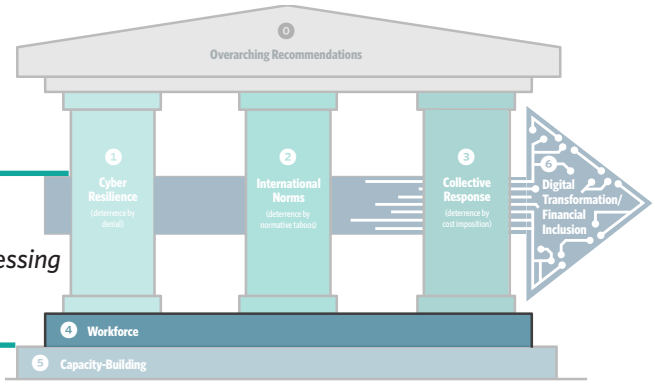
FIUs and other financial crime authorities already have an established rhythm of global cooperation. For example, in December 2019, law enforcement authorities from thirty-one countries, 650 banks, and seventeen bank associations cooperated for the fifth European Money Mule Action (EMMA 5), which resulted in 228 arrests, and disruption of over 3,800 money mules.[318] The European Union has already begun integrating its treatment of cyber crimes and financial crimes by making cyber crime a predicate offense to money laundering through the 2018 Directive on Countering Money Laundering by Criminal Law.[319]

Malicious actors have so far taken advantage of gaps among cybersecurity, AML, and fraud prevention teams across financial institutions and law enforcement. Fusing these functions may not only harden the defenses of the financial system but could also improve authorities' capacity to respond to malicious activity by tracing adversaries' financial activity, denying their access to funds, and disrupting their financial infrastructure and mule networks.

Recommendation 3.7: The FATF should explore how the existing regime to detect and counter money-laundering as well as terrorist and proliferation financing could be leveraged to fight cyber attacks more effectively.

CHAPTER 4

PRIORITY #4: CYBERSECURITY WORKFORCE CHALLENGES



Crosscutting Issue #1: *Build the cybersecurity workforce required to turn ambitions into actions by assessing and expanding effective models for addressing workforce challenges including limited pipelines and a lack of diversity.*

Cybersecurity Workforce in the Private Sector

Problem Statement: The Cybersecurity Talent Shortage

Although exact numbers vary, experts agree that a significant gap exists between supply and demand in the cybersecurity workforce across sectors. A 2019 projection by the International Information System Security Certification Consortium stated that the cybersecurity workforce needs to grow by 145 percent to meet global demand and that the current shortfall amounts to approximately 4 million individuals.[320] "Both banks and financial market infrastructures [in Europe] are struggling to find staff with the skills and experience needed to fend off cyber-attacks,"[321] a member of the ECB's Executive Board noted in 2019.

The financial sector has always been one of the largest employers of cybersecurity talent. One reason for the high demand is that cyber criminals have been targeting financial institutions since the early days of the internet. Yet the financial sector's demand for cybersecurity talent has been growing in recent years. One reason is higher expectations from financial regulators, especially following the 2016 Bangladesh incident. A year later, in 2017, eighteen of the FSB's twenty-five member jurisdictions reported plans to release new rules addressing cybersecurity in the financial sector.[322] This rapid worldwide

increase in cybersecurity regulatory activity is illustrated by a recent survey among financial CISOs who said that close to 40 percent of their time was spent "reconciling cybersecurity and regulatory frameworks."[323] Other factors include the general evolution of the cyber threat landscape and growing awareness among senior executives of cybersecurity's importance.[324]

Other sectors—including governments and central banks—have difficulty competing with the financial industry for cybersecurity talent. Industry offers the highest salaries for cybersecurity professionals globally.[325] An unintended consequence of updating financial regulations focused on cybersecurity is that it will drive well-resourced financial institutions to siphon even more cybersecurity professionals from the already limited pool, exacerbating the workforce challenge for nonfinancial critical infrastructure sectors. (It will also draw talent away from central banks and government agencies. Carnegie plans to tackle the workforce challenge faced by these organizations through a separate project.)

Mapping the Status Quo: Existing Efforts to Address the Workforce Shortage

Existing cybersecurity workforce initiatives range from internal upskilling and retraining programs to cybersecurity competitions, partnerships with post-secondary education institutions, and apprenticeships, among others.[326] They can be grouped into five approaches to tackle the current challenges:

1. **Expand the pipeline bringing in new talent**

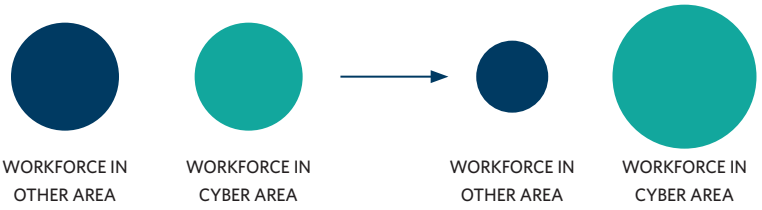
   This means encouraging greater numbers of talented people to enter the cybersecurity workforce, for example, by encouraging more high school students to pursue computer science degrees.

2. **Better identify existing talent and match it with those seeking it**

   This means maximizing the use of the existing workforce, including through diversity initiatives to identify and attract talent that is otherwise neglected.

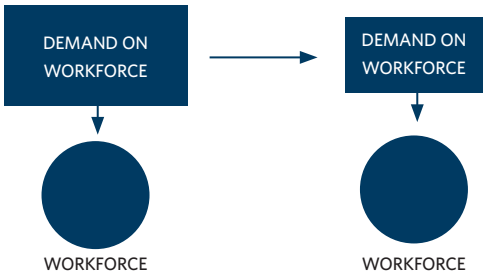
3. **Re-train staff currently in other areas to become part of the cyber workforce**

   This includes initiatives undertaken as part of "Future of Work" planning efforts.



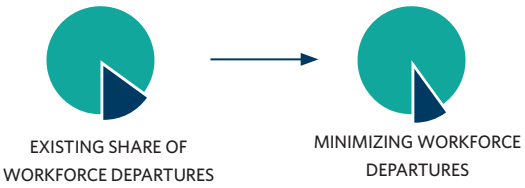
4. **Reduce demand through technological innovation**

   Innovations could include replacing technology to reduce the attack surface, thereby limiting the work required to protect it; or using pooled services with respect to threat intelligence or other needs.



5. **Improve retention of the current workforce**

   This includes offering competitive salaries, opportunities for promotion, and a more inclusive culture.



Workforce retention is a particular challenge for organizations in developing and emerging countries, where staff may not only switch from government to industry and vice versa but may leave the country altogether as part of a cybersecurity brain drain.[327]

"We have a specific problem in emerging economies. I've met a number of excellent cybersecurity people in banks in East Africa—but once their profile rises, they're poached by banks/fintechs in Europe/North America. This brain drain leaves Africa exposed. Creating a much broader pool is clearly the answer, but that's going to take a long time."[328]
—Paul Makin, cybersecurity expert focusing on financial inclusion

Financial institutions themselves have been advancing a series of initiatives. Some key examples include:

- **Apprenticeships:** Examples include Zurich Insurance Group's Cyber Security Apprenticeship program, which has built on the company's broader apprenticeship experience.[329] The Cybersecurity Workforce Alliance (CWA), founded by SIFMA and CISOs of major financial institutions, partners with educational institutions to provide students with courses, mentors, and apprenticeships in cybersecurity.[330]

- **Educational Partnerships:** JPMorgan Chase has provided funding to support the Florida Center for Cybersecurity, based at the University of South Florida;[331] and the Capital One Foundation has provided grants to community colleges seeking to develop cybersecurity career programs.[332]

- **Public-Private Partnerships:** Mastercard helped launch the Cybersecurity Talent Initiative, which provides college graduates with $75,000 in student loan assistance, a two-year placement at a federal agency and, upon completion of the placement, a full-time position with Mastercard or another private partner.[333]

- **Nonprofit Partnerships:** U.S. Bank has invested in youth-focused cybersecurity programs, working with nonprofits like Technovation, Girls Who Code, and the Girl Scouts of Western Ohio to attract girls and women into cybersecurity careers.[334]

- **Reskilling Programs:** JPMorgan Chase is piloting a program called Skills Passport within the bank's IT department to assess which employees could be retrained for cybersecurity roles.[335]

- **Cybersecurity Competitions:** Barclays hosted a cybersecurity competition in 2018 to attract talent.[336]

- **Grants:** In 2018, the MAS unveiled a Cybersecurity Capability Grant to assist the local financial sector's cyber resilience, including through workforce development.[337]

Recommendations: Assessing Effectiveness and Expanding Effective Models

Existing initiatives like the ones listed above are important and much needed to address the workforce shortage. Nonetheless, many questions remain. Which of the existing initiatives are most effective? Which can be scaled most easily? Which have the greatest return on investment? A comparative analysis that could answer such questions does not yet exist. In addition, more granular insights are needed. For example, it is unclear how the financial sector's demand for talent is distributed across entry-level, mid-level, and senior-level positions. Filling entry-level positions is a different challenge compared to filling mid- and senior-level positions.

Financial institutions have their own firm-specific interests in finding answers to these questions. Moreover, large financial institutions are in the unique position of using multiple models to overcome the workforce challenge, therefore enabling comparisons among them. Preliminary research suggests that financial institutions believe workforce development to be a sector-wide, rather than a firm-specific problem and are willing to consider sharing data as a cooperative win-win, as opposed to a competitive win-lose prospect. In addition, investing in the future of the cybersecurity workforce aligns with existing corporate responsibility initiatives and could address broader public policy problems. Meanwhile, financial regulators have incentives to minimize unintended regulatory consequences and to support the private sector in achieving a more robust and diverse workforce.

Recommendation 4.1: Financial services firms should prioritize their efforts to address cybersecurity workforce challenges, ranging from the limited talent pipeline to the lack of diversity in the workforce. The high rate of unemployment in the wake of the coronavirus pandemic represents an important opportunity to retrain and hire talent.

- *Supporting Action 4.1.1:* Large financial services firms should form a dedicated working group to collect, compare, and assess data about their own current workforce and related initiatives with the goal of assessing those initiatives' effectiveness and scalability

and addressing the broader cybersecurity workforce challenges faced by individual firms, the sector, and countries.

- *Supporting Action 4.1.2:* Following an assessment of the effectiveness and scalability of existing models, the dedicated working group should share best practices and lessons learned and issue recommendations for how the financial services sector can better address cybersecurity workforce challenges.

- *Supporting Action 4.1.3:* Financial authorities, central banks, and ministries of finance should explore how they could help expand effective cybersecurity workforce initiatives. This would help alleviate the unintended consequence of financial services firms hiring more talent to comply with recently increased regulatory expectations, which exacerbates the workforce shortage for other sectors that cannot compete with financial sector salaries.

Recommendation 4.2: Financial services firms should provide financial and other resources to help augment effective cybersecurity workforce initiatives, especially those focusing on building and widening the cybersecurity professional pipeline, including high school, apprenticeship, and university programs.

From Recommendation to Implementation

In May 2020, after receiving positive feedback about the idea, Carnegie invited financial institutions to sign up for a dedicated working group like the one described in Supporting Action 4.1.1—thus opening the door to move from recommendation to implementation. The financial institutions that signed up for this working group are: Bank of America, Capital One, HSBC, Intesa Sanpaolo, JPMorgan Chase, Morgan Stanley, Options Clearing Corporation, Standard Chartered, UBS Group AG, Visa, and Zurich Insurance Group.

More details about the findings of this working group will be made available at the end of 2020.

Cybersecurity Workforce in the Public Sector

Problem Statement: The Challenges of Public Sector Workforce Development

Cybersecurity has become a top concern for central banks, ministries of finance, and other financial supervisory authorities.[338] At the same time, these public institutions face a unique mix of challenges related to hiring and retaining staff with expertise and experience in this area. The biggest workforce development challenge for public institutions is that they cannot typically compete for talent with the private sector based on salary alone. In addition, financial sector authorities compete not only with the private sector but also with authorities in other jurisdictions. That is why public institutions must often find other ways than salary to make their workplace appealing to potential and current employees.

When considering other incentives, it is worth noting that public institutions operate in a unique environment, which can drive similarly unique career development opportunities:

- Public institutions rarely focus on only one area of cybersecurity, as they must field a defense across a range of specialties. This breadth of focus presents opportunities for employees to move through the organization, learning as they go.

- Public sector institutions often have unique authority and access to information, providing unique work opportunities that other employers cannot replicate.

- Like most workers, cybersecurity employees are motivated to work in jobs where the mission matters; public sector employers can emphasize the value of public service in workforce development efforts.

In addition, the assertion that public sector employers can never compete when it comes to salary is an oversimplification. For example, in the United States, federal government jobs requiring only a high school education or a bachelor's degree tend to pay more than comparable jobs in the private sector; however, employees in the public sector with advanced degrees made about 24 percent less than their industry counterparts.[339] The salary gap is greater in a highly competitive hiring market like cybersecurity, and government employers certainly do struggle to compete with private sector salaries, but the gap is not insurmountable.[340]

Other factors like learning opportunities, work environments where employers take security seriously, and personally rewarding mission sets can counterbalance the gap in pay.[341] One of the primary reasons cybersecurity employees leave their jobs is because they lack promotion and development opportunities.[342] Conversely, an employer's willingness to offer educational opportunities is one of the major drivers of recruitment and retention.[343]

Mapping the Status Quo: Existing Models in Public Institutions

Public institutions can take advantage of their unique characteristics through a range of workforce development tools including: (1) career path planning, (2) rotational programs, (3) upskilling, (4) work-based learning, (5) hiring requirement exemptions, and (6) public-private partnerships.

1. **Career Path Planning:** Because employees in cybersecurity roles value jobs that allow them to grow and develop, employers that cannot offer lavish salaries can still compete for talent by offering career paths that demonstrate growth and learning potential. Clearly defining a path of possible promotions and creating clear and specific criteria for promotion help to mitigate unconscious bias in promotions.[344] This clarity demonstrates that a workplace provides room to grow and that the employer has implemented thoughtful policies regarding fair treatment of employees.

   For example, the U.S. Interagency Federal Cyber Career Pathways Working Group builds on existing efforts to provide an adaptable template for employees' progression and mobility through the workforce among the twenty-four participating departments and agencies.[345] Modeled after prior successes, this initiative allows employees to pursue two distinct tracks: a supervisory/leadership track and an individual contributor track. This reflects the reality that not all cybersecurity experts want to be managers; some would prefer a nonsupervisory technical role. Building career paths that enable these employees to thrive bolsters retention and infuses the workforce with elite talent.

2. **Rotational Programs:** With careful planning and standardized job descriptions, organizations with cybersecurity roles in multiple departments, offices, or other components can take advantage of rotational programs. In the United States, both the legislative and executive branches of government have proposed creating cybersecurity rotational programs that move employees among federal departments.[346] Rotations into new or adjacent roles provide room to learn while relying on the same basic fundamental skills. This can be valuable at any stage in an employee's

career but is particularly helpful for entry-level employees who may not yet know what type of work is most interesting to them.

A good example is the U.S. National Security Agency's development program.[347] Upon hiring, entry-level employees rotate through a series of positions over the span of three years, allowing them to "enhance their skills, improve their understanding of a specific discipline and even cross-train into a new career field."[348] Thus, employees acquire an evolving series of opportunities and a clear indication that the employer values their development, while the agency gains a workforce that has broad knowledge of the organization and its various functions.

3. **Upskilling:** Public institutions likely already employ personnel in fields that are adjacent to cybersecurity, like information technology (IT) support, audit and compliance specialists, and risk analysts. Employer-sponsored training could allow these workers to grow into future work in cybersecurity. One particular challenge to executing upskilling programs effectively is aligning them with established career pathways. For example, a mid-career employee may not have the discipline-specific knowledge needed to move laterally into a mid-career level cybersecurity position but is unlikely to want to move to an entry-level position and start over.[349] The Federal Cybersecurity Reskilling Academy in the United States is attempting to address this challenge,[350] drawing on a pool of employees without an IT background who volunteered from positions across the federal government.

4. **Work-based Learning:** Fewer than a quarter of surveyed cybersecurity professionals feel that education programs are preparing students to enter the industry,[351] seeing hands-on experience as a better way of acquiring the necessary skills. In addition to using internships as a way to connect early-career workers with experience, some U.S. employers are beginning to experiment with registered apprenticeship programs in cybersecurity. Cybersecurity apprenticeships in U.S. public institutions are rare, but they exist,[352] and the potential for growth is generating interest.[353] In countries with a greater cultural familiarity with apprenticeships—for example, the United Kingdom[354]—cybersecurity apprenticeship programs are already underway, offering a compelling recruiting pitch for promising candidates.

5. **Hiring Requirement Exemptions:** To preserve a fair hiring environment, public institutions often implement requirements for new hires, specifying that they be from specific populations (for example, veterans), possess certain non-negotiable qualifications (for example, a bachelor's degree in a specific field), or be hired via specific pathways. However,

in the highly competitive market for cybersecurity talent, these requirements become increasingly burdensome. One tool to address this issue is a dedicated hiring system for cybersecurity professionals that bypasses these requirements.[355] Creating such a program requires a very clear and standardized definition of what constitutes a cybersecurity role. It is true that exempting cybersecurity professionals from standards and requirements that the rest of the workforce must still observe may not be universally popular.[356] However, creating flexibility does help to mitigate bureaucratic barriers in cybersecurity hiring.

6. **Public-Private Partnerships:** Employers often perceive cybersecurity hiring through the zero-sum perception that employers are competing with one another for a fixed pool of talent. A more sustainable long-term plan is for stakeholders to build a stronger cybersecurity ecosystem overall. For example, the Australian federal government established a nonprofit organization, AustCyber, to cultivate an Australian cybersecurity ecosystem,[357] including building a pipeline for cybersecurity talent. The project is set up to receive government grant funding as well as to offer matched funding for industry-led projects. This enables a hub for government collaboration with industry partners toward the shared goal of a stronger cybersecurity workforce.

Talent recruitment programs offer another potentially fruitful opportunity for public-private collaboration on cybersecurity workforce development. The aforementioned Cybersecurity Talent Initiative in the United States, for example, is a partnership between a number of government offices and corporations.[358] The partners combine on-the-job learning in federal offices and corporate-funded tuition support for those participants who eventually choose jobs in the private sector. While not ideal for the federal government from a retention standpoint, federal workplaces nonetheless benefit from the recruitment opportunity. In particular, such arrangements allow federal workplaces to interact with program participants who might otherwise go directly to the private sector, giving government offices a greater chance of retaining this talent than they would otherwise have had.

Talent exchange programs are another promising route for public-private cooperation. For example, the U.S. Department of Defense has established the Defense-Industry Talent Exchange Pilot Program to temporarily detail civilian employees to the private sector while placing private sector employees in public sector jobs.[359] The program offers an opportunity to forge stronger relationships between the Pentagon and its industry partners while offering participants a unique opportunity to gain a more multidimensional understanding of their field.

A few additional challenges hamper public institutions' efforts to hire cybersecurity talent. These include limitations on hiring foreign nationals, security clearance requirements for some positions,[360] the absence of a classification and monitoring system for the cybersecurity workforce,[361] and related limitations in the ability to assess the success of workforce initiatives.

Lessons Learned From Select Financial Centers

> "A regulator is little more than its staff. The recruitment, development, and retention of staff must be the number one priority."
> —Lyndon Nelson, Bank of England, summer 2020

Lessons From the UK

Recognizing that supervision was becoming an increasingly specialized activity, in 2005, the BoE reorganized its structure and created more specialist teams. The BoE now centralizes its risk specialists, including cyber risk experts, into a single Supervisory Risk Specialists Directorate. According to Lyndon Nelson, "This was a very positive move. We benefited from economies of scope and scale. Specialists liked to be with other specialists and enjoyed learning from each other."

To build its cyber risk team, the BoE prioritizes recruiting and retaining experts that understand social engineering, human behavior, and operations, not "reformed 'hackers.'" The cyber risk team has a diverse background of industry experience, including CISOs, consultants, technology specialists, and simulation experts. According to BoE officials, the BoE's model of centralized talent provides:

- "Flexible use of in-depth expertise to deal with the big issues. [The BoE] uses cross-firm work, data, and analytics to drive insights beyond the sum of [its] firm-specific work."
- The ability to "define job roles that recognize this experience as well as to offer dedicated salary premiums which reflect this expertise." Experts from the BoE note that "we still do not compete with the top tier of financial services firms, but it does make a difference."
- The ability to "concentrate staff from diverse industry backgrounds with exceptional experience and skill who are attracted by the [employment] proposition."[362]

SPOTLIGHT

The Aspen Institute runs a sector-agnostic working group focusing on the cybersecurity workforce in the United States with a specific focus on how to improve the classification, measurement, and overall data. See: https://assets.aspeninstitute.org/content/uploads/2018/11/Aspen-Cybersecurity-Group-Principles-for-Growing-and-Sustaining-the-Nations-Cybersecurity-Workforce-1.pdf

The BoE's model relies on its ability to attract specialists from the deep talent pool anchored to London, one of the world's global financial centers. The BoE anticipates that many of its staff will eventually move on, often to the private sector.[363] Its employment proposition—providing a market-wide perspective and insight into a premier regulatory body in exchange for an individual's expertise—may not be sustainable for central banks that lack the same prestige or thick labor markets.

Lessons From Singapore

The MAS has undertaken several unique initiatives that tackle the cybersecurity workforce challenge in three ways: (1) building a local talent pipeline, (2) developing internal talent, and (3) convening international talent.

(1) Building a local talent pipeline: The MAS focuses on developing a pipeline of cybersecurity talent within its jurisdiction that both the MAS and Singapore-based financial institutions can draw from.[364] Examples include:

- **Cybersecurity Capability Grant:** Launched by the MAS in 2018 to support Singapore-based financial institutions in establishing, expanding, or relocating cybersecurity functions to Singapore, these grants can be used to build up cybersecurity infrastructure capabilities and the talent pipeline. This facilitates the transfer of cybersecurity skill sets from overseas offices and deepens the cybersecurity skill sets of local employees, including Singaporeans.[365]

- **TeSa FinTech Collective:** Launched in 2017 by the MAS, in partnership with local universities, government agencies, and financial associations, this program aims to jointly develop industry-ready professionals capable of meeting the demand for emerging ICT skills like cybersecurity.[366] The program enhances preemployment and continuing education training for undergraduates, postgraduates, and working adults, especially fintech professionals, in emerging ICT skills.

- **FS-ISAC's Asia Pacific Regional Analysis Centre:** Launched by the MAS and FS-ISAC, the center provides internship opportunities where students gain exposure to real world cyber threats to build up their skills in cybersecurity.[367]

(2) Developing Internal Talent: The MAS charts out cybersecurity personnel learning and development through an internal Professional Requisites and Outcomes Framework, outlining a cybersecurity learning pathway and relevant certifications (such as ITIL, CISM, and CISSP).[368]

(3) Convening International Talent: The MAS oversees a major global financial center but must operate in Singapore's labor market, which is small relative to those in other major financial centers. Consequently, the MAS relies in part on attracting international cybersecurity talent.

Lessons From Italy

Italian financial authorities—including the Italian securities regulator CONSOB, the Bank of Italy, and the Ministry of Economy and Finance—prioritize retention of cyber talent through professional development programs.[369] For example, the Bank of Italy's Human Resources Directorate has designated cybersecurity skills as a strategic competency to shape and prioritize recruitment. Furthermore, specific cybersecurity training pathways are designed by internal experts and external consultants. Both the Italian Ministry of Economy and Finance and the Bank of Italy improve retention with rotational programs that provide employees with opportunities for work experiences in other institutions at both national and international levels.

Lessons From Hong Kong

The Professional Development Programme is one of three pillars of the Cybersecurity Fortification Initiative launched by the Hong Kong Monetary Authority (HKMA). This program is designed to increase the number of qualified cybersecurity professionals in the Hong Kong special administrative region. Together with the Hong Kong Institute of Bankers and the Hong Kong Applied Science and Technology Research Institute, the HKMA has developed a local training program and certification scheme for cybersecurity professionals.[370]

Lessons From Other Regulators

A recurring theme among financial authorities is that they cannot compete with the salaries of the private sector.[371] Although government starting salaries are attractive for cybersecurity professionals in some countries, public institutions tend to lose staff to the private sector as their skills mature. Public sector employers therefore try to attract talent with an employment proposition that emphasizes: (1) a call to public service, (2) job security, (3) work-life balance, and (4) the opportunity to work on a wide range of technical projects.[372] Some central banks offer specific degree programs to attract high school graduates with a clear career path within the institution.

There is no silver bullet workforce development strategy appropriate for all financial authorities. What works in one jurisdiction might have less success in another. For example, as the BoE's Lyndon Nelson explained: "In the more

developed economies, the regulator is not able to compete on salary and in many cases also on reputation. In less developed economies, the position is often reversed, with the regulator or central bank attracting some of the brightest and best of a country's talent."[373] In determining the right strategy, regulators should consider their external limitations and unique employment propositions.

Regulators that can offer sufficient prestige to compensate for lower public sector salaries might prioritize external recruitment and rotational programs.[374] The BoE, for example, can recruit staff with diverse industry experience because it operates in a thick labor market and provides staff with experience that will be valued in the private sector. Similarly, the ECB has rotational programs to bring in experts from other eurozone central banks.[375]

Regulators that cannot compete with private sector salaries might also prioritize upskilling internal talent and developing local talent pipelines. The Reserve Bank of India, for example, prefers to focus on upskilling its internal talent because of private sector competition.[376]

Financial authorities are exploring innovative mechanisms to address their workforce shortages. Some regulators increasingly rely on contractors. Others have special authority to temporarily offer their employees "market price compensation."[377] In interviews, many regulators expressed interest in developing a model for shared cybersecurity talent that would support all financial authorities within a jurisdiction, arguing that this model might improve specialization.

Recommendation 4.3: Government agencies and financial authorities should identify, improve, and better promote their employment proposition to cybersecurity professionals, including: (i) exposure to and responsibility for a broad range of technical issues, (ii) access to cutting-edge information and authorities, (iii) providing a market-wide perspective valued by the private sector, (iv) job security, and (v) a service mission to the public.

- *Supporting Action 4.3.1:* Leaders of financial authorities, and lawmakers when needed, should create mechanisms that give hiring managers greater flexibility, for example allowing them to offer salaries to cybersecurity professionals that are competitive with those offered by industry.

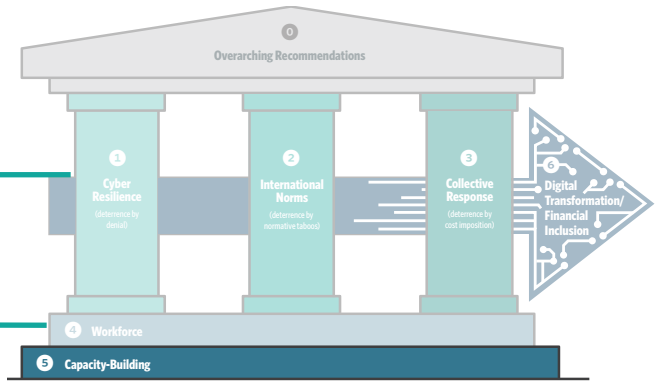
- *Supporting Action 4.3.2:* Financial authorities should design their workforce plans based on the assumption that staff will leave their positions after a few years rather than stay for the medium or long term. This provides the opportunity to think of such staff as a resource that will build capacity for the sector more broadly and to minimize risk resulting from staff turnover. This action will likely require organizations to maintain additional headcount on the assumption that some number of positions will be routinely vacant until replacements are hired.

- *Supporting Action 4.3.3:* Financial authorities should establish secondment mechanisms with government agencies that employ staff with cybersecurity expertise. Financial authorities may be able to attract and retain cybersecurity professionals more effectively by offering opportunities to work on cybersecurity challenges in other government agencies, or with private sector companies. At the same time, other government agencies tend to have limited situational awareness of the financial infrastructure and processes and could benefit from the expertise of seconded cyber supervisors and regulators.

- *Supporting Action 4.3.4:* Financial authorities should establish secondment mechanisms with the financial services and technology sectors. This will offer opportunities for increased knowledge transfer and cybersecurity capability adoption by both public and private sectors. Both sectors could benefit from exposure to alternative cybersecurity risk and operational perspectives, as well as initiatives and technologies that may be brought back to their home organizations for implementation.

CHAPTER 5

PRIORITY #5: CAPACITY-BUILDING



Crosscutting Issue #2: *Align and expand capacity-building efforts across all three core pillars for those seeking assistance.*

Problem Statement: Making Sense of the Nebulous Term "Capacity-Building"

The 2016 Bangladesh incident was a wake-up call for central banks and financial authorities around the world that the threat landscape had evolved beyond criminal activity, and certain threats could now pose systemic risk. The aftermath of the incident also revealed a significant gap in capacity to address cybersecurity. The IMF received significantly more requests from member states for guidance and assistance, and central banks and government agencies even in some G7 member states only had one or two staff members focusing on cybersecurity. Since the 2016 wake-up call, organizations have been busy staffing up, updating regulatory and policy frameworks, and integrating new technologies.

Cybersecurity capacity-building has therefore become a growing priority, especially considering the rising numbers of state-sponsored attacks and the increase in fraud during the coronavirus pandemic. At the same time, "capacity-building" is an amorphous term and requires clarification before we can progress from concept to action. Key questions are: What is it? Who does it? How is it done?

What is it? Capacity-building can be defined as "a way to empower individuals, communities and governments to achieve their developmental goals by

reducing digital security risks stemming from access and use of Information and Communication Technologies."[378] It can cover the spectrum from prevention to response, as illustrated in Figure 12.

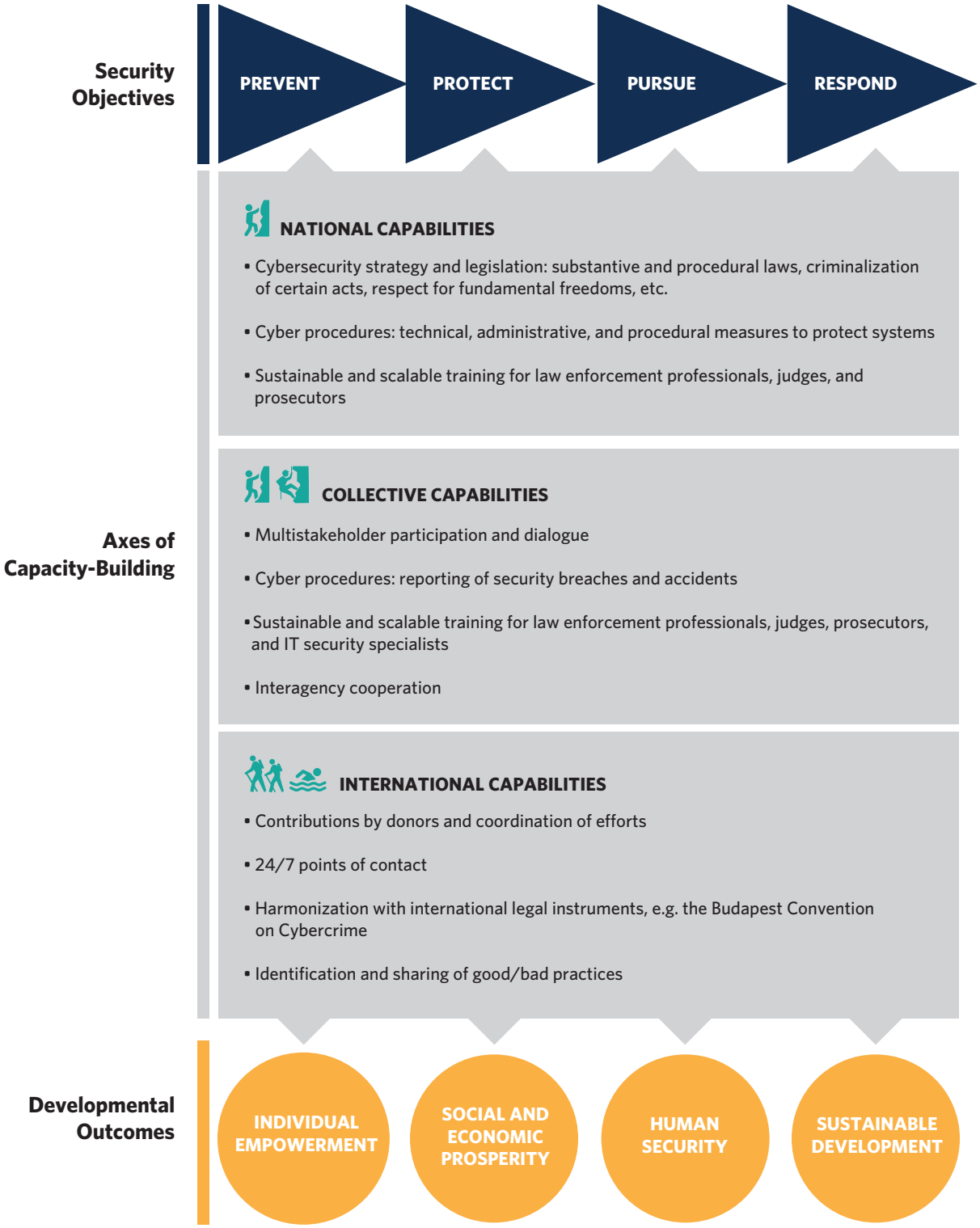
Who does it? Capacity-building can involve a variety of actors ranging from national to international figures and from government to nongovernmental stakeholders.

How is it done? This depends on whether the capacity-building in question focuses on policy, regulation, standards, organizational culture, or training. A growing literature on cybersecurity capacity-building offers frameworks,[379] principles,[380] and lessons learned.[381] Scholars also point to well-known challenges in other capacity-building efforts, ranging from overall questions about effectiveness,[382] asymmetric power dynamics, and the political interests of funders.[383]

In the context of this strategy document, cybersecurity capacity-building with respect to the financial system can be further broken down into how it aligns with the various core pillars. Table 4 provides a partial mapping of ongoing efforts in terms of the strategies laid out in this report. The IMF's capacity-building, for instance, focuses on increasing resilience, whereas the capacity-building efforts of the UNODC and the World Bank focus on strengthening law enforcement capacity.[384] UNIDIR offers materials for diplomats focusing on cybersecurity norms, and the AFI provides a guide on cybersecurity in the context of DFS.[385] Capacity-building in the private sector includes efforts by the major cloud service providers to help their clients build capacity through dedicated education and training programs.[386] And in some parts of the world, industry carries out its own private capacity-building due to local governments' limited ability to provide such services.

To narrow the focus, this strategy report provides a mapping but will not focus in depth on capacity-building efforts to tackle cyber crime or capacity-building efforts focusing on the diplomatic corps. Such efforts already date back at least a decade, are more mature, and have already received attention from initiatives like the aforementioned WEF Partnership Against Cybercrime,[387] Third Way's Cyber Enforcement Initiative, and the Global Forum on Cyber Expertise (GFCE).[388] The biggest challenge for these efforts is how they interconnect with each other, a challenge that several of the recommendations outlined in this report hope to address.

Figure 12: One Way to Conceptualize Cybersecurity Capacity-Building



Source: European Union Institute for Security Studies, "Riding the Digital Wave—The Impact of Cyber Capacity Building on Human Development," December 2014, https://www.iss.europa.eu/content/riding-digital-wave-%E2%80%93-impact-cyber-capacity-building-human-development.

Table 4: Map of Existing Capacity-Building Efforts

PRIORITY AREA	TYPE OF ACTOR	EXAMPLE
Operational Resilience	State actors	**CPMI-IOSCO:** Guidance on cyber resilience[389]
		IMF: Annual workshops and technical assistance training[390]
		FSB: Lexicon and cyber incident response practices[391]
		BIS: Cyber resilience tool kit[392]
		World Bank: Workshops and exercises[393]
		OAS: Report and convenings[394]
	Multistakeholder	**Carnegie:** Capacity-building tool box[395]
		Global Cyber Alliance: Cybersecurity tool kit[396]
	Nonstate actors	**SWIFT:** Customer Security Program[397]
		Cyber Risk Institute: Maturity-based model*[398]
		FS-ISAC: Summits and training[399]
		Cloud service providers: Cloud migration training[400]
International Norms	State actors	**UNIDIR:** Conference series and cyber policy portal[401]
		UNODA: Training for diplomats from UN member states[402]
		UN GGE/OEWG: Dedicated process and preparatory sessions[403]
		OSCE: Dedicated process and preparatory sessions[404]
		OAS: Dedicated process and preparatory sessions[405]
		ASEAN: Dedicated process and preparatory sessions[406]
	Multistakeholder	**GFCE:** Cybil portal[407]
	Nonstate actors	**Microsoft:** Awareness-raising and Cyber Peace Institute[408]
		DiploFoundation: Educational material[409]
		ICT4Peace: Educational material[410]
Collective Response	State actors	**UNODC:** Global Program on Cybercrime and Cybercrime Tools[411]
		World Bank: Combatting Cybercrime Tool Kit[412]
		Council of Europe: Cybercrime Program Office[413]
		Europol: Training and capacity-building program[414]
		INTERPOL: Project Cyber Americas II[415]
		AU: Forum on Cybercrime[416]
	Multistakeholder	**NCFTA:** U.S.-based partnership to tackle cyber crime[417]
		CDA: UK-based partnership to tackle cyber crime[418]
	Nonstate actors	**FSARC:** Project Indigo[419]
Financial Inclusion	State actors	**AFI:** Cybersecurity for financial inclusion framework and guide[420]
		UNSGSA: Briefing on cybersecurity[421]
	Multistakeholder	**World Economic Forum:** Consortium on FinTech Cybersecurity[422]
	Nonstate actors	**Mastercard:** Innovation lab[423]

Capacity-building efforts focused on cyber resilience are still nascent and are therefore the focus of the remainder of this section. The main challenge is that demand outpaces supply. In the wake of the 2016 Bangladesh incident, the IMF's five-person staff dedicated to the issue was inundated with requests for guidance and assistance from its member states. CGAP's vision was developed by a team of two. Such efforts are dwarfed by what SWIFT put behind the update of its Customer Security Program—out of self-interest, clearly, but nevertheless an impressive undertaking. Despite its importance, cybersecurity capacity-building is also still struggling to find its way into existing ODA budgets.

As demand for cybersecurity capacity grows, financial resources to increase supply are limited. In fact, financial resources are likely to shrink because of the coronavirus pandemic, which has ripped a hole in the coffers of governments that fund multilateral organizations and are the main contributors of ODA. As budgets get tighter, pressure to use limited resources more effectively will grow, raising questions about how best to organize cybersecurity capacity-building efforts for the financial system.

SPOTLIGHT

One standout example of public-private partnerships on cybersecurity capacity-building in the financial system is the Commonwealth Cyber Declaration Programme. This initiative arose out of the 2018 Commonwealth Cyber Declaration, an intergovernmental commitment to build cybersecurity capacity throughout Commonwealth states. Citigroup partnered with the UK government, Microsoft, and Templar Executives, a cybersecurity consultancy, to train over 1,000 individuals across the Commonwealth. Citigroup's contributions specifically focused on "strengthen[ing] resilience in the financial sector" of various Commonwealth states.[424] According to the UK Foreign, Commonwealth & Development Office, Citigroup provided valuable "training and information gathering support."[425]

Mapping the Status Quo: Nascent Efforts to Build Cyber Resilience Capacity

The International Monetary Fund's Vision

The IMF recognizes capacity development, in addition to surveillance and lending, as a core function for helping member countries "build strong economic institutions."[426] Well-trained supervisors and regulators are fundamental to bolstering cyber resilience in emerging financial markets. The IMF's

cybersecurity technical assistance program is critical to developing a cadre of financial supervisors and regulators that can keep pace with the financial sector's increasing interconnectedness and reliance on information technology.

Over the last three years, after it declared cybersecurity to be a financial stability risk, the IMF has incorporated into its capacity development efforts a program to assist financial regulators and supervisors with cybersecurity risk management.[427] The IMF's cybersecurity technical assistance program, implemented by the Monetary and Capital Markets Department, has three pillars:

1. **Annual Workshops:** These annual workshops, hosted at IMF headquarters in Washington, DC, bring together financial supervisors and regulators, industry representatives, and technical experts to share best practices, raise awareness about emerging risks, and implement cybersecurity exercises. The workshops have been hosted every December since 2017, and have focused on cyber hygiene, response and recovery, and operational resilience, respectively.

2. **Regional Technical Assistance Center Workshops:** These cyber security capacity-building workshops are hosted in all of the IMF's ten regional technical assistance centers,[428] in partnership with leading central banks in the region. The workshops serve member countries across twelve jurisdictions.

3. **Bilateral Technical Assistance Missions:** Bilateral technical assistance missions are undertaken at the request of member countries, and IMF experts work directly with financial regulators and supervisors to conduct a risk assessment and provide hands-on training.

The IMF's long-term vision is to build the capabilities of financial regulators and supervisors managing cybersecurity risk to help ensure more stable financial and monetary systems in low-income and developing countries. In order to scale this work, the IMF plans to build out and leverage its network of technical assistance centers and partner with regional champions. Future work through this network includes:

- Developing a durable training curriculum, with a focus on hands-on training.

- Making financial supervisors and regulators aware of existing cybersecurity risk management frameworks and best practices so that they do not have to write their own rules from scratch.

Cultivating partnerships and "buddy" systems between countries with mature cybersecurity risk management and low-income and developing countries with less experience. These partnerships are designed to encourage hands-on development.

CGAP's Vision

CGAP, an independent think tank focused on financial inclusion housed at the World Bank, has developed a concept for regional cyber security resource centers to help low-income countries address cybersecurity risks in DFS.[429] The concept, illustrated in Figure 13, proposes addressing the cybersecurity resources and capabilities gap through shared cybersecurity resource centers so that multiple countries can pool resources and talent. Specifically, CGAP proposes that:

- Regional cybersecurity response centers "facilitate cross-border exchange, operate early warning systems, and share regional trends, threats and good practices with other regions and global platforms."[430] These centers would act as a neutral platform for policymakers and financial services providers to collaborate and exchange threat intelligence.

- Continental cybersecurity coordination centers would function as hubs for international and regional collaboration as well as for knowledge and intelligence sharing, including guidance on implementing cybersecurity regulations and standards. Regional cybersecurity response centers would support in-country incident response teams with crisis management, training, and capacity-building services. In-country centers would field security operations teams that focus on operationalizing services like information sharing, 24/7 security monitoring, and emergency response.

- The centers would build on and complement existing service structures like national CERTs and CSIRTs. Additionally, centers would collaborate with local universities for research and development projects and leverage local technical expertise and talent pipelines. Emphasis would be placed on recruiting female students to reduce the gender disparities in IT hiring.

- The centers are intended to become self-sustaining after a few years of reliance on start-up funding as their efficiency increases through economies of scale, in part from mutualizing resources and expenses across regions and countries. Initial feedback from DFS providers and central banks is positive and reflective of the demand for more cybersecurity resources.[431]

Figure 13: CGAP's Vision

Source: CGAP

The World Bank's Activities

The World Bank has undertaken a number of initiatives to strengthen cybersecurity in the financial sector. This work can be seen across three broad categories: (1) capacity-building for financial regulators and supervisors, (2) Financial Sector Assessment Programs led jointly by the World Bank and the IMF, and (3) capacity-building to counter cyber crime in the financial system.

- **Capacity-building for financial regulation and supervision:**[432] This is the World Bank's main line of work around cybersecurity in the financial sector. It is led by the World Bank's Financial Sector Advisory Center within the Finance, Competitiveness & Innovation Global Practice.[433]

- **"Financial Sector's Cybersecurity: A Regulatory Digest":** According to the World Bank, this publication is "intended to be a live, periodically updated compilation of recent laws, regulations, guidelines and other significant documents on cybersecurity for the financial sector."[434] The most recent edition, the fifth, was published in July 2020.

- **Regional Workshop on Financial Cyber Resilience:** This workshop discussing cyber resilience was hosted in Mexico City in November 2019 by the World Bank and the Center for Latin American Monetary Studies.[435]

- **Cybersecurity: A Simulation Exercise:** This exercise was hosted at the Financial Inclusion Global Initiative 2019 Symposium.[436]

- **Capacity-building to counter cyber crime in the financial system:** This stream of work was driven by the Global Cybersecurity Capacity Program (2016–2019), launched by the World Bank in partnership with the Global Cybersecurity Center for Development (operating under the Korea Internet & Security Agency) and Oxford University's Global Cybersecurity

Capacity Centre. The World Bank also developed a specific tool kit dedicated to combating cyber crime.[437]

Cyber Risk Institute's Vision

After a survey of CISOs reported spending 40 percent of their time reconciling various global cybersecurity regulations, the FSSCC, led by the BPI and the ABA, developed a tool to simplify the compliance process: the Financial Services Sector Cybersecurity Profile (the Profile).[438] The Profile is intended to address the concern that "if national level approaches are developed in isolation, without global coordination, the resulting fragmentation will inhibit the strengthening of the financial sector's operational resilience and result in inefficiencies or confusion that increase the cross-border impacts of disruptive events."[439]

The Cyber Risk Institute (CRI), grew out of the FSSCC's work on the Profile. The CRI will maintain and update the Profile, which consolidates more than 2,300 regulations into 277 diagnostic statements to help financial institutions speed up compliance. Moreover, the Profile uses "impact tiering" to tailor its recommendations based on a financial institution's systemic importance.[440] Over the next three years, the CRI plans to road test the Profile among financial institutions and regulators, as well as promoting alignment between the Profile and future standards and regulations.[441] The Profile currently incorporates frameworks from the ISO, the National Institute of Standards and Technology (NIST), and CPMI-IOSCO, and the CRI is mapping additional regulations at the request of other financial authorities. The CRI is additionally working on a "maturity methodology," which is expected to be released by 2021.[442]

Global Forum for Cyber Expertise

The GFCE is a nonprofit coalition whose mission is "to strengthen cyber capacity and expertise globally through international collaboration and cooperation."[443] The GFCE was envisioned in Seoul at the third Global Conference on Cyber Space; it was officially established in 2015 at the fourth Conference in The Hague by the Dutch government and forty-one ministers and senior representatives from industry and international organizations.[444]

The GFCE is the primary coordinating platform for cyber capacity-building. Its focus is to coordinate cyber capacity projects, share knowledge and expertise by recommending tools and publications, and act as a clearing house to match needs for cyber capacities with offers of support.[445] Its members are

primarily international organizations and governments; its only members from the financial system are FS-ISAC and the World Bank, although some member countries work directly through the GFCE on financial sector issues.

The GFCE supports a range of initiatives with partner institutions,[446] some of which are related to the financial system. For example, it partners with international organizations like the UNODC and INTERPOL on building capacity to counter financial cyber crime in Africa and Southeast Asia.[447] In addition, the GFCE's Critical Information Infrastructure Protection Initiative supports government policymakers responsible for critical infrastructure protection, including protection of "financial systems and process control systems."[448]

The GFCE also maintains a cyber capacity database, Cybil, to collect and archive capacity-building projects, their implementors, and their beneficiaries—this database includes dozens of capacity-building projects geared toward the financial system.[449] Cybil and other GFCE products can provide situational awareness, help avoid duplication of work, and align efforts for future sector-specific cyber capacity-building. The GFCE may also provide a potent means of disseminating future capacity-building products among less mature financial institutions and regulators.

Recommendations: Aligning Resources to Maximize Impact

The biggest question in coming years will be how best to organize the still nascent but expanding efforts by multilateral institutions such as the IMF, the World Bank, and the GFCE and those undertaken by industry such as the CRI and FS-ISAC.

Recommendation 5.1: The G20 Finance Ministers and Central Bank Governors should adopt a communiqué creating a mechanism to operationalize a coherent approach to cybersecurity capacity-building for the financial sector. Such an approach could emulate and build on the lessons learned from the Global Infrastructure Hub launched during Australia's G20 presidency or the Global Partnership for Financial Inclusion (GPFI) launched during South Korea's G20 presidency.

- *Supporting Action 5.1.1:* To clarify roles and responsibilities, the G20 Finance Ministers and Central Bank Governors' communiqué

should declare that one of the international financial institutions (ideally the IMF, as the sector-specific multilateral organization) will be the lead coordinating agency for this mechanism, which would also include the World Bank, the Consultative Group to Assist the Poor (CGAP), the Alliance for Financial Inclusion (AFI), and other relevant stakeholders.

- *Supporting Action 5.1.2:* Considering ongoing capacity-building efforts by the private sector—for example, the Customer Security Program advanced by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)—and the public sector's limited financial resources in the wake of the pandemic, the G20 Finance Ministers and Central Bank Governors should invite private sector firms and other relevant stakeholders to participate in and support such capacity-building initiatives, as is the practice in a number of states today.

- *Supporting Action 5.1.3:* The G20 Finance Ministers and Central Bank Governors should welcome and encourage the use of the "Cyber Resilience Capacity-building Tool Box for Financial Organizations," developed by the Carnegie Endowment for International Peace and launched in partnership with the IMF, SWIFT, FS-ISAC, and other organizations.

Models created by the G20, such as those outlined in Recommendation 5.1,[450] provide a mechanism to bring together governments, private sector entities, and other relevant stakeholders, including the various multilateral development banks.[451] Another option would be to create such a mechanism under the auspices of the GFCE. However, this presents challenges given the GFCE's more politicized origins through the Global Conference on Cyber Space series.[452]

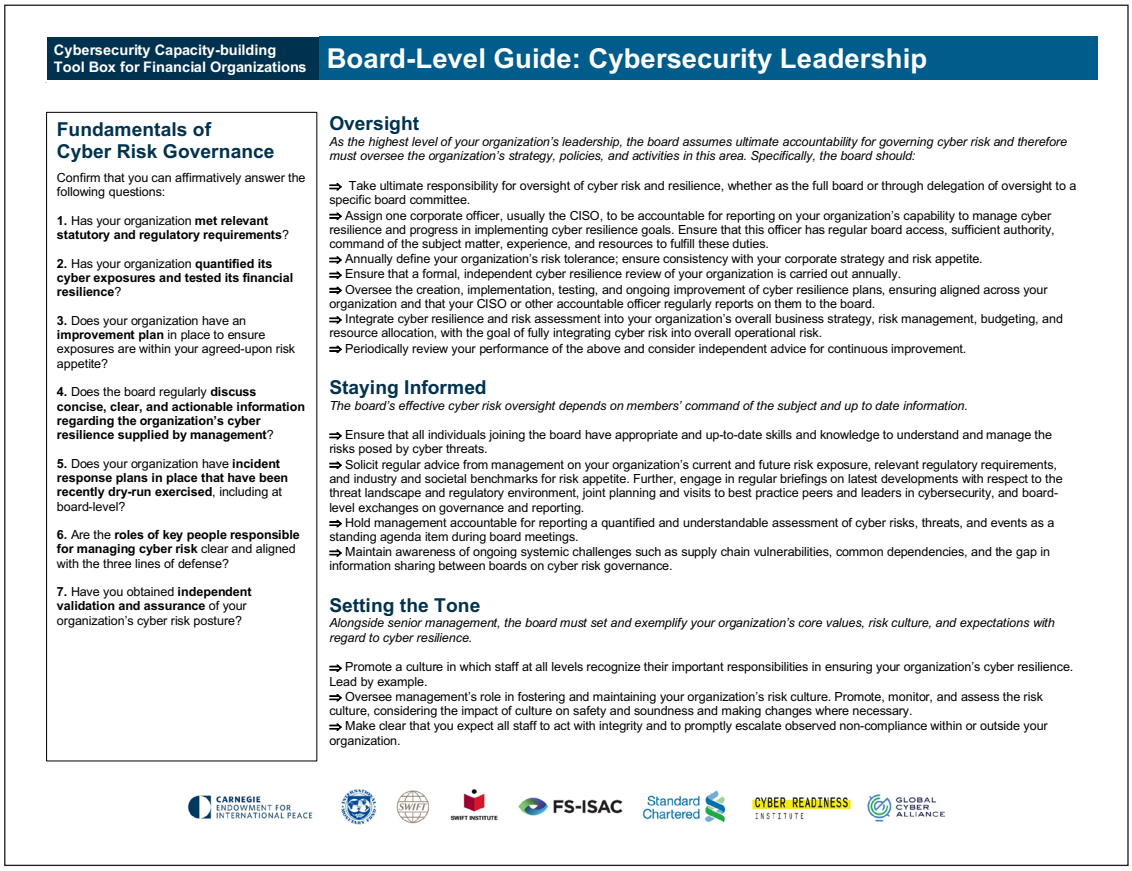
> "The G20 needs to not walk away from poor countries because it has its own fiscal constraints—we need both capacity-building commitment and a commitment to genuine partnership in information sharing and cooperation."
> —Expert at FinCyber Brainstorming Workshop in May 2020

Organizing such a mechanism under the auspices of the IMF would free up the capacity of the other sector-agnostic organizations like the World Bank

to focus on the many other critical infrastructure sectors, such as health and energy, for which states need support. However, the IMF lacks the country office infrastructure of the World Bank and would therefore still benefit from some support for specific areas and activities.

In 2019, Carnegie launched the "Cyber Resilience Capacity-building Tool Box for Financial Organizations" in partnership with the IMF, SWIFT, FS-ISAC, Standard Chartered, the Cyber Readiness Institute, and the Global Cyber Alliance.[453] Available in several languages including Arabic, Dutch, English, French, Portuguese, Russian, and Spanish, this tool box will be updated by the end of 2020 and a new version launched in 2021. Figure 14 shows a page from the tool box.

Figure 14: One of the Tool Box Guides



Cybersecurity Capacity-building Tool Box for Financial Organizations

Board-Level Guide: Cybersecurity Leadership

Fundamentals of Cyber Risk Governance

Confirm that you can affirmatively answer the following questions:

1. Has your organization **met relevant statutory and regulatory requirements**?

2. Has your organization **quantified its cyber exposures and tested its financial resilience**?

3. Does your organization have an **improvement plan** in place to ensure exposures are within your agreed-upon risk appetite?

4. Does the board regularly **discuss concise, clear, and actionable information regarding the organization's cyber resilience supplied by management**?

5. Does your organization have **incident response plans in place that have been recently dry-run exercised**, including at board-level?

6. Are the **roles of key people responsible for managing cyber risk** clear and aligned with the three lines of defense?

7. Have you obtained **independent validation and assurance** of your organization's cyber risk posture?

Oversight

As the highest level of your organization's leadership, the board assumes ultimate accountability for governing cyber risk and therefore must oversee the organization's strategy, policies, and activities in this area. Specifically, the board should:

⇒ Take ultimate responsibility for oversight of cyber risk and resilience, whether as the full board or through delegation of oversight to a specific board committee.
⇒ Assign one corporate officer, usually the CISO, to be accountable for reporting on your organization's capability to manage cyber resilience and progress in implementing cyber resilience goals. Ensure that this officer has regular board access, sufficient authority, command of the subject matter, experience, and resources to fulfill these duties.
⇒ Annually define your organization's risk tolerance; ensure consistency with your corporate strategy and risk appetite.
⇒ Ensure that a formal, independent cyber resilience review of your organization is carried out annually.
⇒ Oversee the creation, implementation, testing, and ongoing improvement of cyber resilience plans, ensuring aligned across your organization and that your CISO or other accountable officer regularly reports on them to the board.
⇒ Integrate cyber resilience and risk assessment into your organization's overall business strategy, risk management, budgeting, and resource allocation, with the goal of fully integrating cyber risk into overall operational risk.
⇒ Periodically review your performance of the above and consider independent advice for continuous improvement.

Staying Informed

The board's effective cyber risk oversight depends on members' command of the subject and up to date information.

⇒ Ensure that all individuals joining the board have appropriate and up-to-date skills and knowledge to understand and manage the risks posed by cyber threats.
⇒ Solicit regular advice from management on your organization's current and future risk exposure, relevant regulatory requirements, and industry and societal benchmarks for risk appetite. Further, engage in regular briefings on latest developments with respect to the threat landscape and regulatory environment, joint planning and visits to best practice peers and leaders in cybersecurity, and board-level exchanges on governance and reporting.
⇒ Hold management accountable for reporting a quantified and understandable assessment of cyber risks, threats, and events as a standing agenda item during board meetings.
⇒ Maintain awareness of ongoing systemic challenges such as supply chain vulnerabilities, common dependencies, and the gap in information sharing between boards on cyber risk governance.

Setting the Tone

Alongside senior management, the board must set and exemplify your organization's core values, risk culture, and expectations with regard to cyber resilience.

⇒ Promote a culture in which staff at all levels recognize their important responsibilities in ensuring your organization's cyber resilience. Lead by example.
⇒ Oversee management's role in fostering and maintaining your organization's risk culture. Promote, monitor, and assess the risk culture, considering the impact of culture on safety and soundness and making changes where necessary.
⇒ Make clear that you expect all staff to act with integrity and to promptly escalate observed non-compliance within or outside your organization.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE

Recommendation 5.2: The member states of the Development Assistance Committee of the Organisation for Economic Co-operation and Development (OECD) should integrate cybersecurity capacity-building into official development assistance (ODA) budgets and significantly increase assistance to countries in need. Even with technical cooperation mechanisms, international financial institutions such as the IMF and World Bank currently do not have the capacity to respond to the disruptions to critical financial services or the hundreds of millions of dollars stolen in countries around the world.

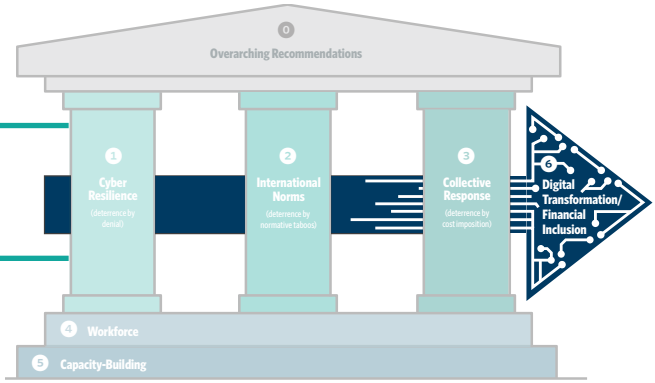
Recommendation 5.3: To further expand and strengthen ongoing capacity-building around international cyber norms and to advance the objectives outlined in this report, the UN Institute for Disarmament Research (UNIDIR) and the UN Office for Disarmament Affairs (UNODA) should integrate a specific module focusing on the financial sector into their capacity-building material.

Recommendation 5.4: To further expand and strengthen ongoing capacity-building efforts with respect to tackling cyber crime more effectively, state and industry stakeholders should support the efforts by the Council of Europe, Europol, INTERPOL, the UN Office on Drugs and Crime (UNODC), and the World Bank to strengthen capabilities to address cyber crime.

CHAPTER 6

PRIORITY #6: DIGITAL TRANSFORMATION AND FINANCIAL INCLUSION

Crosscutting Issue #3: *Safeguard financial inclusion and the G20's achievements of the past decade in this area.*



Problem Statement: Innovative Digital Financial Services Bring New Risks

Financial inclusion has been a top priority for the international community since the G20 recognized financial inclusion as one of the main pillars of the global development agenda in 2010. According to the latest Global Findex report, between 2014 and 2017 alone, 515 million adults opened accounts at financial institutions, raising the percentage of banked adults worldwide from 62 percent to 69 percent.[454] This rapid increase has been facilitated by innovative DFS that do not require the infrastructure of traditional banks. In low-income economies, there are twice as many mobile money accounts as bank accounts per 1,000 adults.[455] This trend is not slowing down. It is projected that by 2022, 1 billion people in Africa will have internet access, thereby also expanding opportunities to advance financial inclusion.[456]

In some countries, DFS have become critical. As early as 2016, Kenya's National Treasury was expressing concerns that M-Pesa, a mobile phone-based money transfer service, was becoming indispensable to the function of the payments system.[457] According to John Walubengo, a member of the faculty of Computing and Information Technology at the Multimedia University of Kenya:

> M-Pesa has grown from an option to literally being a must-have financial service for millions of Kenyans. It has also become integrated in the lifestyles of Kenyans in terms of paying for anything, ranging from groceries to school fees and even bribes. . . . Whereas it is not the only mobile money service in the country and in theory Kenyans do have options, the reality, however, is that it is the only such service with the prerequisite agent network that has a geographic reach and depth to serve its close to 25 million mobile money subscribers. Twenty-five million subscribers is more than the adult population in the country. It is more than the whole of the voting population, and is way more than the employed population of this country.[458]

Financial markets in sub-Saharan Africa, Asia, and Latin America have already experienced an increase in cyber attacks, and markets with more DFS transactions are targeted more often.[459] For example, financial markets in Asia see the highest volume of mobile banking and digital payment applications, and they also experience the highest volume of cyber attacks on financial institutions.[460] One African cybersecurity firm estimated in 2017 that the cost of cyber crime to Africa's banking sector was at least $248 million.[461]

Focusing on cybersecurity is important because DFS introduce a new element of cyber risk. For one, mobile banking is vulnerable to basic cyber attacks. Mobile money systems are vulnerable to several basic attacks and types of fraud. Hackers can exploit vulnerabilities in hardware, software, and at the network level. SIM swaps allow hackers to circumvent two-factor authentication protocols. Banking trojans and mobile malware infect smartphones. Transactions are usually carried out using insecure devices, mostly feature phones, that do not offer the end-to-end encryption that smart phones do.[462]

At the network level, the fundamental problem is that mobile networks rely on insecure communications protocols that are not designed to protect financial information.

Mobile phones rely on protocols like Unstructured Supplementary Service Data and Short Message Service, which hackers can exploit over the network. One exploit involves hackers eavesdropping by setting up a fake mobile network base station to intercept phone traffic.[463] This means that DFS providers must implement their own security measures and can never rely on mobile network operators (MNOs) or other external providers for security.[464]

The specific challenge is that unbanked and underbanked customers are easy targets for cyber criminals because they tend to have lower levels of digital

literacy. For example, it is common practice for PINs to be shared among local communities for convenience.[465] Even if individuals are aware of cyber risks, they are pressured to choose affordable products over secure products. For instance, pirated software is more prevalent in developing countries, making its users more vulnerable if the software does not get patched.[466]

Cyber criminal activity has shifted in response to the growth in online banking by less cyber mature customers in developing regions. Experts have observed cyber criminals moving their activity away from high-income countries and refocusing on less cyber-mature financial markets.[467] Banks and payment service providers in emerging financial markets experience a high volume of cyber attacks. For example, in 2019, Kaspersky Lab reported a 56 percent increase in mobile banking malware.[468]

Most governments are unprepared to counter cyber criminals, and developing countries are especially under-resourced. According to the International Telecommunication Union, "cybercriminals see Africa as a safe haven to operate illegally with impunity."[469] Symantec reported that, out of fifty-four countries in Africa, thirty lacked specific legal provisions to "fight cyber crime and deal with electronic evidence."[470] DFS providers are also constrained by the significant dearth of cybersecurity talent in Africa.[471]

It is important to note that the most significant cybersecurity risk for DFS providers is still insider threats like employee fraud. Multiple surveys show that insider threats are the most common and greatest concern among DFS providers.[472] Paul Makin, an expert at the intersection of financial inclusion and cybersecurity, explained that three separate African MNOs almost faced financial ruin as a result of internal thefts from employees.[473] In 2017, a major MNO in Kenya reported that they fired fifty-two staff members caught engaging in fraudulent activities.[474]

Mapping the Status Quo: Nascent but Fragmented Efforts

A key challenge to strengthening cybersecurity in the context of financial inclusion over the coming years is the fragmentation of the ecosystem. Today, a plethora of institutions focus on advancing financial inclusion, but the space is fragmented by regional initiatives, by competing international institutions, and by inconsistent focus. The most cohesive initiative is the G20's GPFI, a platform for G20 states, nonmember states, and other stakeholders that

implements the G20 Financial Inclusion Action Plan (FIAP). The FIAP aligns efforts with the UN's 2030 Agenda for Sustainable Development and the G20's "High-level Principles for Digital Financial Inclusion," and it aims to provide an evolving financial framework for states, regional organizations, and industry.

The three primary implementing partners of the GPFI are the AFI, CGAP, and the International Finance Corporation. Other key initiatives include the UN Secretary General's Special Advocate (UNSGSA) for Inclusive Finance for Development, and on-the-ground initiatives, like Suricate Solutions, which provides cybersecurity resources directly to the underbanked.

Despite the prevalence of leapfrogging and growing reliance on DFS, most financial inclusion efforts have only recently begun to seriously consider the cybersecurity risks that may ensue. The first more visible efforts to address cybersecurity risks with respect to financial inclusion occurred in 2017 when the AFI hosted a workshop dedicated to this issue.[475] A year later, the UNSGSA for Inclusive Finance for Development published a brief focusing on cybersecurity.[476] In November 2019, the AFI published "Cybersecurity for Financial Inclusion: Framework and Risk Guide," which provides key principles and best practices to assist regulatory and supervisory authorities dealing with cybersecurity risk in the financial sector.[477] The same month, CGAP published "Cyber Security in Financial Sector Development: Challenges and Potential Solutions for Financial Inclusion."[478]

Another sign that cybersecurity is rising on the financial inclusion agenda is in the Bill & Melinda Gates Foundation's grantmaking. A crucial funder of financial inclusion efforts worldwide through its Financial Services for the Poor program, the Gates Foundation awarded the first grant explicitly focused on cybersecurity in DFS in 2018, to Columbia University's DFS Observatory. In November 2019, the Gates Foundation awarded four grants to CREST, the Alan Turing Institute, Carnegie Mellon University, and ID4Africa, and an additional grant focused on AML/financial crime to the Royal United Services Institute.[479] (These are grants focusing specifically on cybersecurity. Other grants also touch on cybersecurity but without an explicit focus.)

The DFS Observatory at Columbia University was established in 2016 with a focus on the expansion, innovation, and regulation of DFS around the world but particularly in developing countries. In addition to conducting research, the DFS Observatory houses a legal library with a collection of over 800 DFS-related laws, policies, and regulations across fifty-eight countries, plus an archive of regulatory sandboxes.[480] With respect to cybersecurity, the DFS Observatory is also developing an "actionable Cybersecurity Risk

Management Framework" (A-RMF) for actors in the DFS ecosystem in developing countries.[481] The A-RMF is designed to first evaluate a user's cybersecurity maturity, based on international cybersecurity standards, principles, and processes, and then conduct a DFS-specific risk assessment based on that evaluation. The A-RMF also provides a tailored threat matrix based on the user's risk assessment, including specific vulnerabilities and potential responses to address them.

A unique challenge to strengthening cybersecurity in the context of financial inclusion efforts is the potential unintended consequence that too strong a focus on cybersecurity could chill the development of financial inclusion initiatives and their capacity for innovation. A separate challenge is that financial inclusion often involves a new set of actors that provide technologies like mobile money, digital currencies, and other variations of distributed ledger technologies that are not yet fully embedded in ongoing policymaking processes. Resource constraints and the need to focus on the overall mission of financial inclusion may further complicate efforts to integrate cybersecurity in financial inclusion.

Recommendation 6.1: The G20 heads of state should strengthen coordination among existing financial inclusion and cybersecurity efforts so as to align limited resources and maximize their impact, especially in the wake of the pandemic. They should also initiate an annual conference to assess latest developments and coordinate next steps; the convening should include major donors, the World Bank, IMF, AFI, CGAP, and other relevant stakeholders.

- *Supporting Action 6.1.1:* The G20 should clarify the role of international financial institutions like the World Bank, CGAP, and the IMF with respect to cybersecurity and financial inclusion. They should also emphasize the need to coordinate on issues that overlap across these institutions.

- *Supporting Action 6.1.2:* The GPFI should deepen the connections between financial inclusion initiatives and the cybersecurity community. As DFS continue to be expanded, especially in the wake of the pandemic, it is critical to develop greater collaboration between the financial inclusion and cybersecurity communities.

- *Supporting Action 6.1.3:* The GPFI should deepen the connections between financial inclusion actors and the law enforcement community. As more people gain access to financial services, the platforms they use will become increasingly attractive targets for cyber criminals. By strengthening the relationship between the financial inclusion community and the law enforcement community, stakeholders can more effectively address cyber crime that targets products and services used for financial inclusion.

From Recommendation to Implementation

Carnegie's FinCyber initiative will host a conference on "Cybersecurity and Financial Inclusion" together with the IMF, the World Bank, and the WEF on December 10, 2020, as a first step to create more connective tissue among the relevant stakeholders.

Recommendation 6.2: A network of experts should be created to focus specifically on cybersecurity and financial inclusion in Africa to complement other existing regional initiatives. The fifty-four countries in Africa are experiencing a significant transformation of their financial sectors as they extend financial inclusion and leapfrog to DFS. At the same time, this transformation makes African countries a prime target for cyber criminals who exploit soft targets and financial institutions with limited capacity to effectively protect themselves. Cybersecurity expertise across the African continent remains limited and scattered.

Recommendation 6.3: The G20 should highlight that cybersecurity must be designed into technologies used to advance financial inclusion from the start rather than included as an afterthought. An example of such a foundational expectation is the reference in the GPFI's "G20 Action Plan on SME Financing" to a strong credit infrastructure as a fundamental requirement for small- and medium-sized enterprises to have access to loans and other credit. By looking ahead and mapping initiatives that will come online in the coming years, GPFI can help ensure that cybersecurity will ideally no longer be an

afterthought but be incorporated in future financial inclusion developments beyond payment systems.

Recommendation 6.4: The GPFI, main funders, and DFS platforms should explore how financial inclusion efforts could be leveraged to increase general awareness of basic cybersecurity principles. Raising awareness of best cybersecurity practices is critical, especially among users in developing countries, who recently gained access to financial services and the internet, often via a mobile phone. Financial inclusion platforms could be leveraged to offer basic cybersecurity resources for the individuals and businesses using them.

From Recommendation to Implementation

To help foster a community of experts such as that envisioned in Recommendation 6.1, Carnegie is creating a network of experts focusing on cybersecurity and financial inclusion in Africa. Carnegie will leverage this network of experts to carry out research: (i) mapping key issues and challenges as well as the disconnect between global and local efforts; (ii) analyzing the threat landscape in Africa; (iii) identifying lessons learned from DFS in the Global South for the Global North; (iv) exploring how DFS could be leveraged to increase basic cybersecurity principles; and (v) assessing preliminary insights from the coronavirus's impact on cybersecurity with respect to DFS.

APPENDIX A: OVERVIEW OF RELEVANT GROUPINGS AND THEIR MEMBERSHIP

Members of the G20	Major Financial Markets	Members of the G10	Major Cyber Powers	States With Global Systemic Insurers	States With Global Systemic Banks	Globally Systemically Important Insurers[482]	Globally Systemically Important Banks[483]
UK	UK	UK	UK	UK (2)	UK (4)	Aegon	Agricultural Bank of China
United States	United States	United States	United States	United States (3)	United States (8)	Allianz	Bank of America
China	China		China	China (1)	China (4)	AIG	Bank of China
Germany	Germany	Germany		Germany (1)	Germany (1)	Aviva	Bank of New York Mellon
France		France		France (1)	France (3)	AXA	Barclays
Japan	Japan	Japan			Japan (3)	MetLife	BNP Paribas
Canada	Canada	Canada			Canada (1)	Ping An	China Construction Bank
Italy		Italy			Italy (1)	Prudential	Citigroup
Russia			Russia			Prudential Financial	Crédit Agricole
Argentina							Credit Suisse
Australia	Australia						Deutsche Bank
Brazil							Goldman Sachs
India							Groupe BPCE
Indonesia							HSBC
Mexico							Industrial and Commercial Bank of China
Saudi Arabia							ING
South Africa							JPMorgan Chase
South Korea							Mitsubishi UFJ FG
Turkey							Mizuho FG
	Hong Kong						Morgan Stanley
	Switzerland	Switzerland			Switzerland (2)		Royal Bank of Canada
	Singapore						Santander Bank
	Luxembourg						Société Générale
	United Arab Emirates						Standard Chartered
		Sweden			Sweden (1)		State Street
		Belgium					Sumitomo Mitsui FG
		Netherlands		Netherlands (1)	Netherlands (1)		Toronto Dominion
			Israel				UBS
			North Korea				UniCredit
			Iran				Wells Fargo
					Spain (1)		

APPENDIX B:
OVERVIEW OF EXISTING FINCERTS

		Public Sector FinCERTs
G7	France	CERT Banque de France / CERT Caisse des Dépôts
	UK	NCSC / Bank of England Cyber Defence Centre
	Italy	CERT Banca d'Italia
	Germany	CERT-Bundesbank
	Japan	-
	US	-
	Canada	-
Other Government	Denmark	Nordic Financial CERT
	Finland	Nordic Financial CERT
	Iceland	Nordic Financial CERT
	Israel	Israeli FinCERT
	Norway	Nordic Financial CERT
	Portugal	CSIRT Banco de Portugal
	Russia	Russia FinCERT (Central Bank of Russia)
	Singapore	Financial Sector Security Operations Centre (FS-SOC, Monetary Authority of Singapore)
	South Korea	Financial Security Institute CERT
	Sri Lanka	Sri Lanka FinCSIRT (Central Bank of Sri Lanka)
	Sweden	SBAB-SIRT (SBAB Bank AB)
	Sweden	Nordic Financial CERT
	Switzerland	SWITCH-CERT
	Tunisia	Tunisian Financial CERT
Multilateral	OCINT-CSIRT	World Bank Group
	EU	CSIRT-ECB (European Central Bank)

This list does not include the national cybersecurity agencies, CIRTs, CSIRTs, or CERTs that provide services to but are not exclusively focused on the financial sector.

Financial Institution CERTs (TF-CSIRT and/or FIRST accredited)	
Argentina	Banelco CSIRT
Australia	CBAcert (Commonwealth Bank of Australia)
Australia	nabCERT (National Australia Bank)
Austria	Raiffeisen Informatik CERT
Belgium	KBC Group CERT
Canada	BMO InfoSec Incident Response Team
Canada	CIBC CIRT
Canada	TDBFG CSIRT (TD Bank)
China	Alibaba Security Response Center
Colombia	CSIRT Financiero Asobancaria
Czech Republic	CSIRT CSAS
Czech Republic	CSOB-Group-CSIRT
Czech Republic	NN-Group CSIRT
Denmark	JN Data Cyber Defence Center
Denmark	NetsCERT (Nets A/S)
France	AXA CERT
France	CERT-AG (Crédit Agricole)
France	CSIRT BNP Paribas
France	CERT Groupe BPCE
France	CERT SG (Société Générale)
France	CERT La Poste
Germany	Commerzbank CERT
Germany	Deutsche Bank Cyber Threat Response Team
Germany	S-CERT (German Savings Banks Organization)
Germany	Clearstream—Deutsche Boerse AG CERT
Greece	Alpha Bank CSIRT
Italy	CERTFin
Italy	Intesa Sanpaolo CSIRT
Japan	Mitsubishi UFJ Financial Group (CERT Japan)
Japan	Hitachi Incident Response Team
Japan	SoftBank CSIRT
Luxembourg	DBG-CERT
Malaysia	Standard Chartered Cyber Defence Centre
Netherlands	ING CCERT
Netherlands	PGGM-CERT
Netherlands	Rabobank Cyber Defense Center
Norway	DNB Cyber Defence Center
Norway	SpareBank 1 Incident Response Team
Poland	CERT PKO Bank Polski
Poland	CERT Alior
Poland	CERT BIK (Biuro Informacji Kredytowej)
Poland	CERT mBank
Poland	Polish Financial CERT (Polish Bank Association)
Portugal	Euronext CSIRT
Singapore	DBSCERT
South Africa	Standard Bank Group CSIRT
Spain	SIA-CEC CERT
Spain	BBVA CERT
Spain	CaixaBank Team CSIRT

Financial Institution CERTs (TF-CSIRT and/or FIRST accredited) cont.	
Spain	Santander Global CERT
Spain	MAPFRE-CCG-CERT
Sweden	Handelsbanken SIRT
Sweden	SEB CSIRT
Sweden	Swedbank SIRT
Switzerland	Bank Vontobel CERT
Thailand	Thailand Banking Sector CERT (Thai Bankers' Association)
UK	HSBC CSIRT
UK	ISPIRIT (Barclays Information Security and Privacy)
UK	Royal Bank of Scotland, Investigation and Threat Management
Ukraine	KredoBank Cybersecurity Center
U.S.	Bank of America/Merrill Lynch Computer Incident Response TeamCIRT
U.S.	Capital Group Security Intelligence Response Team
U.S.	Fidelity Intelligence Operations CERT
U.S.	JPMC-GCS: (JPMorgan Chase Global Cyber Security)
U.S.	Morgan Stanley CERT
U.S.	PayPal GSIRT
U.S.	US Bank CSIRT
U.S.	Wells Fargo Security Operation Center

APPENDIX C: SECTOR-SPECIFIC STATEMENTS BY U.S. GOVERNMENT

Election-specific: On July 31, 2018, then U.S. secretary of homeland security Kirstjen Nielsen issued the following sector-specific declaratory statement:

> Let me be clear in this, ANY attempt to interfere in our elections is a direct attack on our democracy, it is unacceptable, and it will not be tolerated. Mark my words: America will not tolerate this meddling. . . . Let me also again take this opportunity today to issue a warning, as I have in other speeches, to any foreign power that would consider meddling in our networks or in the affairs of our democracy: The United States will no longer tolerate your interference. You will be exposed. And, you will pay a high price.[484]

Health sector-specific: On April 17, 2020, U.S. Secretary of State Mike Pompeo issued the following sector-specific warning:

> Malicious cyber activity that impairs the ability of hospitals and healthcare systems to deliver critical services could have deadly results. Anyone that engages in such an action should expect consequences. We call upon the actor in question to refrain from carrying out disruptive malicious cyber activity against the Czech Republic's healthcare system or similar infrastructure elsewhere. We also call upon all states not to turn a blind eye to criminal or other organizations carrying out such activity from their territory.
>
> The United States has zero tolerance for malicious cyber activity designed to undermine U.S. and international partners' efforts to protect, assist, and inform the public during this global pandemic. Such activity against critical civilian infrastructure is deeply irresponsible and dangerous. The United States promotes a framework of responsible state behavior in cyberspace, including nonbinding norms regarding states refraining from cyber activities that intentionally damage critical infrastructure and knowingly allowing their territory to be used for malicious cyber activities. When states do not abide by this framework, we hold them accountable.[485]

Health sector-specific: In May 2020, the United States joined Australia, the Czech Republic, Estonia, Japan, and Kazakhstan in proposing that the OEWG report reflect that:

> The OEWG developed its report in the context of the COVID-19 pandemic. In these circumstances, the OEWG underscored that all states considered medical services and medical facilities to be critical infrastructure for the purposes of norms (f) and (g) . . . In providing guidance for the implementation of these norms, States should note that highlighting particular sectors as critical infrastructure is not intended to be an exhaustive list and does not impact on the national designation, or not, of any other sector, nor does it implicitly condone malicious activity against a category not specified.[486]

APPENDIX D: BIPARTISAN LETTER FROM U.S. CONGRESSMEN

Congress of the United States
Washington, DC 20515

November 5, 2018

The Honorable Mike Pompeo
Secretary
U.S. Department of State
2201 C Street, N.W.
Washington, DC 20520

Dear Mr. Secretary:

We write to urge you to work with your fellow ministers at the upcoming 2019 G20 Finance Ministers and Central Bank Governors' meeting in Japan to issue a declaratory statement to protect the financial system in the face of growing cyber threats. The United States is the center of the global financial system, which depends upon trust to properly function. As you know, increasing malicious cyber activity threatens this important system. We must work even more diligently and efficiently to protect consumers, companies, and markets from these new threats.

While malicious cyber activity is not new, this threat has evolved in recent years from traditional criminals to include more state-sponsored activity, such as Iranian hackers targeting U.S. financial institutions and North Korea's cyber theft of more than $80 million from Bangladesh's account at the Federal Reserve Bank in New York. These attacks have highlighted cybersecurity weaknesses in some of the core systems underlying global financial markets, and – as we learned in the 2008 global financial crisis – vulnerabilities in one country's financial system can quickly affect the stability of others.

In order to protect our national and economic security against these threats, we believe that the United States should work with other G20 nations to develop specific declaratory language condemning malicious cyber activity and calling for partner governments and private sector institutions to facilitate better international cooperation on this issue. Such a statement would be consistent with America's efforts to advance international norms of responsible state behavior in cyberspace, including a commitment that countries not engage in cyber-enabled activity that damages or otherwise impairs the use of critical infrastructure services to the public.

We thank you for your attention to this issue, and we look forward to working with you to support our nation's economic and cyber security.

Sincerely,

EDWARD R. ROYCE
Member of Congress

JAMES R. LANGEVIN
Member of Congress

CC: The Honorable Steven T. Mnuchin, Secretary of the Treasury

PRINTED ON RECYCLED PAPER

156

Congress of the United States
Washington, DC 20515

November 5, 2018

The Honorable Steven T. Mnuchin
Secretary
U.S. Department of the Treasury
1500 Pennsylvania Avenue, N.W.
Washington, DC 20220

Dear Mr. Secretary:

We write to urge you to work with your fellow ministers at the upcoming 2019 G20 Finance Ministers and Central Bank Governors' meeting in Japan to issue a declaratory statement to protect the financial system in the face of growing cyber threats. The United States is the center of the global financial system, which depends upon trust to properly function. As you know, increasing malicious cyber activity threatens this important system. We must work even more diligently and efficiently to protect consumers, companies, and markets from these new threats.

While malicious cyber activity is not new, this threat has evolved in recent years from traditional criminals to include more state-sponsored activity, such as Iranian hackers targeting U.S. financial institutions and North Korea's cyber theft of more than $80 million from Bangladesh's account at the Federal Reserve Bank in New York. These attacks have highlighted cybersecurity weaknesses in some of the core systems underlying global financial markets, and – as we learned in the 2008 global financial crisis – vulnerabilities in one country's financial system can quickly affect the stability of others.

In order to protect our national and economic security against these threats, we believe that the United States should work with other G20 nations to develop specific declaratory language condemning malicious cyber activity and calling for partner governments and private sector institutions to facilitate better international cooperation on this issue. Such a statement would be consistent with America's efforts to advance international norms of responsible state behavior in cyberspace, including a commitment that countries not engage in cyber-enabled activity that damages or otherwise impairs the use of critical infrastructure services to the public.

We thank you for your attention to this issue, and we look forward to working with you to support our nation's economic and cyber security.

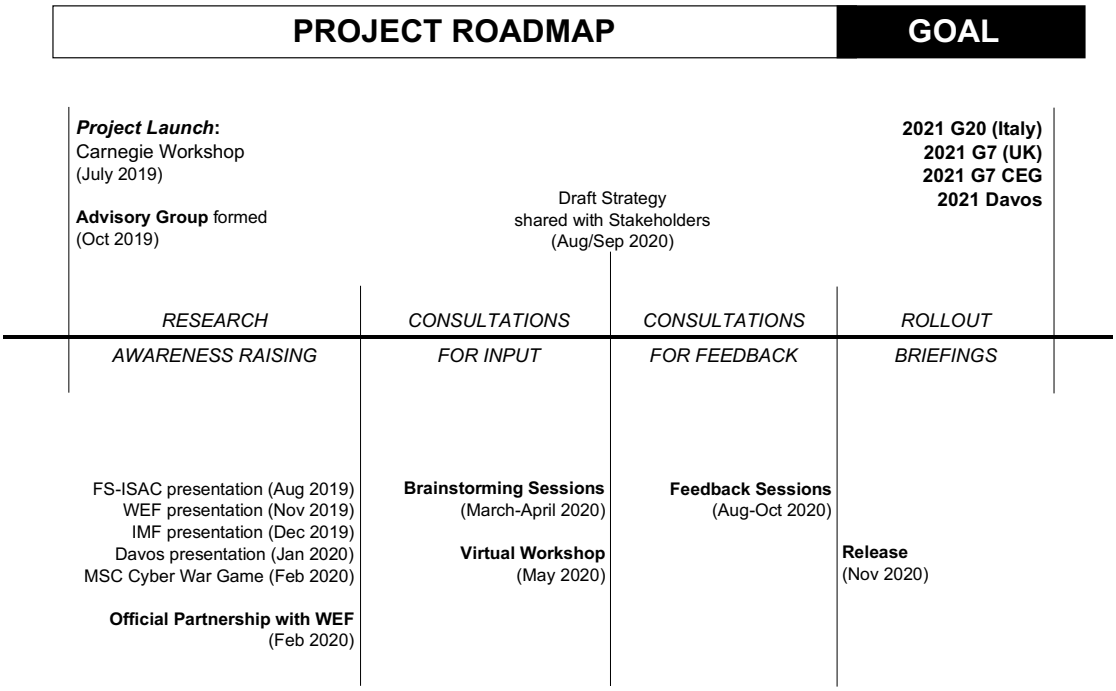
Sincerely,

EDWARD R. ROYCE
Member of Congress

JAMES R. LANGEVIN
Member of Congress

CC: The Honorable Mike Pompeo, Secretary of State

APPENDIX E:
PROJECT ROADMAP



APPENDIX F:
ADVISORY GROUP

CATEGORY		NAME	AFFILIATION
Government	1	**Lyndon Nelson**, Co-chair of G7 Cyber Experts Group	Bank of England
	2	**Paolo Ciocca**, Commissioner of CONSOB	CONSOB, Italy
	3	**Art Lindo**, Deputy Director, Division of Supervision and Regulation	Federal Reserve Board, United States
	4	**Tobias Feakin**, Ambassador for Cyber Affairs and Critical Technology	Department of Foreign Affairs and Trade, Australia
	5	**Yeow Seng Tan**, Chief Cyber Security Officer	MAS, Singapore
	6	**Jon Fanzun**, Special Envoy for Cyber Foreign and Security Policy	Federal Department of Foreign Affairs, Switzerland
Industry	7	**Cheri McGuire**, (former) Chief Information Security Officer	Standard Chartered
	8	**Cameron "Buck" Rogers**, Global Head of Resilience Advisory Function	HSBC
	9	**Natasha de Teran**, (former) Head of Corporate Affairs	SWIFT
	10	**Rahul Prabhakar**, Principal, Security Assurance	Amazon Web Services
	11	**Valerie Abend**, Managing Director, Global Financial Services Cybersecurity and Global Cyber Regulatory Practices	Accenture
	12	**Marc Radice**, Head of International Affairs	Zurich Insurance Group
	13	**Jason Witty**, Global Chief Information Security Officer	JPMorgan Chase
	14	**Mark Morrison**, Chief Information Security Officer (and chair of the cybersecurity working group of the World Federation of Exchanges)	Options Clearing Corporation
	15	**Sultan Meghji**, Co-founder and CEO	Neocova
	16	**Ramy Houssaini**, Global Chief Cyber and Technology Risk Officer and Group Data Protection Officer	BNP Paribas
Other	17	**Jennifer Elliott**, Division Chief, Technical Assistance Strategy, Monetary and Capital Markets	IMF
	18	**Belisario Contreras**, Manager, Cyber Security Programme	OAS
	19	**Steven Silberstein**, CEO	FS-ISAC
	20	**Alois Zwinggi**, Member of the Managing Board, Head of the Centre for Cybersecurity	World Economic Forum
	21	**Boris Ruge**, Ambassador and Vice-Chairman	Munich Security Conference
	22	**Dmitri Alperovitch**, Co-founder and (former) Chief Technology Officer	CrowdStrike
	23	**Lisa Monaco**, Distinguished Senior Fellow	NYU School of Law, Reiss Center on Law and Security
	24	**Juan Zarate**, Chairman and Co-founder	Financial Integrity Network

APPENDIX G: STAKEHOLDER ENGAGEMENTS

Carnegie hosted a series of stakeholder engagements for this project in addition to briefings to various associations, regulatory bodies, and other interested stakeholders, including:

Governments, Central Banks, and Financial Authorities

Australian Government Department of Foreign Affairs and Trade
Australian Prudential Regulation Authority
Bank of Canada
Bank of England
Bank of France
Bank of Italy
Bank of Japan
Bank of Kenya
Bank of Spain
Canadian Office of the Superintendent of Financial Institutions
Chilean Computer Security Incident Response Team
CONSOB, Italy
Cyber Security Agency of Singapore
Department of Finance Canada
Deutsche Bundesbank
Dutch Central Bank (DNB)
Dutch Ministry of Foreign Affairs
Estonian Ministry of Foreign Affairs
Federal Reserve Bank of New York
French Ministry for the Economy and Finance
French Ministry of Europe and Foreign Affairs
German Ministry of Finance
HM Treasury (UK)
Israeli Ministry of Finance
Italian Ministry of Economy and Finance
Japanese Financial Services Agency
MELANI, Swiss Federal Intelligence Service
Mexican Ministry of Foreign Affairs

Mexican National Banking and Securities Commission
Monetary Authority of Singapore
National Bank of Georgia
National Security Research Institute, Republic of Korea
New York State Department of Financial Services
New Zealand Ministry of Foreign Affairs and Trade
Philippine Central Bank
Reserve Bank of Australia
Swiss Federal Department of Foreign Affairs
U.S. Cyberspace Solarium Commission
U.S. Department of Homeland Security
U.S. Department of Labor
U.S. Department of the Treasury
U.S. Federal Reserve Board
U.S. National Institute of Standards and Technology
U.S. Public Company Accounting Oversight Board
U.S. Secret Service
U.S. Securities and Exchange Commission
U.S. State Department
UK Financial Conduct Authority
UK National Cyber Security Centre

Multilateral Organizations

Bank for International Settlements
Basel Committee on Banking Supervision
Committee on Payments and Market Infrastructures
European Central Bank
European Commission
European External Action Service
Europol
Financial Stability Board
Financial Stability Institute
Inter-American Development Bank
International Association of Insurance Supervisors
International Monetary Fund
International Organization of Securities Commissions
Office of the UN Secretary-General's Special Advocate for Inclusive Finance

Organization of American States
UN Institute for Disarmament Research
UN Office for Disarmament Affairs
World Bank

Financial Services Industry

AIG
American Express
Arab Bank
Asia Securities Industry & Financial Markets Association
Association for Financial Markets in Europe
Bank of America
Bank Policy Institute
Barclays
BNP Paribas
Business Round Table
Capital One
Citigroup
CME Group
Commerzbank
Commonwealth Bank of Australia
Cyber Defence Alliance
Cyber Risk Institute
European Banking Federation
Financial Integrity Network
Financial Services Sector Coordinating Council
Financial Systemic Analysis and Resilience Center
FS-ISAC
Geneva Association
Global Financial Markets Association
Goldman Sachs
HSBC
Institute of International Finance
Intesa Sanpaolo
JPMorgan Chase
Julius Baer
Mastercard
Mitsubishi UFJ Financial Group

Morgan Stanley
MUFG Union Bank
Options Clearing Corporation
PayPal
PricewaterhouseCoopers
Prudential
Santander Bank
Securities Industry & Financial Markets Association
Standard Chartered
State Street
SWIFT
SWIFT Institute
UBS Group
Union Bank of India
US Bank
Visa
World Federation of Exchanges
Zurich Insurance Group

Other Industry Stakeholders

Accenture
Amazon Web Services
BAE Systems
Cambridge Quantum Computing
CrowdStrike
CyberVista
Facebook
iQ4
Manifold Technology
Microsoft
Neocova
Serianu
Steptoe & Johnson
Twitter
WhatsApp

Other Organizations

Albright Stonebridge Group
Alliance for Financial Inclusion
Aspen Institute
AustCyber
Better Than Cash Alliance
Bill & Melinda Gates Foundation
Center for Strategic and International Studies
Chertoff Group
Consultative Group to Assist the Poor
Cyber Threat Alliance
CyberPeace Institute
Cybersecurity Talent Initiative
Forum of Incident Response and Security Teams
Global Cyber Alliance
Global Forum on Cyber Expertise
International Committee of the Red Cross
Munich Security Conference
Suricate Solutions
Third Way

Academia

Centre for Intellectual Property and Information Technology Law
Columbia University
George Mason University
Georgetown University
Harvard University
Korea University School of Law
Seoul National University of Science and Technology
Temple University
U.S. Military Academy
University of Oxford

APPENDIX H: COMPENDIUM OF ACTORS

African Forum on Cybercrime: The African Forum on Cybercrime, convened by the African Union and first hosted in 2018, is an organization effort for African countries to facilitate international cooperation to fight against cyber crime and strengthen law enforcement authorities in Africa through capacity-building. The African Forum receives support from the Council of Europe, the European Union, INTERPOL, the UN Office on Drugs and Crime (UNODC), and others.[487]

Alliance for Financial Inclusion (AFI): Founded by the Bill & Melinda Gates Foundation in 2008, the AFI is an advocacy and policy organization for financial inclusion, whose members are central banks and financial regulatory institutions.[488] The AFI organizes the annual Global Policy Forums. In 2017, the AFI held a policy forum for cybersecurity and financial inclusion in Malaysia, in partnership with Bank Negara Malaysia.[489] In November 2019, the AFI published "Cybersecurity for Financial Inclusion: Framework and Risk Guide," which provides key principles and best practices to assist regulatory and supervisory authorities dealing with cybersecurity risk in the financial sector.[490]

Asia Securities Industry and Financial Markets Association (ASIFMA): ASIFMA is a financial industry trade association that represents financial institutions in Asia, particularly with the Monetary Authority of Singapore (MAS) and the Hong Kong Monetary Authority (HKMA).[491]

Association for Financial Markets in Europe (AFME): AFME is a financial industry trade association that represents financial institutions in Europe. AFME advocates for cybersecurity regulatory harmonization across the European Union.[492]

Association for South East Asian Nations (ASEAN) Regional Forum (ARF): The ARF is a forum consisting of ten countries from southeast Asia that is dedicated to regional stability and economic cooperation. The ARF has focused on cybersecurity capacity-building and confidence-building measures at a regional level, especially after the UN Group of Governmental Experts (UN GGE) failed to reach consensus in 2017. Countering transnational cyber crime was a core focus of the twentieth ARF in 2019.[493]

(Australia) AustCyber: Australia's federal government established a non-profit organization, AustCyber, to cultivate an Australian cybersecurity ecosystem,[494] including building a pipeline for cybersecurity talent.

(Australia) Australian Cyber Security Centre (ACSC): The ACSC is the Australian government's lead body on national cybersecurity issues, housed under the Australian Signals Directorate.[495]

(Australia) Australian Prudential Regulatory Authority (APRA): APRA is an independent authority that supervises financial institutions and promotes financial system stability in Australia. In July 2019, APRA implemented a new information security guidance for financial institutions, "Prudential Practice Guide CPG 234 Information Security."[496]

(Australia) Australian Transaction Reports and Analysis Centre (AUSTRAC): AUSTRAC is Australia's financial intelligence unit and has been involved in international cyber crime investigations with like-minded allies.[497]

(Australia) Council of Financial Regulators (CFR): The CFR is the coordinating body for Australia's main financial regulatory agencies. In 2020, the CFR noted that "cyber risk is consistently ranked among the top risks to the Australian financial system."[498]

(Australia) Fintel Alliance: The Fintel Alliance is a public-private partnership comprised of twenty-two public and private sector organizations, led by the Australian Transaction Reports and Analysis Centre (AUSTRAC), Australia's national financial intelligence unit (FIU).[499] The public-private partnership focuses primarily on domestic crime and works with ReportCyber to counter financial cyber crime.

(Australia) Reserve Bank of Australia (RBA): As Australia's central bank, the RBA is tasked with maintaining financial stability. In its 2018 "Financial Stability Review," the RBA recognized that "cyber security will be a core challenge for the financial system for years to come."[500]

Bank for International Settlements (BIS): The BIS, the international organization of central banks, helps its members manage cyber risk and build resilience through key regulator stocktakes,[501] convenings,[502] consultations, and guidance.[503] Most recently, the BIS established the Cyber Resilience Coordination Centre (CRCC) as part of its Innovation BIS 2025 strategy to facilitate collaboration on cyber resilience within the central bank community.[504]

Better Than Cash Alliance (BTCA): The BTCA is a global partnership administered by the UN Capital Development Fund (UNCDF) that supports

governments, companies, and international organizations involved in the transition from cash to digital payments.[505] The BTCA has created a series of toolkits for businesses, governments, and development partners and another series related to ecosystem diagnostics, payment measurements, and accelerators.[506]

Bill & Melinda Gates Foundation: Since 2010, the Gates Foundation has given over $350 million in grants to support its Financial Services for the Poor strategy, which promotes the development of digital payment systems, the advancement of gender equality, and the creation of national and regional financial inclusion strategies.[507] The foundation invests in national financial inclusion initiatives in Africa, South Asia, and Southeast Asia.[508]

(Canada) Bank of Canada: As Canada's central bank, the Bank of Canada is tasked with ensuring financial stability. The bank's "2019–2021 Cyber Security Strategy" assumes that cyber breaches are inevitable and outlines strategic actions to "enhance the cyber resilience of the Canadian financial system."[509] The Bank of Canada contributed to a 2016 report from the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO): "Guidance on Cyber Resilience for Financial Market Infrastructures." The bank also participates in the G7 Finance Track Cyber Expert Group (CEG).[510]

Charter of Trust: At the 2018 Munich Security Conference, a group of CEOs of major multinational companies, led by Siemens, launched the Charter of Trust. This charter aims to develop standards to ensure greater digital security and integrity in both the public and private sectors. The Charter of Trust has three primary goals: to protect the data of individuals and businesses; to prevent harm to people, businesses, and infrastructure; and to establish a reliable basis to ensure confidence in digital assets.[511]

(China) Cyberspace Administration of China (CAC): The CAC is the central agency for cybersecurity oversight and data governance in China. However, cybersecurity governance in China is rapidly evolving and there is some ambiguity about who, between China's financial regulators and the CAC, holds ultimate authority over cybersecurity supervision of financial institutions.[512]

(China) China Banking and Insurance Regulatory Commission (CBIRC): CBIRC was established in 2018 when the China Banking Regulatory Commission and the China Insurance Regulatory Commission merged. CBIRC's Statistics, IT and Risk Surveillance Department is responsible for "information security, as well as information technology risk supervision of banking and insurance institutions."[513] CBIRC also oversees the "Guidelines on the Risk Management

of Commercial Banks' Information Technology," published in 2009 under the CBRC.[514]

(China) People's Bank of China (PBOC): PBOC is China's central bank. It works closely with the Cyberspace Administration of China (CAC) and financial authorities to develop cybersecurity requirements for financial institutions. In February 2020, PBOC issued the "Personal Financial Information Protection Technical Specification," a comprehensive guidance on handling financial data.[515]

Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO): The CPMI and IOSCO work closely together on cybersecurity issues but are two separate organizations. The CPMI, housed within the Bank for International Settlements (BIS), is a global standard setter for payment, clearing, and settlement in the financial system, and a forum for central bank cooperation on such functions. IOSCO is an international body for financial authorities that regulate securities and futures markets markets and is recognized as the global standard setter for the securities sector.[516] In June 2016, CPMI-IOSCO released their joint "Guidance on Cyber Resilience for Financial Market Infrastructures," which is regarded as the first internationally agreed upon guidance on cybersecurity for the financial industry.[517]

Consultative Group to Assist the Poor (CGAP): CGAP, an independent think tank focused on financial inclusion, housed at and administered by the World Bank, has developed a concept for regional cyber security resource centers to help low-income countries to address cybersecurity risks in digital financial services.[518] In November 2019, CGAP published "Cyber Security in Financial Sector Development: Challenges and Potential Solutions for Financial Inclusion."

CyberPeace Institute (CPI): The CPI was launched by Microsoft, Mastercard, the William & Flora Hewlett Foundation, and others in 2019 to reduce the "frequency, impact and scale" of cyber attacks on civilians and critical infrastructure. It focuses on attribution, advancement of international norms, and capacity-building. The CPI is based in Geneva, Switzerland.

Cyber Risk Institute (CRI): The CRI is a newly created private sector organization that maintains the Financial Services Sector Cybersecurity Profile. The CRI is affiliated with the Bank Policy Institute.

Cybersecurity Tech Accord: In April 2018, a group of companies led by Microsoft announced the Cybersecurity Tech Accord, a public commitment

by multinational tech companies to protect and empower civilians online and improve the stability of cyberspace. Forty-four companies—including Cisco, Facebook, HP, Microsoft, Nokia, Oracle, and Trend Micro—have agreed to defend all customers, regardless of country, against malicious cyber attacks by state and nonstate actors.[519]

Cyber Threat Alliance (CTA): The CTA is a nonprofit organization that serves as a platform for information sharing among companies and organizations. CTA members are primarily cybersecurity service providers; the CTA is a partner with FS-ISAC.

Digital Financial Services (DFS) Observatory: The DFS Observatory, based at Columbia University, is currently developing a cybersecurity framework for digital financial services. It holds a curated library of DFS-related laws, regulations and policies.[520]

Digital Geneva Convention: After many years of engaging in international cybersecurity policy discussions, in 2017 Microsoft President Brad Smith stepped up Microsoft's engagement by publicly calling for a Digital Geneva Convention. The multistakeholder initiative called for nation-states to refrain from launching cyber attacks on industry, national critical infrastructure, and intellectual property. Additionally, the proposal encouraged the tech sector to adopt shared principles, such as consumer protection and political neutrality. Microsoft also proposed establishing a nongovernmental global cyber attribution organization to independently investigate systemically important cyber incidents.[521]

(EU) Cyber Information and Intelligence Sharing Initiative (CIISI-EU): In February 2020, the European Union Agency for Cybersecurity (ENISA), the European Cybercrime Centre (EC3), and the Euro Cyber Resilience Board within the ECB established the CIISI-EU, with the aim of "bringing central banks, clearing houses, stock exchanges, and payment system providers together in order to share expertise with the purpose of protecting the European financial system from cyberattacks."[522]

(EU) EU Law Enforcement Emergency Response Protocol: In March 2019, in response to WannaCry and NotPetya, the Council of Europe adopted the EU Law Enforcement Emergency Response Protocol, which clarified roles and responsibilities, and communication procedures for EU law enforcement. In the fall of 2019, the European Union Agency for Cybersecurity (ENISA) and the European Cybercrime Centre (EC3) organized CyLEEx19, a cyber law enforcement exercise, to test the EU Law Enforcement Emergency Response Protocol. The exercise brought together cyber crime investigators and experts

from the public and private sectors and simulated ransomware attack on the EU's financial sector.[523]

(EU) European Banking Authority (EBA): In late 2019, the EBA published its "Guidelines on ICT and Security Risk Management," to go into full force in June 2020.[524] Among other things, these guidelines call for firms to conduct "business impact analysis by analyzing their exposure to severe business disruptions."[525] In February 2019, the EBA also published its outsourcing guidelines.[526]

(EU) European Banking Federation (EBF): EBF is a financial industry trade association that represents financial institutions in Europe. EBF represents the interests of financial institutions when negotiating cybersecurity regulation with European authorities like the European Banking Authority (EBA), the European Union Agency for Cybersecurity (ENISA), the European Central Bank, and the European Commission.[527]

(EU) European Central Bank (ECB): As the eurozone's central bank, the ECB is focused on maintaining the cyber resilience of its members' financial system. In 2020, the ECB established the Euro Cyber Resilience Board (ECRB) for pan-European Financial Infrastructures, a forum for senior officials to advance cyber resilience policy. In 2019, the ECB published the Cyber Resilience Oversight Expectations (CROE), which provides guidance to FMIs and supervisors about cyber resilience expectations. Additionally, they published the TIBER-EU, a penetration testing framework. The ECB also hosts UNITAS, a cybersecurity exercise that tests the resilience of crisis communications between supervisors and firms.

(EU) European Commission (EC): The EC, which functions as the executive branch of the European Union, has helped coordinate European supervisory authorities to focus on cyber risk in the financial system. Recently, in December 2019, the EC launched a consultation, "Digital Operational Resilience Framework for Financial Services: Making the EU Financial Sector More Secure."[528]

(EU) European Union Agency for Cybersecurity (ENISA): ENISA was established in 2004 with the aim of strengthening cybersecurity expertise, policy, and capacity across the European Union. ENISA works closely with the European Cybercrime Centre (EC3) and was one of the founding members of the European Financial Institutes—Information Sharing and Analysis Centre (European FI-ISAC).[529]

(EU) Europol Cybercrime Centre (EC3): EC3 is the primary law enforcement unit within Europol to combat cyber crime. EC3 coordinates an Advisory Group on Financial Services that brings together experts from major financial institutions to provide private sector insight into the fight against cyber crime in Europe. The advisory group played a supporting role in the arrest of a leader of the Carbanak/Cobalt cyber crime group.[530]

(EU) Global Action on Cybercrime Extended (GLACY+): GLACY+ is a joint effort of the EU and the Council of Europe to build up capacity to combat cyber crime in fifteen priority and hub countries in Africa, Asia-Pacific, Latin America, and the Carribean region.[531]

Financial Action Task Force (FATF): The FATF was created in 1989 through the G7, initially focusing on anti-money laundering and eventually expanding its activities to also focus on combating terrorist financing and nuclear proliferation. After some initial work on virtual currencies in 2014, and following growing concerns about this topic throughout 2017 and 2018, FATF has also become more involved in the debate about the governance of cryptocurrencies.[532]

Financial Services Information Sharing and Analysis Centre (FS-ISAC): FS-ISAC is a nonprofit industry consortium dedicated to cybersecurity information sharing across the global financial system. Over the past two decades, FS-ISAC's membership has grown to nearly 7,000 members in over seventy jurisdictions.[533] It now operates three hubs: the Americas hub in the United States; the Europe, Middle East, and Africa (EMEA) hub in London; and the Asia-Pacific hub in Singapore. In addition to information sharing, FS-ISAC also acts as an international convener and hosts cybersecurity exercises.

Financial Stability Board (FSB): The FSB (formerly the Financial Stability Forum) was established in 2009 by the G20 following the 2008 global recession and is hosted and funded by the Bank for International Settlements (BIS). In 2017, the G20 tasked the FSB with taking stock of approaches on cybersecurity and the financial system.[534] The FSB also published a cyber lexicon to promote a common language in the industry.[535]

Financial Stability Institute (FSI): The FSI was jointly established in 1998 by the Bank for International Settlements (BIS) and the Basel Committee on Banking Supervision (BCBS). Its mandate is to assist supervisors around the world in improving and strengthening their financial systems. The FSI produces research on cybersecurity and resilience through policy briefs, crisis exercises, and papers on best practices.

FINCA International: FINCA is an international charity that promotes financial inclusion through a network of community-based microfinance institutions that provide loans, savings accounts, insurance, and money transfers to individuals and groups in Africa, Eurasia, Latin America, the Middle East, and South Asia.[536] FINCA has made leveraging fintech to support its microfinance and social enterprise efforts a priority, and it partners with technology companies and financial institutions around the globe to integrate digital technologies into their products and services.[537]

Forum of Incident Response and Security Teams (FIRST): FIRST is a global coordinating body for CSIRTs and CERTs, including FinCERTs.[538]

(France) Bank of France: The central bank of France is an active participant in the G7 Finance Track Cyber Group of Experts. The Bank of France hosted the G7 Cyber Expert Group in 2019 and facilitated a cybersecurity exercise.[539] In November 2019, the central bank signed a memorandum of understanding with the Monetary Authority of Singapore (MAS) to enhance cooperation in cybersecurity.[540]

(France) Prudential Supervision and Resolution Authority (ACPR): The ACPR is a supervisor of financial institutions in France. In 2013, the ACPR published "ACPR Guidance: The Risks Associated With Cloud Computing."[541]

G7 24/7 Cybercrime Network: The 24/7 Network, made up of seventy nations, established points of contact for responding to government requests regarding cyber crime cases. It was established in 1997 by the G8 Justice and Interior Ministers to provide "timely, effective response to transnational high-tech cases."[542]

G7 Cyber Expert Group (CEG): The G7 CEG was established by the G7 Finance Ministers and Central Bank Governors in 2015 to identify the core cybersecurity risks to the financial system. The group has released a series of best practices and recommendations since 2016.[543]

G7 Deauville Partnership Action Plan for Financial Inclusion: The G8 launched the Deauville Partnership in 2011 to support democratic transitions in the Arab world through economic and governance assistance.[544] In 2015, the "Deauville Partnership Action Plan for Financial Inclusion" outlined G7 priorities for advancing financial inclusion, one of which is the development of digital financial inclusion policies with adequate risk management measures.[545]

G7 Finance Ministers and Central Bank Governors: This forum is the lead mechanism to coordinate work in the G7 Finance Track.[546] Work is directed

through consensus communiqués. The ministers and governors established the G7 Cyber Expert Group in 2015.

G7 Ise-Shima Cyber Group: In 2016, the heads of state of the G7 created a new work stream through the G7 dedicated to international cybersecurity. This work stream led to the 2017 Lucca Declaration on Responsible State Behavior in Cyberspace, the most detailed outline by a group of Western states regarding their views for rules of the road for cyberspace.

G20 Finance Ministers and Central Bank Governors: This forum is the primary mechanism to coordinate work in the G20 Finance Track. In March 2017, G20 Finance Ministers and Central Bank Governors warned for the first time that cyber attacks could threaten financial stability and instructed the Financial Stability Board to investigate the risks.[547]

(Germany) Deutsche Bundesbank (Bundesbank): Germany's central bank is an active participant in the G7 Cyber Expert Group. In the 2018 "Financial Stability Review," the Bundesbank determined that an extreme cyber attack could "destabilise the entire [financial] system."[548]

(Germany) Federal Financial Supervisory Authority (BaFin): BaFin is a German financial regulator that supervises financial institutions. In 2018 BaFin published the "Supervisory Requirements for IT in Financial Institutions," which aims to create a comprehensive framework for management of IT resources in financial institutions.[549]

Global Cyber Alliance (GCA): The GCA is a nonprofit organization established in 2015 by the Center for Internet Security, the New York County district attorney, and the City of London police commissioner to "address systemic cyber risk" and build capacity to combat cyber crime. The GCA provides organizations with resources, toolkits, and accessible education to reduce cyber risk.[550]

Global Financial Markets Association (GFMA): The GFMA is a global financial industry trade association that represents the interests of multinational financial institutions and that engages in advocacy about cybersecurity regulations. It is the parent association of the Securities Industry and Financial Markets Association (SIFMA), the Asia Securities Industry and Financial Markets Association (ASIFMA), and the Association for Financial Markets in Europe (AFME). The GFMA advocates for global cybersecurity regulatory harmonization and is a leading industry voice on regulated penetration testing.[551]

Global Forum on Cyber Expertise (GFCE): The GFCE is a nonprofit coalition whose mission is "to strengthen cyber capacity and expertise globally through international collaboration and cooperation."[552] The GFCE is the primary coordinating platform for cyber capacity-building. Its focus is to coordinate cyber capacity projects, share knowledge and expertise by recommending tools and publications, and act as a clearing house to match needs for cyber capacities with offers of support.[553]

Global Partnership for Financial Inclusion (GPFI): In 2010, G20 leaders adopted the "G20 Principles for Innovative Financial Inclusion"[554] and launched the GPFI at the Seoul Summit. The GPFI is primarily tasked with implementing the G20 Financial Inclusion Action Plan (FIAP) through policy analysis and recommendations, with tracking G20 financial inclusion indicators, and with coordinating global financial inclusion efforts.[555]

GSMA: The GSMA is a major industry association representing mobile operators.[556] In 2019, it launched the Inclusive Tech Lab with the goal of promoting industry collaboration on technological solutions driving financial inclusion.[557] The lab works on openness and interoperability of payment systems, access to financial services by women and vulnerable populations, and digital identity.[558]

(Hong Kong) Hong Kong Monetary Authority (HKMA): The HKMA is the primary financial regulator for financial institutions in Hong Kong. In 2016, the HKMA published the "Enhanced Competency Framework on Cybersecurity" and launched the Cybersecurity Fortification Initiative, which includes a maturity assessment, an inherent risk assessment, and a penetration testing requirement.[559]

(India) Reserve Bank of India (RBI): The RBI is India's central bank and acts as the lead government body on cybersecurity in India's financial sector. The RBI works closely with India's national CERT (CERT-In), and the Institute for Development and Research in Banking Technology (IDRBT) to facilitate information sharing and issue alerts to Indian financial institutions.[560] Since issuing a circular on cybersecurity to banks in 2016, the RBI has become increasingly proactive on cybersecurity issues.[561] In 2019, the RBI centralized all regulatory and supervisory functions related to cyber risk within its Cyber Security and IT Risk Group in the Department of Supervision.

Institute of International Finance (IIF): The IIF is a global association of the finance industry based in Washington, DC. In April 2018, the IIF published the white paper, "Addressing Regulatory Fragmentation to Support a

Cyber-Resilient Global Financial Services Industry," that called for improved regulatory harmonization.[562]

International Criminal Police Organization (INTERPOL): INTERPOL is an international organization that coordinates international cooperation on crime, including financial cyber crime.[563] It operates the Cyber Fusion Centre which co-locates industry and law enforcement cyber experts to provide stakeholders with actionable threat intelligence. It also facilitates regular INTERPOL Regional Working Groups on Cybercrime.

International Finance Corporation (IFC): IFC works with approximately 800 financial institutions in over 100 countries to create and leverage markets to solve development challenges. With the support of the Mastercard Foundation, IFC has launched the Partnership for Financial Inclusion, a $37.4 million initiative to expand microfinance and DFS in sub-Saharan Africa.[564]

International Monetary Fund (IMF): The IMF oversees the international monetary and financial system and monitors the activities of its 189 member countries. In 2018, the IMF established a program to assist financial regulators and supervisors with cybersecurity risk management after it declared cybersecurity to be a financial stability risk.[565] The IMF's cybersecurity technical assistance program, implemented by the Monetary and Capital Markets Department, has three pillars: annual workshops, regional technical assistance center workshops, and bilateral technical assistance missions.[566]

International Telecommunications Union (ITU): In 2014, the ITU established a Focus Group on Digital Financial Services to convene telecom and financial service regulators, digital financial service providers, mobile network operators, and international organizations.[567] The group released twenty-eight position papers, including one on security aspects of digital financial services.[568] The ITU works with the World Bank, the Committee on Payments and Market Infrastructures (CPMI), and the Bill & Melinda Gates Foundation to administer the Financial Inclusion Global Initiative (see entry for World Bank below).

(Israel) Bank of Israel: In 2015, Israel's central bank issued a directive on Cyber Defense Management that outlines a cyber risk management framework for financial institutions.[569]

(Israel) Cyber and Finance Continuity Center (FC3): FC3 provides specialized cybersecurity capabilities to Israel's financial sector. FC3 was established after a cybersecurity exercise with the country's financial leadership revealed "a need for integration and 'translation' between the financial language, the

cyber and technology language and the risk management needs."[570] FC3 is co-owned and co-managed by the Israeli Ministry of Finance and the Israeli National Cyber Directorate, which provide expertise in the financial ecosystem and expertise in cyber and technology, respectively.

(Italy) Bank of Italy: The central bank of Italy is an active participant in the G7 Cyber Expert Group.[571] The bank also chairs Italy's CODISE, the body responsible for crisis management coordination in the Italian financial sector. In 2020, the Bank of Italy and CONSOB announced a joint "Strategy on Cyber Security for the Financial System," which aims to ensure the reliability of the financial system as a whole.[572]

(Italy) CONSOB: CONSOB is the regulator that oversees the Italian securities market. In 2020, the Bank of Italy and CONSOB announced their "Joint Strategy for the Cyber Security of the Financial Sector," which aims to ensure the reliability of the financial system as a whole.[573]

(Japan) Bank of Japan: Japan's central bank is an active participant in the G7 Cyber Expert Group. In 2020, the Bank of Japan warned its financial institutions that they were vulnerable to cyber attacks ahead of the Olympic Games.[574]

(Japan) Financial Services Agency (JFSA): The JFSA conducts supervision and inspection of cyber security management in Japanese financial institutions. In 2015, the JFSA published policy approaches that address cybersecurity for the financial sector.[575]

(Japan) Japan Cybercrime Control Center (JC3): The JC3 was established in 2014 as a nonprofit organization designed to "identify, mitigate, and neutralize the root of threats to cyberspace." It was modeled after the U.S. National Cyber-Forensics and Training Alliance (NCFTA).[576]

Joint Cybercrime Action Taskforce (J-CAT): J-CAT, launched in 2014 and based at EC3 headquarters, is a standing operational team of cyber liaison officers from around the world. There are sixteen member countries (nine EU members and seven non-EU countries). J-CAT focuses on countering transnational cyber crime and has conducted successful operations against cyber crime in the financial sector.[577]

(Netherlands) De Nederlandsche Bank (DNB): DNB, the central bank of the Netherlands, is best known in the financial cybersecurity community as the creator of the TIBER-NL framework for penetration testing.[578]

(Netherlands) National Cyber Security Centre (Dutch NCSC): The Dutch NCSC, founded in 2012, is an information center that facilitates public-private cooperation in the fight against cyber crime.[579]

(Netherlands) National High Tech Crime Unit (NHTCU): The NHTCU is an investigative unit within the Dutch Police Services Agency focused on combating cyber crime.[580] The NHTCU prioritizes investigating cyber attacks on vital infrastructure and the financial system.[581] It runs the Dutch Electronic Crimes Task Force, established in 2011 at the request of major Dutch banks.[582]

(Nigeria) Nigeria Electronic Fraud Forum (NeFF): NeFF is a consortium of public and private institutions established to exchange information and knowledge around fraud issues. Members include banks, mobile payment operators, payment system operators, national security and intelligence authorities, and the Central Bank of Nigeria.[583]

North Atlantic Treaty Organization (NATO): NATO recognizes cyberspace as a domain of military operations and has declared that a cyber attack could trigger an invocation of Article 5, the collective defence clause.[584] NATO operates the Cooperative Cyber Defence Centre of Excellence.[585] In 2018, NATO established a Cyberspace Operations Centre and has established Cyber Rapid Reaction teams to assist allies. NATO also cooperates with the private sector on cybersecurity through the NATO Industry Cyber Partnership.[586]

Organisation for Economic Co-operation and Development (OECD): The OECD has worked to promote consumer protection in financial inclusion efforts and national strategies for financial education. To this end, the OECD is an implementing partner of the Global Partnership for Financial Inclusion (GPFI) and has organized a Task Force on Financial Consumer Protection to implement the G20's "High-level Principles for Financial Consumer Protection," which were endorsed at the October 2011 G20 meeting.[587]

Organization for Security and Co-operation in Europe (OSCE): The OSCE is a security-focused organization comprised of fifty-seven member countries based in Europe, northern and central Asia, and North America. The OSCE wants to "operationalize pertinent UN guidance by [the GGE] on the regional level."[588] Like the ASEAN Regional Forum (ARF), the OSCE has been focused on cybersecurity capacity-building and confidence-building measures at a regional level, especially after the UN Group of Governmental Experts (UN GGE) failed to reach consensus in 2017.

Organization of American States (OAS): The OAS focuses on cooperation in South America and Latin America. It focuses on cybersecurity

confidence-building measures and increasing trust among states through a variety of transparency, cooperation, and stability measures that reinforce and complement the discussions at the UN Group of Governmental Experts (UN GGE). OAS also facilitates the Inter-American Cooperation Portal on Cyber-Crime and the Cyber-Crime Working Group, which aim to strengthen Western hemispheric cooperation on combating cyber crimes.[589]

Paris Call for Trust and Security in Cyberspace (Paris Call): In November 2018, French President Emmanuel Macron announced the Paris Call for Trust and Security in Cyberspace, a high-level declaration of principles for promoting an open, secure, accessible, and peaceful cyberspace. These principles supported the applicability of international law and the UN Charter to cyberspace as well as affirming the UN norms efforts. Sixty-six states, 139 international and civil society organizations, and 347 private sector entities have signed on, although the United States has not joined.[590] Interestingly, this initiative grew out of outreach from the private sector, when Microsoft sought French support for its Cybersecurity Tech Accord and the French government took the opportunity to lead in this space.

(Russia) Central Bank of the Russian Federation (CBR): In 2019, the CBR outlined its near-term approach to cybersecurity for the financial system in the "Guidelines for the Advancement of Information Security in the Financial Sector for 2019–2021."[591] The CBR acknowledges that "the rise in cyber crime, primarily in the credit and financial sector, is a global trend that requires coordinated efforts by regulators, law enforcement agencies, credit and financial institutions and financial service consumers," and goes on to note that "cyber attacks on digital financial systems can provoke a financial crisis."[592] CBR also operates Russia's FinCERT.[593] CBR published "Maintenance of Information Security of the Russian Banking System Organisations" in June 2014.[594]

SANS Institute: SANS runs the SANS Cyber Workforce Academy, a three- to four-month, scholarship-based training program for those seeking to enter the cybersecurity workforce. SANS has run a Chicago program, and is currently accepting applications for a Maryland program supported by the Maryland Department of Labor.[595] SANS also ran the Cyber Retraining Academy for the British government, which provided an immersive ten-week training program for individuals seeking to enter cybersecurity professions. (The Cyber Retraining Academy website has not been updated since 2017.)[596]

Securities Industry and Financial Markets Association (SIFMA): SIFMA is a financial industry trade association that represents U.S. financial institutions. Among other advocacy work, SIFMA coordinates the global Quantum Dawn cybersecurity exercises.[597]

Shanghai Cooperation Organisation (SCO): In 2009, the SCO, with Russia and China taking the lead, released its "Agreement on Cooperation in Ensuring International Information Security." Two years later, four members of the SCO submitted a draft International Code of Conduct for Information Security to the UN General Assembly. This group of four was expanded to six members and introduced a revised draft code to the UN in 2015. Russia's resolution to establish the UN Open-Ended Working Group (OEWG) draws from language within the SCO's International Code of Conduct for Information Security.[598]

(Singapore) Cyber Security Agency of Singapore (CSA): Singapore's CSA was formed in 2015 to provide dedicated and centralised oversight of national cybersecurity functions. The CSA works with the Monetary Authority of Singapore (MAS) to protect the financial sector, one of the nation's Critical Information Infrastructure Sectors. The CSA also engages with various industries and stakeholders to heighten cybersecurity awareness as well as to ensure the holistic development of Singapore's cybersecurity landscape. It is part of the Prime Minister's office and is managed by the Ministry of Communications and Information.[599]

(Singapore) Monetary Authority of Singapore (MAS): The MAS, as Singapore's primary financial regulator, leads work on cybersecurity and operational resilience in the financial sector. The MAS has become a thought leader in building cyber resilience internationally. For example, the MAS served as co-chair in developing the Committee on Payments and Market Infrastructures-International Organization of Securities Commission's (CPMI-IOSCO) principles, one of the earliest international efforts focused on operational resilience.[600] In March 2019, the MAS proposed changes to their Business Continuity Management (BCM) Guidelines, citing concerns about the increase in the scale and frequency of cyber attacks.[601]

Society for Worldwide Interbank Financial Telecommunication (SWIFT): SWIFT provides a standardized messaging network that allows financial institutions to facilitate financial transactions. SWIFT is a cooperative society under Belgian law and is owned and controlled by its shareholders. Following the 2016 Bangladesh incident, SWIFT updated its Customer Security Program to include cybersecurity standards for its clients in its contractual relationships.[602]

(South Africa) South African Banking Risk Information Centre (SABRIC): SABRIC is a nonprofit set up by South Africa's four major banks to coordinate interbank activities to address organized financial cyber crime. SABRIC serves the more than twenty members of the banking and payments sector in South Africa, and it serves as a conduit between the private sector and regulators.

SABRIC also leads public education programs to improve digital and cybersecurity literacy.

(South Korea) Cyber Bureau, National Police Agency: The South Korean National Police Agency established its Cyber Bureau in 2014, partially in response to a massive breach of credit card data that affected 20 million South Koreans.[603]

(South Korea) Cybercrime Investigation Division: The Cybercrime Investigation Division exists within the National Digital Forensics Center of the Supreme Prosecutors' Office of South Korea.[604]

(South Korea) Financial Security Institute (FSI): The Financial Security Institute was established by the South Korean government in 2015 to protect their financial sector.[605] FSI's CERT, known as FSI-CERT, is a member of the Forum of Incident Response and Security Teams (FIRST).

Task Force on Computer Security Incident Response Teams (TF-CSIRT): TF-CSIRT is a global coordinating body for CSIRTs and CERTs, including FinCERTs. TF-CSIRT works closely with the European Union Agency for Cybersecurity (ENISA) to help coordinate European CSIRTs and CERTs.[606]

(UK) Bank of England (BoE): The BoE, the United Kingdom's central bank, is a global thought leader in cyber resilience. It is one of the UK Financial Service Authorities (UK FSAs). In July 2018, the UK FSAs published a series of discussion papers, "Building the UK Financial Sector's Operational Resilience," that argued for shifting focus away from firms' ability to prevent disruptions and instead ensuring that individual firms and the financial sector had the ability to withstand disruptions, or "shocks."[607] The BoE also created CBEST, a penetration testing framework.[608]

(UK) Cyber Defence Alliance (CDA): CDA was established in 2015 by a small number of UK-based financial institutions as a nonprofit public-private partnership that works collaboratively across the financial sector and law enforcement.[609] In October 2018, the CDA signed a memorandum of understanding with Europol's European Cybercrime Centre (EC3) to formalize information sharing between the two organizations.[610]

(UK) Financial Conduct Authority (FCA): FCA is one of the UK Financial Service Authorities (UK FSAs), and one of the global thought leaders on cyber resilience. In July 2018, the UK FSAs published a series of discussion papers, "Building the UK Financial Sector's Operational Resilience."[611]

(UK) Financial Sector Cyber Collaboration Centre (FSCCC): Modeled after the Financial Systemic Analysis & Resilience Center (FSARC), FSCCC was established by UK Finance in 2017. FSCCC is comprised of twenty large banks and other financial institutions in collaboration with the United Kingdom's National Cyber Security Centre (NCSC), the UK's Financial Supervisory Authorities, and the UK's National Crime Agency.[612]

(UK) National Cyber Security Centre (NCSC): The NCSC was operationalized in 2016 under the UK Government Communications Headquarters (GCHQ) to provide cybersecurity advice to public and private institutions in the United Kingdom.[613] It facilitates public-private cooperation through the Financial Sector Cyber Collaboration Centre (FSCCC) and the Cyber Security Information Sharing Partnership, a "joint industry and government initiative set up to exchange cyber threat information sharing in real time."[614] The NCSC was established, in part, to address concerns from the Bank of England (BoE). Robert Hannigan, the former director of the GCHQ and the driving champion behind the NCSC's establishment, reflects: "[BoE Governor Mark Carney] came to the GCHQ's London office and told me that there were too many sources of advice from government and too much confusion for industry."[615]

(UK) Prudential Regulatory Authority (PRA): PRA is one of the UK Financial Service Authorities (UK FSAs), and one of the global thought leaders on cyber resilience. In July 2018, the UK FSAs published a series of discussion papers, "Building the UK Financial Sector's Operational Resilience."[616]

(UK) UK Finance: UK Finance is a financial industry trade association established after Brexit. It represents financial institutions in discussions with the UK Financial Service Authorities: the Prudential Regulatory Authority, the Financial Conduct Authority, and the Bank of England.[617]

(United Nations) UN Department of Economic and Social Affairs (UN DESA): In 2015, UN DESA organized the Third International Conference on Financing for Development, resulting in the Addis Ababa Action Agenda (AAAA). This document created a global framework for financing the 2030 Agenda for Sustainable Development and mandated a high-level dialogue on financing for development be held every four years.[618] The most recent round of these dialogues was held in September 2019.

(United Nations) UN Group of Governmental Experts (UN GGE): The UN GGE was established in 2004 to examine how information communications technology affected national security and military affairs. The UN GGE is composed of twenty-five member countries: five are the permanent members of the Security Council and the remaining members are chosen "on the basis

of equitable geographical distribution." There have been six iterations of the UN GGE thus far. The sixth UN GGE is currently running in parallel with the UN Open-Ended Working Group (OEWG).

(United Nations) UN Office on Drugs and Crime (UNODC): The UNODC "promotes long-term and sustainable capacity-building in the fight against cybercrime," through resources, trainings, and guidance. It facilitates the Global Programme on Cybercrime, which provides technical assistance, prevention and awareness raising, and analysis in developing countries.[619]

(United Nations) UN Open-Ended Working Group (OEWG): In 2018, the UN General Assembly created the OEWG as a second process alongside the UN Group of Governmental Experts (UN GGE) that would focus on norms of responsible state behavior in cyberspace. In contrast to the UN GGE, which limited its membership to twenty-five UN member states, the OEWG is open to all UN members and holds consultative meetings with industry, academia, and civil society. The duplicate GGE and OEWG processes are the product of rival resolutions proposed by the United States and the Russian Federation, respectively. In 2018 the UN First Committee voted to pass both, thus establishing the concurrent processes.

(United Nations) UN Secretary-General's Special Advocate (UNSGSA) for Inclusive Finance for Development: In 2009, UN Secretary-General Ban Ki-Moon designated Queen Máxima of the Netherlands the UN Secretary-General's Special Advocate for Inclusive Finance for Development. The UNSGSA's strategic priorities include 1) usage and development impact; 2) policies for digital financial inclusion;[620] and 3) underserved populations.

(United Nations) UN Security Council (UNSC): The UNSC, charged with maintaining international peace and security, has not yet held a formal debate on cybersecurity. However, the 2019 UNSC Panel of Experts report on North Korea examined how North Korean cyber attacks were used to evade counter-proliferation sanctions and steal billions of dollars.[621]

(U.S.) American Bankers Association (ABA): The ABA is a U.S.-based financial industry trade association that primarily represents small and mid-sized financial institutions. The ABA was a co-creator of the Financial Services Sector Cybersecurity Profile.[622]

(U.S.) Bank Policy Institute (BPI): The BPI is a U.S.-based financial industry trade association. It was established in 2018 after the Financial Services Roundtable and the Clearing House Association merged. BITS is the

technology policy division of the BPI. The BPI was a co-creator of the Financial Services Sector Cybersecurity Profile.[623]

(U.S.) Board of Governors of the U.S. Federal Reserve System (Federal Reserve Board): The Federal Reserve Board is the main governing body of the U.S. Federal Reserve Banks. The Board is embracing operational resilience slowly by prioritizing regulatory harmonization and private sector input over speed. In 2016, it signaled an advance notice of proposed rulemaking around enhanced cyber risk management standards; these rules were to be issued in 2017 but were later deprioritized after comments from the private sector.[624] In the fall of 2019, the Fed reopened the consultation process for the proposed "Enhanced Cyber Risk Management Standards," suggesting that resilience is once again becoming a priority.

(U.S.) Cyber Fraud Task Forces (CFTFs): The Cyber Fraud Task Forces were created in July 2020 after the U.S. Secret Service announced that it would merge its Electronic Crimes Task Forces (ECTFs) and its Financial Crimes Task Forces (FCTFs). The Electronic Crimes Task Forces program is a series of regional agreements between the U.S. Secret Service, federal and local law enforcement, the private sector, and academia "for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment system."[625] The first ECTF, the New York Electronic Crimes Task Force (NY ECTF) was established in 1995 to "combat computer-based threats to our financial payment systems and critical infrastructures."[626] Subsequent ECTFs were mandated by the USA PATRIOT Act (2001). The ECTFs have "prevented over $13 billion in potential losses and arrested approximately 10,000 individuals."[627]

(U.S.) Cyber Readiness Institute: Launched in 2017 by Mastercard, Microsoft, and others, the Cyber Readiness Institute builds and promotes capacity-building resources for small and medium-sized enterprises.[628] It is administered by the Center for Global Enterprise.

(U.S.) Cybersecurity Talent Initiative (CTI): Announced in April 2019, CTI is a public-private partnership that provides students in cybersecurity-related fields with two-year placements at federal agencies with cybersecurity needs. Following completion of federal service placements, graduating students are also invited to apply for private sector jobs.[629] CTI is supported by Mastercard, Microsoft, Workday, and Partnership for Public Service.

(U.S.) Cyber Workforce Alliance (CWA): Created in 2015 as a division of the online learning platform iQ4, CWA is a partnership of government, industry,

and university leaders committed to training cybersecurity professionals. It provides an online platform and curriculum and connects industry mentors and university professors with students seeking to gain new cybersecurity skills.[630] According to a press release, CWA's partners include individuals at the Federal Reserve Bank of New York and its member banks, at the Securities Industry and Financial Markets Association (SIFMA), as well as 600 corporate executives.[631]

(U.S.) Department of the Treasury: The U.S. Department of the Treasury is charged with protecting the critical infrastructure of financial institutions. Within the Treasury Department, the Office of the Comptroller of the Currency and the Office of Critical Infrastructure Protection work closely with U.S. financial institutions on cybersecurity issues. The Treasury Department also runs the Office of Foreign Assets Control (OFAC), the body in charge of managing U.S. sanctions. In 2020, legislation was introduced, with the support of the Trump administration, including the U.S. Department of Homeland Security, to move the U.S. Secret Service back to the Department of the Treasury.[632]

(U.S.) Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3): IC3, a branch of the FBI, provides the public with a mechanism for reporting cyber crime. IC3's Recovery Asset Team (RAT) was established in February 2018 to "streamline communication with financial institutions." In 2019, RAT reported 1,307 incidents, with $304 million recovered from a total of $384 million is losses.[633]

(U.S.) Financial and Banking Information Infrastructure Committee (FBIIC): Established following the attacks on September 11, 2001, the FBIIC was created to coordinate the security and reliability of the financial sector infrastructure in the United States. The Committee is composed of eighteen member organizations across the U.S. financial regulatory community and is chaired by the Assistant Secretary of the Treasury for Financial Institutions.[634]

(U.S.) Financial Crimes Enforcement Network (FinCEN): FinCEN is a bureau of the U.S. Department of the Treasury whose mission is to "safeguard the financial system from illicit use and combat money laundering and promote national security through collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities."[635] In 2019, FinCEN restructured and established the new Cyber and Emergent Issues Section under the Strategic Operations Division.[636]

(U.S.) Financial Services Sector Coordinating Council (FSSCC): FSSCC, an industry initiative established in 2002, is the coordinating body for critical

infrastructure protection within the financial sector. FSSCC facilitates coordination between the private sector and U.S. government agencies charged with critical infrastructure protection. It established the Financial Services Sector Cybersecurity Profile in 2018.[637]

(U.S.) Financial Systemic Analysis and Resilience Sector (FSARC): A consortium of the most critical U.S. financial institutions established the FSARC in 2016 with the mission to "proactively identify, analyze, assess and coordinate activities to mitigate systemic risk to the U.S. financial system."[638] FSARC functions as a mechanism for banks to collaborate with the U.S. national security community, including the Departments of Defense, Homeland Security, the Treasury, and the FBI. Its offices are steps away from the Department of Homeland Security's National Cybersecurity and Communications Integration Center. In 2017, FSARC began providing the U.S. Cyber Command with cyber threat data in an arrangement called "Project Indigo."[639]

(U.S.) National Cyber-Forensics and Training Alliance's (NCFTA) Cyber Financial (CyFin) Program: The NCFTA is a nonprofit partnership between industry and government focused on "two-way collaboration and cooperation to identify, mitigate, and disrupt cybercrime."[640] NCFTA's CyFin program was established in 2007 to focus on disrupting malicious actors in the financial services industry. CyFin's analysis has been frequently cited in Department of Justice indictments, including the arrest of FIN7 members.[641]

(U.S.) National Initiative for Cybersecurity Education (NICE): A program of the National Institute of Standards and Technology (NIST), NICE was founded in 2010 to convene government, academic, and private sector stakeholders around cybersecurity education and training.[642] In August 2017, NICE published a Cybersecurity Workforce Framework to help standardize descriptions of cybersecurity work.[643]

(U.S.) New York State Department of Financial Services (NYDFS): NYDFS is the financial regulator for New York State and oversees most financial institutions in the U.S. financial sector located in New York City. In 2016, NYDFS published "Cybersecurity Requirements for Financial Service Companies," a major revision to existing cybersecurity supervision requirements that focused less on preventing cyber incidents and more on recovering from them.[644]

(U.S.) Office of Foreign Assets Control (OFAC): OFAC is an office within the U.S. Department of the Treasury that administers and enforces U.S. sanctions, including cyber-related sanctions authorized by U.S. Executive Order 13694 (Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities).

(U.S.) Securities and Exchange Commission (SEC): The SEC is the U.S. financial authority that oversees securities markets. Primarily through its Office of Compliance Inspections and Examinations and its Cyber Unit (part of the SEC's Division of Enforcement), the SEC provides guidance, conducts examinations, issues risk alerts, and sets policy on cybersecurity and resilience for key market participants like securities exchanges, securities brokers and dealers, investment advisors, and mutual funds. The SEC also coordinates with other financial authority counterparts to advance the cybersecurity of the broader U.S. financial sector.

(U.S.) Sheltered Harbor: Sheltered Harbor is a U.S. financial sector-led initiative designed to improve the resilience of and preserve public confidence in the U.S. financial system, specifically with respect to the integrity of financial data.[645] It functions as a fail-safe to restore financial data for banks and customers in the event of a major disruption. As of October 2018, Sheltered Harbor holds the data for 70 percent of U.S. deposit accounts and 55 percent of U.S. retail brokerage client assets.[646]

U.S. Secret Service: The U.S. Secret Service is the primary law enforcement agency countering financial cyber crimes in the United States. The U.S. Secret Servic runs the Cyber Fraud Task Forces.[647] At the time of writing, the U.S. Congress is considering legislation, which the Trump administration supports, to move the U.S. Secret Service and its cyber investigative capabilities from the Department of Homeland Security back to the Department of the Treasury.[648]

World Bank: The World Bank focuses on developing law enforcement capacity to combat cyber crime.[649] It also focuses on cybersecurity in financial inclusion efforts through the provision of technical assistance, and data collection. Two of its initiatives, Harnessing Innovation for Financial Inclusion and the Financial Inclusion Global Initiative, emphasize digital innovation for financial inclusion and provide technical assistance to financial services providers seeking to modernize or expand national payment systems.[650] The World Bank also runs Identification for Development, a program that provides technical assistance and advisory services and facilitates knowledge-sharing among national initiatives to implement digital identification systems.

World Economic Forum (WEF): In January 2018, the WEF established the Global Centre for Cybersecurity, based in Geneva, Switzerland, to help promote a secure and open cyberspace.[651] The center strives to create a global platform for governments, businesses, experts, and law enforcement agencies to collaborate on cybersecurity challenges. The organization focuses on

collaboration, information sharing, and common standards to combat international cyber crime.[652]

World Federation of Exchanges: The WFE is a global financial industry association for publicly regulated stock, futures, and options exchanges and central counterparties. In addition to engagement with financial authorities, the WFE conducts industry-relevant cybersecurity research and operates the Global Exchange Cyber Security Working Group.

ABOUT CARNEGIE'S FINCYBER PROJECT

Launched in 2015, Carnegie's FinCyber project focuses on how to better protect the global financial system against cyber threats. From its early focus on the G20, this work soon expanded to include a cyber resilience capacity-building tool box as well as the timeline tracking cyber incidents involving financial institutions and a monthly newsletter to keep track of latest developments. This strategy report is built on and inspired by these other ongoing workstreams with more details available at: https://carnegieendowment.org/specialprojects/fincyber/.

G20 Proposal on an International Norm Against Manipulating the Integrity of Financial Data. This early work focused on securing a G20 commitment not to engage in offensive cyber operations that could undermine financial stability, namely manipulating the integrity of financial data, and to cooperate when such incidents occur.

Cyber Resilience Capacity-building Tool Box. Released in 2019, this tool box consists of designed six one-page guides for an organization's Board, CEO, and CISO outlining best practices for smaller financial institutions—now available in multiple languages. Carnegie partnered with the IMF, SWIFT, FS-ISAC, Standard Chartered, the Cyber Readiness Institute, and the Global Cyber Alliance to help disseminate this work.

Working Group on Cybersecurity Workforce. In April 2020, Carnegie launched this working group, comprised of 10 major financial institutions and several independent experts, focusing on cybersecurity workforce challenges in the financial sector.

Timeline of Cyber Incidents Involving Financial Institutions. This timeline, developed in association with BAE Systems' Cyber Threat Intelligence unit, tracks the evolution of the cyber threat landscape and details over 200 filterable cyber incidents since 2007.

FinCyber Research Working Paper Series. This paper series is designed to be a platform for thought-provoking studies and to strengthen cross-disciplinary research. Contributors include central bank and government officials, industry representatives, and other relevant experts in addition to Carnegie scholars.

FinCyber Monthly Newsletter. Carnegie publishes the "FinCyber Update" monthly newsletter tracking latest developments at the intersection of cybersecurity and finance.

The following organizations have provided funding support for Carnegie's FinCyber project: the William and Flora Hewlett Foundation, the Bill & Melinda Gates Foundation, the SWIFT Institute, Bank of America, Capital One, the Commonwealth Bank of Australia, JPMorgan Chase, Standard Chartered, Accenture, Amazon Web Services, and the Ministry of Foreign Affairs of The Netherlands.

ABOUT THE AUTHORS

Tim Maurer is the director of the Cyber Policy Initiative and a senior fellow in Carnegie's Technology and International Affairs Program. He works on the geopolitical implications of the internet and cybersecurity, with a focus on the global financial system, influence operations, and other areas of importance as actors exploit the gray space between war and peace. In 2018, Cambridge University Press published his *Cyber Mercenaries: The State, Hackers, and Power*, a comprehensive analysis examining proxy relationships between states and hackers.

Arthur Nelson is a research analyst in Carnegie's Cyber Policy Initiative. He works on international cybersecurity and technology policy issues, including encryption policy, cybersecurity in the context of the financial system, and the geopolitical dimensions of fintech. Prior to Carnegie, he worked on election security issues at Elections Ontario.

ACKNOWLEDGMENTS

With any project that is based on engaging more than 200 stakeholders, there are more people that deserve thanks than there is space to properly do so and there are likely some that are not but should have been mentioned—but certainly none that are and should not have been!

To highlight a few, the authors are particularly grateful to their partners at the World Economic Forum, namely Alois Zwinggi and Sean Doyle for their early and unwavering support. They are also indebted to the members of the international FinCyber Advisory Group who time and again offered essential counsel and criticism. The staff at Wilton Park, the International Monetary Fund, and the Munich Security Conference provided wonderful venues and support to road test some of the initial ideas and to share proposals with key stakeholders and senior officials.

The authors are indebted to the contributions of their current and former colleagues at the Carnegie Endowment for International Peace, including George Perkovich, Jon Bateman, Taylor Grossman, Natalie Thompson, Evan Burke, Kamaal Thomas, and Kathryn Taylor. They wish to thank Isabella Furth and Sam Brase for their assistance with the final manuscript, and Jocelyn Soly, Amy Mellon, and the Glen Echo Group for their excellent design skills. Cheri McGuire, Chris Finan, Natasha de Teran, and Sultan Meghji deserve special mention here in addition to Secretary Michael Chertoff, Congressman Jim Langevin, Siobhan MacDermott, Greg Rattray, and Laura Bate. Eli Sugarman deserves a stand-alone shoutout, as does Claire Felten for her patience and the design of the cover page.

Finally, sincere gratitude goes to the dozens of experts around the globe and across the financial services industry, the central bank and financial regulatory community, the diplomatic and national security communities, and the technical community for their outstanding insights, suggestions, and participation in the dozens of workshops and briefings held over the last year. The report's contents are the sole responsibility of the authors and do not necessarily represent the views of any other individuals or institutions.

LIST OF ABBREVIATIONS

ABA	American Bankers Association
ABS	Association of Banks in Singapore
ACPR	Prudential Supervision and Resolution Authority (France)
AFI	Alliance for Financial Inclusion
AFME	Association for Financial Markets in Europe
AML	anti-money laundering
ARF	ASEAN Regional Forum
A-RMF	Actionable Cybersecurity Risk Management Framework
ASEAN	Association of Southeast Asian Nations
ASIFMA	Asia Securities Industry and Financial Markets Association
BaFin	Federal Financial Supervisory Authority (Germany)
BCBS	Basel Committee on Banking Supervision
BCM	Business Continuity Management
BIS	Bank for International Settlements
BoE	Bank of England
BPI	Bank Policy Institute
CAPS	Cyber-attack Against Payment Systems
CBM	confidence-building measures
CDA	Cyber Defence Alliance
CEG	Cyber Expert Group
CERT	computer emergency response team
CGAP	Consultative Group to Assist the Poor
CI	critical infrastructure
CII	critical information infrastructure
CIISI-EU	Cyber Information and Intelligence Sharing Initiative-European Union
CISO	chief information security officer
CMORG	Cross Market Operational Resilience Group
CPMI	Committee on Payments and Market Infrastructures
CRCC	Cyber Resilience Coordination Centre

CRI	Cyber Risk Institute
CROE	cyber resilience oversight expectations
CSA	Cyber Security Agency (Singapore)
CSIRT	computer security incident response team
CTF	counter terrorist financing
CWA	Cybersecurity Workforce Alliance
DDoS	distributed denial-of-service
DFS	digital financial services
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
EBF	European Banking Federation
EC	European Commission
ECB	European Central Bank
ECRB	Euro Cyber Resilience Board
EC3	European Cybercrime Centre
EMEA	Europe, Middle East, and Africa
ENISA	European Union Agency for Cybersecurity
ESAs	European supervisory authorities
EU	European Union
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation (U.S.)
FCA	Financial Conduct Authority (UK)
FC3	Cyber and Finance Continuity Center (Israel)
FDIC	Federal Deposit Insurance Corporation (U.S.)
FIRST	Forum of Incident Response and Security Teams
FIUs	financial intelligence units
FMI	financial market infrastructures
FSARC	Financial Systemic Analysis and Resilience Center (U.S.)
FSCCC	Financial Sector Cyber Collaboration Centre (UK)
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordinating Council
FIAP	Financial Inclusion Action Plan (G20)
FSB	Financial Stability Board

GCHQ	Government Communications Headquarters (UK)
GDPR	General Data Protection Regulation
GFCE	Global Forum on Cyber Expertise
GFMA	Global Financial Markets Association
GGE	Group of Governmental Experts (UN)
GPFI	Global Partnership for Financial Inclusion
HKMA	Hong Kong Monetary Authority
IAIS	International Association of Insurance Supervisors
IB-CART	Indian Banks–Center for Analysis of Risks and Threats
IDRBT	Institute for Development and Research in Banking Technology (India)
IIF	Institute of International Finance
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
ISO	International Organization for Standardization
J-CAT	Joint Cybercrime Action Taskforce
MAS	Monetary Authority of Singapore
MNOs	mobile network operators
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre (UK)
NIST	National Institute of Standards and Technology (U.S.)
NYDFS	New York State Department of Financial Services
OAS	Organization of American States
OCC	Office of the Comptroller of the Currency (U.S.)
ODA	official development assistance
OECD	Organisation for Economic Co-operation and Development
OEWG	Open-Ended Working Group (UN)
OSCE	Organization for Security and Co-operation in Europe
RBI	Reserve Bank of India
SARs	suspicious activity reports
SIFMA	Securities Industry and Financial Markets Association
STRs	suspicious transaction reports
SWIFT	Society for Worldwide Interbank Financial Telecommunication

TIBER-EU	Framework for Threat Intelligence-Based Ethical Red Teaming-European Union
TF-CSIRT	Task Force on Computer Security Incident Response Teams
UK FSAs	United Kingdom Financial Service Authorities
UN	United Nations
UNIDIR	UN Institute for Disarmament Research
UNODA	UN Office for Disarmament Affairs
UNODC	UN Office on Drugs and Crime
UNSGSA	UN Secretary General's Special Advocate
WEF	World Economic Forum
WFE	World Federation of Exchanges

LIST OF FIGURES AND TABLES

Figures

Tables

NOTES

Preface

1 Michael Corkery and Matthew Goldstein, "North Korea Said to Be Target of Inquiry Over $81 Million Cyberheist," *New York Times,* March 22, 2017, DealBook, https://www.nytimes.com/2017/03/22/business/dealbook/north-korea-said-to-be-target-of-inquiry-over-81-million-cyberheist.html?_r=0.

2 "GDP (current US$)—Bangladesh," World Bank, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=BD.

3 Niaz Alam, "The Great Bangladesh Cyber Heist Shows Truth Is Stranger Than Fiction," *Dhaka Tribune,* March 12, 2016, https://www.dhakatribune.com/uncategorized/2016/03/12/the-great-bangladesh-cyber-heist-shows-truth-is-stranger-than-fiction.

4 FinCyber Project, "Cybersecurity and the Financial System," Carnegie Endowment for International Peace, https://carnegieendowment.org/specialprojects/fincyber/.

5 FinCyber Project, "Protecting Financial Stability: G20 Proposal," Carnegie Endowment for International Peace, https://carnegieendowment.org/specialprojects/protectingfinancialstability/.

6 FinCyber Project, "Cyber Resilience and Financial Organizations: A Capacity-building Tool Box," Carnegie Endowment for International Peace, https://carnegieendowment.org/specialprojects/fincyber/guides.

7 FinCyber Project, "Timeline of Cyber Incidents Involving Financial Institutions," Carnegie Endowment for International Peace, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

Part I: Strategy and Overview of Recommendations

8 Deloitte, "Realizing the Digital Promise: COVID-19 Catalyzes and Accelerates Transformation in Financial Services," 2020, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-realizing-the-digital-promise-covid-19-catalyzes-and-accelerates-transformation.pdf.

9 Christine Lagarde, "Payments in a Digital World," speech, Deutsche Bundesbank online conference on banking and payments in the digital world, Frankfurt am Main, September 10, 2020, https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200910~31e6ae9835.en.html.

10 Lily Hay Newman, "The Billion-Dollar Hacking Group Behind a String of Big Breaches," *Wired,* April 4, 2018, https://www.wired.com/story/fin7-carbanak-hacking-group-behind-a-string-of-big-breaches/.

11 United Nations Security Council, "Letter Dated 31 July 2019 From the Panel of Experts Established Pursuant to Resolution 1874 (2009) Addressed to the Chair of the Security Council Committee Established Pursuant to Resolution 1718 (2006)." U.S. Government Joint Advisory, "Alert (AA20-239A) FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks," August 26, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-239a.

12 Tim Maurer and Arthur Nelson, "COVID-19's Other Virus: Targeting the Financial System," *Strategic Europe* (blog), April 21, 2020, 1, https://carnegieeurope.eu/strategiceurope/81599.

13 David E. Sanger, "U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam," *New York Times*, March 24, 2016, https://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html.

14 Tim Maurer et al., "Toward a Global Norm Against Manipulating the Integrity of Financial Data," Carnegie Endowment for International Peace, March 2017, https://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403; European Systemic Risk Board, "Systemic Cyber Risk," February 25, 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk-101a09685e.en.pdf; Greg Ros, "The Making of a Cyber Crash: A Conceptual Model for Systemic Risk in the Financial Sector," European Systemic Risk Board, Occasional Paper Series No 16, May 2020, https://www.esrb.europa.eu/pub/pdf/occasional/esrb.op16~f80ad1d83a.en.pdf.

15 Davey Winder, "$645 Billion Cyber Risk Could Trigger Liquidity Crisis, ECB's Lagarde Warns," *Forbes*, March 10, 2020, https://www.forbes.com/sites/daveywinder/2020/02/08/645-billion-cyber-risk-could-trigger-liquidity-crisis-ecbs-lagarde-warns/.

16 Mark Bendeich and Leika Kihara, "Cyber Threat Could Become Banking's Most Serious Risk," Reuters, January 24, 2019, https://www.reuters.com/article/davos-meeting-cyber-kuroda/davos-cyber-threat-could-become-bankings-most-serious-risk-boj-idUSS8N1PK01N.

17 Hugh Son, "Jamie Dimon Says Risk of Cyberattacks 'May Be Biggest Threat to the US Financial System,'" CNBC, April 4, 2019, https://www.cnbc.com/2019/04/04/jp-morgan-ceo-jamie-dimon-warns-cyber-attacks-biggest-threat-to-us.html.

18 Financial Stability Board, "Effective Practices for Cyber Incident Response and Recovery: Consultative Document," April 20, 2020, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document/.

19 IOSCO Cyber Task Force, "Final Report," The Board of the International Organization of Securities Commissions, June, 2019, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf.

20 Gerald J. Schueler, "The Unpredictability of Complex Systems," *Journal of the Washington Academy of Sciences* 84, no. 1 (1996): 3–12; John H. Holland, "Complex Adaptive Systems," *Daedalus* 121, no. 1, (1992): 17–30; George A. Polacek et al., "On Principles and Rules in Complex Adaptive Systems: A Financial System Case Study," *Systems Engineering* 15, no. 4 (2012): 433–47, https://doi.org/10.1002/sys.21213.

21 Ryan Browne, "Banks Must Behave 'More Like Technology Companies' to Survive, Finance Execs Say," CNBC, November 18, 2019, https://www.cnbc.com/2019/11/18/banks-must-behave-like-tech-companies-to-survive-amid-fintech-threat.html; Gregory Barber, "Every Tech Company Wants to Be a Bank—Someday, at Least," *Wired*, November 16, 2019, https://www.wired.com/story/tech-companies-banks/.

22 Financial Stability Board, "Effective Practices for Cyber Incident Response and Recover: Consultative document," April 20, 2020, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document/.

23 For a comprehensive overview of individual countries' red team testing frameworks, see: Raymond Kleijmeer, Jermy Prenio, and Jeffery Yong, "FSI Insights on Policy Implementation No 21—Varying Shades of Red: How Red Team Testing Frameworks Can Enhance the Cyber Resilience of Financial Institutions," Financial Stability Institute, November 2019, https://www.bis.org/fsi/publ/insights21.pdf.

24 "Digital Finance Package: Commission Sets Out New, Ambitious Approach to Encourage Responsible Innovation to Benefit Consumers and Businesses," European Commission, Brussels, September 24, 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684.

25 Hanna Ziady, "New Zealand Spy Agency Investigating 'Severe' Cyberattack on Shody Exchange," CNN Business, August 28, 2020, https://www.cnn.com/2020/08/27/investing/new-zealand-stock-exchange-cyber-attack/index.html.

26 This is modeled after the exercise series carried out by the financial sector's Securities Industry and Financial Markets Association: "Cybersecurity Exercise: Quantum Dawn V," Security Industry and Financial Markets Association (SIFMA), https://www.sifma.org/resources/general/cybersecurity-exercise-quantum-dawn-v/.

27 This is modeled after the Financial Systemic Analysis & Resilience Center (FSARC): "Identifying Cyber Threats With FSARC," JP Morgan, October 9, 2018, https://www.jpmorgan.com/commercial-banking/insights/cyber-threats-fsarc.

28 For example, in 2014, the U.S. Department of Justice and the Federal Trade Commission issued a joint statement for that purpose regarding the sharing of cyber threat information. The 2015 U.S. Cybersecurity Information Sharing Act (CISA) goes a step further by making clear that "activity authorized by CISA does not violate federal and state antitrust laws." U.S. CERT, "Cybersecurity Information Sharing Act—Frequently Asked Questions," accessed July 20, 2020, https://www.us-cert.gov/sites/default/files/ais_files/CISA_FAQs.pdf.

29 Relatedly, see also the submissions by members of the World Economic Forum's "Global Coalition to Fight Financial Crime" to inform the European Commission's Anti-Money Laundering Action Plan: "Press Release: Statement on the European Commission Action Plan on Preventing Money Laundering and Terrorism Financing," Global Coalition to Fight Financial Crime, Brussels, August 26, 2020, https://www.gcffc.org/press-release-statement-on-the-european-commission-aml-action-plan/.

30 Jim Edwards, "A False Rumor on WhatsApp Started a Run on a London Bank," Business Insider, May 13, 2019, https://www.businessinsider.com/whatsapp-rumour-started-run-on-metro-bank-2019-5.

31 Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (January 2017): 44–71, https://doi.org/10.1162/ISEC_a_00266.

32 International Committee of the Red Cross, "Building Respect for the Law," https://www.icrc.org/en/what-we-do/building-respect-ihl.

33 This would build on the ICRC's existing publications on the topic, including: Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, "Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts," *International Review of the Red Cross* (2020), 0 (0), 1–48, https://international-review.icrc.org/sites/default/files/reviews-pdf/2020-09/Twenty-years-on-IHL-and-cyber-operations.pdf; Laurent Gisel, Tilman Rodenhäuser, and Kubo Mačák, "Cyber Attacks Against Hospitals and the COVID-19 Pandemic: How Strong Are International Law Protections?," *Humanitarian Law & Policy Blog* (blog), ICRC, April 2, 2020, https://blogs.icrc.org/law-and-policy/2020/04/02/cyber-attacks-hospitals-covid-19/; Peter Maurer et. al., "Call to Governments: Work Together to Stop Cyber Attacks on Health Care," ICRC, May 25, 2020, https://www.icrc.org/en/document/governments-work-together-stop-cyber-attacks-health-care.

34 U.S. Department of Homeland Security, "Joint Advisory—Alert (AA20-239A) FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks," August 26, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-239a.

35 United Nations Security Council, "Letter Dated 31 July 2019 From the Panel of Experts Established Pursuant to Resolution 1874 (2009) Addressed to the Chair of the Security Council Committee Established Pursuant to Resolution 1718 (2006)," August 30, 2019, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf.

36 Global Infrastructure Hub, "Funders and Strategic Partners," accessed July 20, 2020, https://www.gihub.org/about/funders-and-strategic-partners/; and Global Partnership for Financial Inclusion, "GPFI," accessed July 20, 2020, https://www.gpfi.org/.

37 The changing nature of the financial system also influences what Harvard professor Joseph Nye calls "deterrence by entanglement"—the more entangled actors are in a system, the more likely it is that they will be deterred from attacking parts of the system. See Nye.

Priority #1: Cyber Resilience

38 G20 Finance Ministers and Central Bank Governors, "Communiqué," March 17, 2017, Carnegie Endowment for International Peace, https://carnegieendowment.org/files/g20-communique.pdf.

39 "FSB Publishes Stocktake on Cybersecurity Regulatory and Supervisory Practices," October 13, 2017, https://www.fsb.org/2017/10/fsb-publishes-stocktake-on-cybersecurity-regulatory-and-supervisory-practices/.

40 "FSB Publishes Stocktake on Cybersecurity Regulatory and Supervisory Practices."

41 GFMA and IIF, "Discussion Draft Principles Supporting the Strengthening of Operational Resilience Maturity in Financial Services," October 2019, https://www.gfma.org/wp-content/uploads/2019/10/discussion-draft-iif-gfma-operational-resilience-principles-october-2019.pdf.
42 Bank of England, Financial Conduct Authority, and Prudential Regulatory Authority, "Building Operational Resilience: Impact Tolerances for Important Business Services."
43 Davey Winder, "$645 Billion Cyber Risk Could Trigger Liquidity Crisis, ECB's Lagarde Warns," *Forbes*, accessed March 10, 2020, https://www.forbes.com/sites/daveywinder/2020/02/08/645-billion-cyber-risk-could-trigger-liquidity-crisis-ecbs-lagarde-warns/.
44 Art Lindo, "Oversight of Cyber Resilience in the Financial Regulatory System: Seminar for Senior Bank Supervisors From Emerging Economies," October 25, 2019, http://pubdocs.worldbank.org/en/388141572546457065/Day-5-ArtLindo-FRB-CyberResilience.pdf.
45 G7 Finance Ministers and Central Bank Governors, "Press Release," G7 Information Centre, University of Toronto, October 13, 2017, http://www.g7.utoronto.ca/finance/171013-cybercrime.html.
46 G7 Finance Ministers and Central Bank Governors, "Press Release," G7 Information Centre, University of Toronto, October 13, 2017, http://www.g7.utoronto.ca/finance/171013-cybercrime.html.
47 Italian Ministry of the Economy and Finance, "The G7 Reaffirms Its Commitment to Strengthening Cybersecurity in the Financial Sector," October 11, 2018, http://www.dt.mef.gov.it/en/news/2018/G7_cyber_security.html.
48 Bank of Japan, "G-7 Fundamental Elements for Threat-Led Penetration Testing and Third Party Cyber Risk Management in the Financial Sector," Press Release, October 15, 2018, https://www.boj.or.jp/en/announcements/release_2018/rel181015k.htm/.
49 "Cybersecurity: Coordinating Efforts to Protect the Financial Sector in the Global Economy," (conference, Banque de France and the French Ministry for the Economy and Finance, Paris, France, May 10, 2019), https://www.banque-france.fr/en/conferences-and-media/seminars-and-symposiums/research-conferences-and-symposiums/french-presidency-g7-2019-cybersecurity-coordinating-efforts-protect-financial-sector-global-economy.
50 Leigh Thomas, "G7 Countries to Simulate Cross-Border Cyber Attack Next Month: France," Reuters, May 10, 2019, https://www.reuters.com/article/us-g7-france-cyber-idUSKCN1SG1KZ.
51 Jaime Vazquez and Martin Boer, "Addressing Regulatory Fragmentation to Support a Cyber-Resilience Global Financial Services Industry," n.d., https://www.iif.com/portals/0/Files/private/iif_cyber_reg_04_25_2018_final.pdf.
52 GFMA and IIF, "Discussion Draft Principles Supporting the Strengthening of Operational Resilience Maturity in Financial Services."
53 Marc Saidenberg, John Liver, and Eugene Goyne, "2020 Global Bank Regulatory Outlook: Four Major Themes Dominating the Regulatory Landscape in 2020," EY, January 20, 2020, https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-global-regulatory-outlook-four-major-themes-dominating-the-regulatory-landscape-in-2020_v2.pdf.
54 Bank of England and Financial Conduct Authority, "Building the UK Financial Sector's Operational Resilience," July 2018, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf.
55 "Building Operational Resilience: Impact Tolerances for Important Business Services," Bank of England and Financial Conduct Authority, December 2019, https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper.
56 "Building Operational Resilience: Impact Tolerances for Important Business Services."
57 Bank of England, "CBEST Implementation Guide," Bank of England, 2016, https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf.
58 Jeffrey Roman, "Bank of England Launches Cyber Framework," BankInfoSecurity, June 10, 2014, https://www.bankinfosecurity.com/bank-england-launches-cyber-framework-a-6934.

59 Alex Hern, "Operation 'Waking Shark II' Tests the Ccybersecurity of Britain's Banks," *Guardian,* November 12, 2013, https://www.theguardian.com/technology/2013/nov/12/operation-waking-shark-ii-tests-cybersecurity-banks; Bank of England, "Sector Simulation Exercise: SIMEX 2018 Report," September 27, 2019, https://www.bankofengland.co.uk/report/2019/sector-simulation-exercise-simex-2018-report.

60 David Milliken, "U.S. and UK to Test Financial Cyber-Security Later This Month," Reuters, November 2, 2015, https://www.reuters.com/article/us-britain-usa-cybersecurity-idUSKCN0SR1DW20151102.

61 SIFMA, "Cybersecurity Exercise: Quantum Dawn V," February 28, 2020, https://www.sifma.org/resources/general/cybersecurity-exercise-quantum-dawn-v/.

62 National Cyber Security Centre, "Cyber Security Information Sharing Partnership (CiSP)," September 2016, https://www.ncsc.gov.uk/information/cyber-security-information-sharing-partnership--cisp-.

63 Andrew Gracie, "Cyber in Context," Speech at the UK Financial Services Cyber Security Summit, London, July 2015, https://www.bankofengland.co.uk/-/media/boe/files/speech/2015/cyber-in-context.pdf.

64 Stephen Jones, "A Resilient Banking Sector," UK Finance, December 7, 2018, https://www.ukfinance.org.uk/blogs/resilient-banking-sector.

65 Bank for International Settlements (BIS), "Cyber Resilience: Range of Practices," December 2018, https://www.bis.org/bcbs/publ/d454.pdf.

66 European Commission, "Executive Summary of the Impact Assessment Accompanying the Document: Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector," Commission Staff Working Document, September 24, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2020:199:FIN.

67 The ESAs are the European Banking Authority, the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA). European Commission, "FinTech Action Plan: For a More Competitive and Innovative European Financial Sector," March 2018, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

68 European Supervisory Authorities, "Joint Advice of the European Supervisory Authorities," April 10, 2019, https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf.

69 European Banking Authority, "EBA Guidelines on ICT and Security Risk Management," November 28, 2019, https://eba.europa.eu/eba-publishes-guidelines-ict-and-security-risk-management.

70 European Banking Authority, "EBA Guidelines on ICT and Security Risk Management," November 28, 2019, https://eba.europa.eu/eba-publishes-guidelines-ict-and-security-risk-management.

71 European Banking Authority, "Guidelines on Outsourcing Arrangements," June 5, 2019, https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements.

72 European Commission, "Consultation Document: Digital Operational Resilience Framework for Financial Services: Making the EU Financial Sector More Secure," December 2019, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf.

73 European Commission, "Consultation Document: Digital Operational Resilience Framework for Financial Services: Making the EU Financial Sector More Secure."

74 European Banking Federation, "Digital Operational Resilience Framework: EBF Key Messages on the Commission Consultation," April 6, 2020, https://www.ebf.eu/cybersecurity/ebf-key-messages-on-the-commission-consultation-on-a-digital-operational-resilience-framework/.

75 European Commission, "Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU," September 24, 2020, https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-591-F1-EN-MAIN-PART-1.PDF.

76 European Commission, "Executive Summary of the Impact Assessment Accompanying the Document: Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector," Commission Staff Working Document, September 24, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2020:199:FIN.

77 European Commission, "Executive Summary of the Impact Assessment Accompanying the Document: Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector," Commission Staff Working Document, September 24, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2020:199:FIN.

78 European Banking Authority, "EBA Guidelines on ICT and Security Risk Management."

79 European Commission, "Executive Summary of the Impact Assessment Accompanying the Document: Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector," Commission Staff Working Document, September 24, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2020:199:FIN.

80 Euro Cyber Resilience Board Secretariat, "Cyber Information and Intelligence Sharing: A Practical Example," Cyber Information Sharing and Intelligence Sharing Initiative, European Central Bank, September 2020, https://www.ecb.europa.eu/paym/groups/euro-cyber-board/shared/pdf/ciisi-eu_practical_example.pdf.

81 Euro Cyber Resilience Board Secretariat, "Cyber Information and Intelligence Sharing: Community Rulebook," Cyber Information Sharing and Intelligence Sharing Initiative, European Central Bank, August 2020, https://www.ecb.europa.eu/paym/groups/euro-cyber-board/shared/pdf/ciisi-eu_community_rulebook.pdf.

82 EU member states currently implementing TIBER-EU: Belgium, Denmark, Finland, Germany, Ireland, Italy, Norway, Romania, Sweden, and the Netherlands.

83 Weuro Jaakko, "Resilience of Financial Market Infrastructure and the Role of the Financial Sector in Countering Hybrid Threats," Presidency Issues Note for the Informal ECOFIN Working Session, September 9, 2019, https://eu2019.fi/documents/11707387/15400298/Hybrid+Threats+Informal+ECOFIN+final+Issues+Note+2019-09-09_S2.pdf/29565728-f476-cbdd-4c5f-7e0ec970c6c4/Hybrid+Threats+Informal+ECOFIN+final+Issues+Note+2019-09-09_S2.pdf.

84 Based on written input received from officials at Singapore's Cyber Security Agency and the Monetary Authority of Singapore on October 16, 2020.

85 Aquiles A. Almansi and Yejin Carol Lee, "Financial Sector's Cybersecurity: A Regulatory Digest," World Bank Group, Financial Sector Advisory Center, November 2019, http://pubdocs.worldbank.org/en/940481575300835196/CybersecDIGEST-NOV2019-FINAL.pdf.

86 Monetary Authority of Singapore, "Technology Risk Management Guidelines," Consultation Paper, March 2019, https://www.mas.gov.sg/-/media/Consultation-Paper-on-Proposed-Revisions-to-Technology-Risk-Management-Guidelines.pdf.

87 "Consultation Paper on Proposed Revisions to Business Continuity Management Guidelines," Monetary Authority of Singapore, March 2019, https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/Consultation-Paper-on-Proposed-Revisions-to-Business-Continuity-Management-Guidelines.pdf.

88 "Minutes of the Federal Open Market Committee" (U.S. Federal Reserve System, January 28, 2020), https://www.federalreserve.gov/monetarypolicy/files/fomcminutes20200129.pdf.

89 FS-ISAC, "FS-ISAC & MAS to Strengthen Cyber Info Sharing Across Nine Countries," Press Release, November 14, 2017, https://www.fsisac.com/newsroom/fs-isac-and-mas-to-strengthen-cyber-information-sharing-across-nine-countries.

90 FS-ISAC, "FS-ISAC Launches the Ceres Forum: World's Premier Threat Information Sharing Group for Central Banks," Reston, Virginia and Singapore, June 11, 2018, https://www.fsisac.com/newsroom/fs-isac-launches-the-ceres-forum-worlds-premier-threat-information-sharing-group-for-central-banks-regulators-and-supervisors; CSA Singapore, "11 CII Sectors Tested on More Complex Cyber Attack Scenarios," September 4, 2019, https://www.csa.gov.sg/news/press-releases/exercise-cyber-star-2019.

91 Federal Reserve System, "Enhanced Cyber Risk Management Standards," Advance Notice of Proposed Rulemaking, Fall 2019, 7100-AE61, Office of Information and Regulatory Affairs,

OMB, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201910&RIN=7100-AE61.

92 Robert Armstrong, Kiran Stacey, and Laura Noonan, "US Banks Face Tighter Scrutiny of Cyber Defences," *Financial Times,* June 17, 2019, https://www.ft.com/content/69a25232-8eaa-11e9-a1c1-51bf8f989972.

93 Federal Reserve System, "Enhanced Cyber Risk Management Standards," Advance Notice of Proposed Rulemaking, Fall 2019, 7100-AE61, Office of Information and Regulatory Affairs, OMB, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201910&RIN=7100-AE61.

94 Randal Quarles, "Speech by Vice Chairman for Supervision Quarles on the Financial Regulatory System and Cybersecurity," Board of Governors of the Federal Reserve System, February 2018, https://www.federalreserve.gov/newsevents/speech/quarles20180226b.htm.

95 Randal Quarles, "Speech by Vice Chairman for Supervision Quarles on the Financial Regulatory System and Cybersecurity," Board of Governors of the Federal Reserve System, February 2018, https://www.federalreserve.gov/newsevents/speech/quarles20180226b.htm.

96 Robert Armstrong, Kiran Stacey, and Laura Noonan, "US Banks Face Tighter Scrutiny of Cyber Defences," *Financial Times,* June 17, 2019, https://www.ft.com/content/69a25232-8eaa-11e9-a1c1-51bf8f989972.

97 Art Lindo, "Oversight of Cyber Resilience in the Financial Regulatory System: Seminar for Senior Bank Supervisors From Emerging Economies."

98 Board of Governors of the Federal Reserve System, "Strategic Plan 2020–23, December 2019," 2019, 20.

99 "Minutes of the Federal Open Market Committee" (U.S. Federal Reserve System, January 28, 2020), https://www.federalreserve.gov/monetarypolicy/files/fomcminutes20200129.pdf.

100 New York State Department of Financial Services, "NYDFS 23 NYCRR 500," 2017, https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.

101 Aquiles A. Almansi and Yejin Carol Lee, "Financial Sector's Cybersecurity: A Regulatory Digest," World Bank Group, Financial Sector Advisory Center, July 2020, http://pubdocs.worldbank.org/en/361881595872293851/CybersecDigest-v5-Jul2020-FINAL.pdf.

102 Aquiles A. Almansi and Yejin Carol Lee, "Financial Sector's Cybersecurity: A Regulatory Digest," World Bank Group, Financial Sector Advisory Center, July 2020, http://pubdocs.worldbank.org/en/361881595872293851/CybersecDigest-v5-Jul2020-FINAL.pdf.

103 Institute for Development and Research in Banking Technology, "Indian Banks—Center for Analysis of Risks and Threats (IB-CART)," last modified September 30, 2020, https://www.idrbt.ac.in/ib-cart.html.

104 Institute for Development and Research in Banking Technology, "Indian Banks—Center for Analysis of Risks and Threats (IB-CART)," last modified September 30, 2020, https://www.idrbt.ac.in/ib-cart.html.

105 Reserve Bank of India, "Financial Stability Report," July 2020, https://www.rbi.org.in/Scripts/FsReports.aspx.

106 "Cyber Threats Against Banking Industry on the Rise in Post Covid-19 Lockdown Phase, Says RBI," *Hindu Business Line,* https://www.thehindubusinessline.com/money-and-banking/cyber-threats-against-banking-industry-on-the-rise-in-post-covid-19-lockdown-phase-says-rbi/article32201404.ece.

107 Reserve Bank of India, "Financial Stability Report," July 2020, https://www.rbi.org.in/Scripts/FsReports.aspx.

108 "CBI to Set Up Cyber-Crime Investigation Branch in Mumbai," *Business Standard,* March 1, 2016, https://www.business-standard.com/article/news-ians/cbi-to-set-up-cyber-crime-investigation-branch-in-mumbai-116030100949_1.html.

109 Rajeev Jayaswal, "Govt Plans Cyber Security System for Financial Sector," *Hindustan Times,* August 18, 2020, https://www.hindustantimes.com/india-news/govt-plans-cyber-security-system/story-bHRwwBeFVGLIrA3VMmOaDO.html.

110 Bank of England, Financial Conduct Authority, and Prudential Regulatory Authority, "Building Operational Resilience: Impact Tolerances for Important Business Services."

111 European Banking Authority, "EBA Guidelines on ICT and Security Risk Management," https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management.
112 "Consultation Paper on Proposed Revisions to Business Continuity Management Guidelines," Monetary Authority of Singapore, March 2019, https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/Consultation-Paper-on-Proposed-Revisions-to-Business-Continuity-Management-Guidelines.pdf.
113 Art Lindo, "Oversight of Cyber Resilience in the Financial Regulatory System: Seminar for Senior Bank Supervisors From Emerging Economies."
114 Global Financial Markets Association, "Response to Bank of England and FCA Discussion Paper on 'Building the UK Financial Sector's Operational Resilience,'" October 2018, https://www.afme.eu/portals/0/globalassets/downloads/consultation-responses/tao-gfma-response-to-bank-of-england-fca-building-uk-financial-resilience-5-oct-2018.pdf.
115 International Organization of Securities Commissions, "About CPMI-IOSCO," accessed July 20, 2020, https://www.iosco.org/about/?subsection=cpmi_iosco.
116 Committee on Payments and Market Infrastructures and The Board of the International Organization of Securities Commissions, "Guidance on Cyber Resilience for Financial Market Infrastructures."
117 Committee on Payments and Market Infrastructures and The Board of the International Organization of Securities Commissions, "Guidance on Cyber Resilience for Financial Market Infrastructures."
118 The Board of the International Organization of Securities Commissions, "Cyber Task Force Final Report," June 2019, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf.
119 Committee on Payments and Market Infrastructures, "Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security," Bank for International Settlements, May 8, 2018, 178, https://www.bis.org/cpmi/publ/d178.htm.
120 "FSB Publishes Stocktake on Cybersecurity Regulatory and Supervisory Practices," October 13, 2017, https://www.fsb.org/2017/10/fsb-publishes-stocktake-on-cybersecurity-regulatory-and-supervisory-practices/.
121 Financial Stability Board, "Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices," October 13, 2017, https://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory-practices/.
122 Financial Stability Board, "FSB Publishes Stocktake on Cybersecurity Regulatory and Supervisory Practices," press release, October 13, 2017, https://www.fsb.org/2017/10/fsb-publishes-stocktake-on-cybersecurity-regulatory-and-supervisory-practices/.
123 Financial Stability Board, "Effective Practices for Cyber Incident Response and Recovery: Consultative Document," April 20, 2020, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document/.
124 Aquiles A. Almansi and Yejin Carol Lee, "Financial Sector's Cybersecurity: A Regulatory Digest," World Bank Group, Financial Sector Advisory Center, November 2019, http://pubdocs.worldbank.org/en/940481575300835196/CybersecDIGEST-NOV2019-FINAL.pdf.
125 Basel Committee on Banking Supervision, "Consultative Document: Principles for Operational Resilience," August 2020, https://www.bis.org/bcbs/publ/d509.pdf.
126 Basel Committee on Banking Supervision, "Consultative Document: Principles for Operational Resilience," August 2020, https://www.bis.org/bcbs/publ/d509.pdf.
127 Bank for International Settlements (BIS), "Cyber Resilience: Range of Practices," December 2018, https://www.bis.org/bcbs/publ/d454.pdf.
128 Committee on Payments and Market Infrastructures, "Payment, Clearing and Settlement Operators Meet on Global Cyber-Resilience," Press Release, September 14, 2018, https://www.bis.org/press/p180914.htm.
129 Committee on Payments and Market Infrastructures and The Board of the International Organization of Securities Commissions, "Guidance on Cyber Resilience for Financial Market Infrastructures," Bank for International Settlements, 2016, http://www.bis.org/cpmi/publ/d138.htm.
130 Bank for International Settlements, "BIS Annual Report 2018/2019," 2019, https://www.bis.org/about/areport/areport2019.pdf#bis2025.

131 Agustin Carstens, "The New BIS Strategy—Bringing the Americas and Basel Closer Together" (Speech, Fourteenth ASBA-BCBS-FSI High-level Meeting on Global and Regional Supervisory Priorities, Lima, 1 October 2019), https://www.bis.org/speeches/sp191001.htm.

132 Bank for International Settlements, "FSI Publications," https://www.bis.org/fsi/publications.htm?m=1%7C17%7C161.

133 Senior officials at the Financial Stability Institute in written correspondence with the authors, May 2020.

134 European Banking Federation, Global Financial Markets Association, and International Swaps and Derivatives Association, "International Cybersecurity, Data and Technology Principles," letter, May 2016, https://www.gfma.org/wp-content/uploads/0/83/197/211/13187d1e-077f-43c5-85a1-1da370608a2b.pdf.

135 Financial Services Sector Coordinating Council, "The Financial Services Sector Cybersecurity Profile," October 25, 2018, https://fsscc.org/files/galleries/Financial_Services_Sector_Cybersecurity_Profile_Overview_and_User_Guide_2018-10-25.pdf.

136 Financial Services Sector Coordinating Council, "The Financial Services Sector Cybersecurity Profile," October 25, 2018, https://fsscc.org/files/galleries/Financial_Services_Sector_Cybersecurity_Profile_Overview_and_User_Guide_2018-10-25.pdf.

137 European Banking Authority, "EBF Response to the EBA Guidelines on ICT and Security Risk Management," accessed July 20, 2020, https://eba.europa.eu/node/82021/submission/62742.

138 Asia Securities Industry & Financial Markets Association (ASIFMA), "Response to Consultation Paper: Proposed Revisions to Guidelines on Business Continuity Management," April 2019, https://www.asifma.org/wp-content/uploads/2019/04/final-asifma-response-to-mas-consultation-paper-on-guidelines-on-business-continuity-management.pdf.

139 SIFMA, "Quantum Dawn V Fact Sheet," accessed January 5, 2020, https://www.sifma.org/wp-content/uploads/2019/11/QuantumDawnV-Factsheet_2019.pdf.

140 FS-ISAC, "FS-ISAC Upcoming Events, Summits, Webinars and Exercises," accessed July 20, 2020, https://www.fsisac.com/events.

141 Chris Keeling, "Waking Shark II Desktop Cyber Exercise: Report to Participants," November 12, 2013, https://www.bba.org.uk/wp-content/uploads/2014/02/Banking_3192106_v_1_Waking-Shark-II-Report-v1.pdf.pdf.

142 Bank of England, "Sector Simulation Exercise: SIMEX 2018 Report," September 27, 2019, https://www.bankofengland.co.uk/report/2019/sector-simulation-exercise-simex-2018-report.

143 Shaun Waterman, "Bank Regulators Briefed on Treasury-Led Cyber Drill," *FedScoop*, July 20, 2016, https://www.fedscoop.com/us-treasury-cybersecurity-drill-july-2016/.

144 Financial Services Information Sharing and Analysis Center, "Exercises Overview," accessed July 20, 2020, https://www.fsisac.com/hubfs/Resources/FS-ISAC_ExercisesOverview.pdf.

145 David Milliken, "U.S. and UK to Test Financial Cyber-Security Later This Month," Reuters, November 2, 2015, https://www.reuters.com/article/us-britain-usa-cybersecurity-idUSKCN0SR1DW20151102.

146 European Central Bank, "UNITAS Crisis Communication Exercise Report," December 2018, https://www.ecb.europa.eu/pub/pdf/other/ecb.unitasreport201812.en.pdf.

147 Leigh Thomas, "G7 Countries to Simulate Cross-Border Cyber Attack Next Month: France," Reuters, May 10, 2019, https://www.reuters.com/article/us-g7-france-cyber-idUSKCN1SG1KZ.

148 Leigh Thomas, "G7 Countries to Simulate Cross-Border Cyber Attack Next Month: France," Reuters, May 10, 2019, https://www.reuters.com/article/us-g7-france-cyber-idUSKCN1SG1KZ.

149 UK National Cyber Security Centre, "Exercise in a Box," 2019, https://exerciseinabox.service.ncsc.gov.uk/

150 Isabel Skierka et al., "CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams," Working Paper, New America and Global Public Policy Institute, May 2015, https://static.newamerica.org/attachments/2943-csirt-basics-for-policy-makers/CSIRT%20Basics%20for%20Policy-Makers%20May%20

2015%20WEB%2009-15.16efa7bcc9e54fe299ba3447a5b7d41e.pdf.

151 GEANT, "TF-CSIRT: Computer Security Incident Response Teams—GÉANT," accessed July 20, 2020, https://www.geant.org:443/People/Community_Programme/Task_Forces/Pages/TF-CSIRT.aspx.

152 Isabel Skierka et al., "CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams," Working Paper, New America and Global Public Policy Institute, May 2015, https://static.newamerica.org/attachments/2943-csirt-basics-for-policy-makers/CSIRT%20Basics%20for%20Policy-Makers%20May%202015%20WEB%2009-15.16efa7bcc9e54fe299ba3447a5b7d41e.pdf.

153 Robert Morgus et al., "National CSIRTs and Their Role in Computer Security Incident Response," New America and Global Public Policy Institute, November 2015, https://d1y8sb8igg2f8e.cloudfront.net/documents/CSIRTs-incident-response.pdf.

154 European Union Agency for Cybersecurity, "NIS Directive Details," https://www.enisa.europa.eu/topics/nis-directive. Accessed September 26, 2020.

155 "FC3—Finance and Cyber Continuity Center: Israel's National Financial CERT," senior officials from the Israeli Ministry of Finance in written correspondence with the authors, April 16, 2020.

156 CERTFin, "CERT Finanziario Italiano (CERTFIN) - RFC 2350," Bank of Italy, https://www.certfin.it/media/pdf/rfc2350.pdf. Accessed September 26, 2020.

157 CERTFin, "CERT Finanziario Italiano (CERTFIN) - RFC 2350," Bank of Italy, https://www.certfin.it/media/pdf/rfc2350.pdf. Accessed September 26, 2020.

158 GEANT, "TF-CSIRT: Computer Security Incident Response Teams - GÉANT," accessed July 20, 2020, https://www.geant.org:443/People/Community_Programme/Task_Forces/Pages/TF-CSIRT.aspx.

159 Finance and Cyber Continuity Center, "FC3—Finance and Cyber Continuity Center: Israel's National Financial CERT," April 16, 2020.

160 "FC3—Finance and Cyber Continuity Center: Israel's National Financial CERT," senior officials from the Israeli Ministry of Finance in written correspondence with the authors, April 16, 2020.

161 "FC3—Finance and Cyber Continuity Center: Israel's National Financial CERT," senior officials from the Israeli Ministry of Finance in written correspondence with the authors, April 16, 2020.

162 "FC3—Finance and Cyber Continuity Center: Israel's National Financial CERT," senior officials from the Israeli Ministry of Finance in written correspondence with the authors, April 16, 2020.

163 "FC3—Finance and Cyber Continuity Center: Israel's National Financial CERT," senior officials from the Israeli Ministry of Finance in written correspondence with the authors, April 16, 2020.

164 Brian F. Tivnan, "Financial System Mapping," November 7, 2018, https://www.mitre.org/publications/technical-papers/financial-system-mapping.

165 Telis Demos, "Banks Build Line of Defense for Doomsday Cyberattack," *Wall Street Journal*, December 3, 2017, https://www.wsj.com/articles/banks-build-line-of-defense-for-doomsday-cyberattack-1512302401.

166 Sheltered Harbor, "Sheltered Harbor - About," accessed July 20, 2020, https://shelteredharbor.org/index.php/about#who.

167 Stacy Cowley, "Banks Adopt Military-Style Tactics to Fight Cybercrime," *New York Times*, May 20, 2018, https://www.nytimes.com/2018/05/20/business/banks-cyber-security-military.html.

168 Rob Nichols, Gregory Baer, Jim Nussle, Kevin Fromer, Steven Silberstein, and Kenneth Bentsen to Financial Institution CEOs, May 14, 2019, https://www.shelteredharbor.org/images/SH/Docs/Sheltered_Harbor_Trade_Assn_Exec_Letter_Genericfinal_051619.pdf.

169 Rob Nichols, Gregory Baer, Jim Nussle, Kevin Fromer, Steven Silberstein, and Kenneth Bentsen to Financial Institution CEOs, May 14, 2019, https://www.shelteredharbor.org/images/SH/Docs/Sheltered_Harbor_Trade_Assn_Exec_Letter_Genericfinal_051619.pdf.

170 Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency, "Joint Statement on Heightened Cybersecurity Risk," January 16, 2020, https://occ.gov/news-issuances/bulletins/2020/bulletin-2020-5a.pdf.

171 U.S. Federal Financial Institutions Examination Council, "Cybersecurity Resource Guide for Financial Institutions," October 2018, https://www.ffiec.gov/press/pdf/FFIEC%20Cybersecurity%20Resource%20Guide%20for%20Financial%20Institutions.pdf.

172 For the purposes of this section, exchanges refer to those that operate in a regulated and secure market, and are distinct from "cryptocurrency exchanges."

173 European Central Bank, "Cyber Resilience Oversight Expectations for Financial Market Infrastructures," December 2018, https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf.

174 Darrell Duffie and Joshua Younger, "Cyber Runs: How a Cyber Attack Could Affect U.S. Financial Institutions," Hutchins Center on Fiscal and Monetary Policy, Brookings Institution, June 2019, https://www.brookings.edu/research/cyber-runs/.

175 World Federation of Exchanges, "WFE Response to the EU Commission's Digital Operational Resilience Framework for Financial Services: Making the EU Financial Sector More Secure," March 2020, https://www.world-exchanges.org/storage/app/media/regulatory-affairs/WFE%20response%20EU%20Consultation%20Digital%20Resilience%20FINAL.pdf.

176 Rohini Tendulkar, "Cyber-Crime, Securities Markets, and Systemic Risk," Joint Staff Working Paper of the IOSCO Research Department and World Federation of Exchanges, July 2013, https://www.world-exchanges.org/storage/app/media/research/Studies_Reports/2013-cyber-crime-securities-markets-amp-systemic-risk.pdf.

177 Rob Stock, "Five Eyes Cybersecurity Agencies Will Be Involved in Fight Against NZX Cyberattackers," *Stuff,* August 29, 2020, https://www.stuff.co.nz/business/122604872/five-eyes-cybersecurity-agencies-will-be-involved-in-fight-against-nzx-cyberattackers.

178 Nish and Naumaan, "The Cyber Threat Landscape: Confronting Challenges to the Financial System."

179 "The Evolving Advanced Cyber Threat to Financial Markets," SWIFT and BAE Systems, 2018, https://www.baesystems.com/en/cybersecurity/feature/the-evolving-advanced-cyber-threat-to-financial-markets.

180 Nish and Naumaan, "The Cyber Threat Landscape: Confronting Challenges to the Financial System."

181 FinCyber Project, "Timeline of Cyber Incidents Involving Financial Institutions," Carnegie Endowment for International Peace, accessed July 20, 2020, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

182 "Consultation Paper on Proposed Revisions to Business Continuity Management Guidelines," Monetary Authority of Singapore, March 2019, https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/Consultation-Paper-on-Proposed-Revisions-to-Business-Continuity-Management-Guidelines.pdf.

183 European Commission, "Executive Summary of the Impact Assessment Accompanying the Document: Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector," Commission Staff Working Document, September 24, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2020:199:FIN.

184 Carmen Reinicke, "3 Reasons One Wall Street Firm Says to Stick With Cloud Stocks Amid the Coronavirus-Induced Market Rout," Business Insider, March 30, 2020, https://markets.businessinsider.com/news/stocks/wedbush-reasons-own-cloud-stocks-coronavirus-pandemic-tech-buy-2020-3-1029045273#2-the-move-to-cloud-will-accelerate-more-quickly-amid-the-coronavirus-pandemic2.

185 Sara Castellanos, "Nasdaq Ramps Up Cloud Move," *Wall Street Journal,* September 15, 2020, https://www.wsj.com/articles/nasdaq-ramps-up-cloud-move-11600206624.

186 Mark Carney, "Enable, Empower, Ensure: A New Finance for the New Economy" (Speech, Mansion House Bankers' and Merchants' Dinner, London, June 20, 2019), http://www.bankofengland.co.uk/speech/2019/mark-carney-speech-at-the-mansion-house-bankers-and-merchants-dinner.

187 Tim Maurer and Garrett Hinck, "Cloud Security: A Primer for Policymakers," Carnegie Endowment for International Peace, August 31, 2020, https://carnegieendowment

.org/2020/08/31/cloud-security-primer-for-policymakers-pub-82597.

188 Buckley LLP, "Democratic Members Request FSOC Designate Cloud Providers as Systemically Important," *InfoBytes Blog*, August 29, 2019, https://www.lexology.com/library/detail.aspx?g=049d5593-658b-4379-835b-9a42bc26758b.

189 White and Williams LLP and Osborne Clarke LLP, "Threat Information Sharing and GDPR: A Lawful Activity That Protects Personal Data," FS-ISAC, 2018, https://www.osborneclarke.com/wp-content/uploads/2019/01/Threat-Information-Sharing-and-GDPR_Final_TLP-WHITE.pdf.

190 Based on input from officials at the European Central Bank.

191 European Central Bank, "Major European Financial Infrastructures Join Forces Against Cyber Threats," February 2020, https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr200227_1~062992656b.en.html.

192 "Exemptions," ICO, May 15, 2020, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/.

193 "Exemptions," ICO, May 15, 2020, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/.

194 Stephanie von Maltzan, "No Contradiction Between Cyber-Security and Data Protection? Designing a Data Protecton Compliant Incident Response System," *European Journal of Law and Technology* 10, no. 1 (May 16, 2019), http://ejlt.org/article/view/665. Also known as IT-Security incidents. Key issues such as information exchange formats and sharing platforms remain on the agenda of the cybersecurity community, especially for incident responders. Incident Response activities require additional processing of personal data, so may themselves create a privacy risk. Current developments towards Incident Response show that systems are increasingly insecure to data breaches, especially due to the massive amounts of personal data and the possibility of linking this data to personal identifiers. Therefore, the joint project ITS. Overview has set itself the goal of creating a detailed overview of IT-Security incidents in different industrial sectors that can be correlated and exchanged among companies to be able to quickly identify cyberattacks. This article aims to offer an initial assessment of data protection measures using Incident Response management. The key problems in this context are legal and technical barriers. The main factors are the possibility of entering free text in Ticketing Systems and the legal obligations for sharing information under the General Data Protection Regulation (GDPR).

195 Financial Stability Board, "Effective Practices for Cyber Incident Response and Recover: Consultative Document," April 20, 2020, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document/.

196 Elise Thomas, Natalie Thompson, and Alicia Wanless, "The Challenges of Countering Influence Operations," Carnegie Endowment for International Peace, June 10, 2020, https://carnegieendowment.org/2020/06/10/challenges-of-countering-influence-operations-pub-82031.

197 Jon Bateman, "Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios," Cybersecurity and the Financial System Working Paper Series, Carnegie Endowment for International Peace, July 2020, https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237.

198 Jim Edwards, "A False Rumor on WhatsApp Started a Run on a London Bank," Business Insider, May 13, 2019, https://www.businessinsider.com/whatsapp-rumour-started-run-on-metro-bank-2019-5.

199 Patrick Collinson Money, "Metro Bank Shares Crash After Loans Blunder Revealed," *Guardian*, January 23, 2019, https://www.theguardian.com/business/2019/jan/23/metro-bank-shares-crash-after-loans-blunder-revealed.

200 Ariel E. Levite, Scott Kannry, and Wyatt Hoffman, "Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance," Carnegie Endowment for International Peace, 2018, https://carnegieendowment.org/files/Cyber_Insurance_Formatted_FINAL_WEB.PDF; Jon Bateman, "War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions," Carnegie Endowment for International Peace, October 5, 2020, https://carnegieendowment.org/2020/10/05/war-terrorism-and-catastrophe-in-cyber-insurance-understanding-and-reforming-exclusions-pub-82819.

Priority #2: International Norms

201 This section includes text from the previously published, short article by Tim Maurer and Michael Schmitt, "Protecting Financial Data in Cyberspace: Precedent for Further Progress on Cyber Norms?," *Just Security* (blog), August 24, 2017, and the Carnegie white paper "Toward a Global Norm Against Manipulating the Integrity of Financial Data" co-authored by Tim Maurer, Ariel Levite, and George Perkovich, released on March 27, 2017.

202 "It's the Economy, Stupid," Wikipedia, https://en.wikipedia.org/wiki/It%27s_the_economy,_stupid.

203 Group-IB, "Group-IB: Cobalt's Latest Attacks on Banks Confirm Connection to Anunak," www.group-ib.com, May 2018, https://www.group-ib.com/media/group-ib-cobalts-latest-attacks-on-banks-confirms-connection-to-anunak/.

204 Nish and Naumaan, "The Cyber Threat Landscape: Confronting Challenges to the Financial System."

205 European Systemic Risk Board, "Systemic Cyber Risk," February 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

206 Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare* (blog), November 9, 2018, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

207 For more details, see Carnegie's "Timeline of Cyber Incidents Involving Financial Institutions," developed in association with BAE Systems: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

208 Tim Maurer et al., "Toward a Global Norm Against Manipulating the Integrity of Financial Data," Carnegie Endowment for International Peace, March 2017, https://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403.

209 Tim Maurer et al., "Toward a Global Norm Against Manipulating the Integrity of Financial Data," Carnegie Endowment for International Peace, March 2017, https://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403.

210 Tim Maurer et al., "Toward a Global Norm Against Manipulating the Integrity of Financial Data," Carnegie Endowment for International Peace, March 2017, https://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403.

211 Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 1st Ecco pbk. ed (New York: Ecco, 2012), 202–3; John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *New York Times*, August 1, 2009, https://www.nytimes.com/2009/08/02/us/politics/02cyber.html.

212 The Ministry of Foreign Affairs of the Russian Federation, "Convention on International Information Security," September 2011, https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.

213 Mark Wells and Nick Fahey, "Charts: Who Loses When the Renminbi Joins the IMF Basket?," CNBC, December 2, 2015, https://www.cnbc.com/2015/12/02/who-loses-when-the-renminbi-joins-the-imf-basket.html.

214 United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," Pub. L. No. A/68/98, A/68/98 (2013), https://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf.

215 Michael Schmitt and Tim Maurer, "Protecting Financial Data in Cyberspace: Precedent for Further Progress on Cyber Norms?," *Just Security* (blog), August 24, 2017, https://www.justsecurity.org/44411/protecting-financial-data-cyberspace-precedent-progress-cyber-norms/.

216 Attorney General Jeremy Wright QC MP, "Cyber and International Law in the 21st Century" (Speech, Chatham House, London, May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

217 Australian Mission to the United Nations, "Australian Paper - Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security," Open Ended Working Group, September 2019, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf.

218 Stef Blok, "Letter to the Parliament on the International Legal Order in Cyberspace From the Government of the Kingdom of the Netherlands to Parliament," July 5, 2019, https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

219 United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174 § (2015), https://undocs.org/A/70/174.

220 Catalin Cimpanu, "All Five Eyes Countries Formally Accuse Russia of Orchestrating NotPetya Attack," *BleepingComputer*, February 18, 2018, https://www.bleepingcomputer.com/news/security/all-five-eyes-countries-formally-accuse-russia-of-orchestrating-notpetya-attack/; Dustin Volz, "U.S. Blames North Korea for 'WannaCry' Cyber Attack," Reuters, December 19, 2017, https://www.reuters.com/article/us-usa-cyber-northkorea-idUSKBN1ED00Q.

221 Open Ended Working Group, "Initial 'Pre-Draft' of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security," 2020, https://www.un.org/disarmament/open-ended-working-group/.

222 Permanent Mission of the Republic of Singapore to the United Nations, "Singapore's Written Comment on the Chair's Pre-Draft of the OEWG Report," Open Ended Working Group, 2020, https://front.un-arm.org/wp-content/uploads/2020/04/singapore-written-comment-on-pre-draft-oewg-report.pdf.

223 David Reid, "New York Stretches Lead Over London as the World's Top Financial Center, Survey Shows," CNBC, September 19, 2019, https://www.cnbc.com/2019/09/19/new-york-beats-london-again-as-the-worlds-top-financial-center.html.

224 Permanent Mission of the Republic of Singapore to the United Nations, "Singapore's Written Comment on the Chair's Pre-Draft of the OEWG Report."

225 Permanent Mission of France to the United Nations, "France's Response to the Pre-Draft Report From the OEWG Chair," Open Ended Working Group, 2020, https://front.un-arm.org/wp-content/uploads/2020/04/contribution-fr-oewg-eng-vf.pdf.

226 U.S. Cyberspace Solarium Commission, "Cyberspace Solarium Commission Final Report," March 2020, https://www.solarium.gov/.

227 Letter by Congressman Royce and Langevin to Secretary Mnuchin, November 5, 2018; Letter by Congressman Royce and Langevin to Secretary Pompeo, November 5, 2018.

228 Letter by the FSSCC to Secretary Mnuchin dated November 19, 2018.

229 Tim Maurer and Arthur Nelson, "COVID-19's Other Virus: Targeting the Financial System," *Strategic Europe* (blog), Carnegie Europe, April 21, 2020, 1, https://carnegieeurope.eu/strategiceurope/81599.

230 Tim Maurer et al., "Toward a Global Norm Against Manipulating the Integrity of Financial Data," Carnegie Endowment for International Peace, March 2017, https://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403.

231 Tim Maurer et al., "Toward a Global Norm Against Manipulating the Integrity of Financial Data," Carnegie Endowment for International Peace, March 2017, https://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403.

232 Tim Maurer et al., "Toward a Global Norm Against Manipulating the Integrity of Financial Data," Carnegie Endowment for International Peace, March 2017, https://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403.

233 Tim Maurer et al., "Toward a Global Norm Against Manipulating the Integrity of Financial Data," Carnegie Endowment for International Peace, March 2017, https://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403.

234 Tim Maurer et al., "Toward a Global Norm Against Manipulating the Integrity of Financial Data," Carnegie Endowment for International Peace, March 2017, https://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403.

235 Carnegie Endowment for International Peace, "Launch Event: Toward a Global Norm Against Manipulating the Integrity of Financial Data," June 19, 2017, accessed October 30, 2020, https://carnegieendowment.org/2017/06/19/launch-toward-global-norm-against-manipulating-integrity-of-financial-data-event-5617.

236 Brad Smith, "The Need for a Digital Geneva Convention," https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

237 Cyber Security Program of the Inter-American Committee against Terrorism, "State of Cybersecurity in the Banking Sector in Latin America and the Caribbean," Organization of American States, 2018, https://www.oas.org/es/sms/cicte/sectorbancarioeng.pdf.

238 "CyberPeace Institute - Home," CyberPeace Institute, accessed February 28, 2020, https://cyberpeaceinstitute.org/.

239 SWIFT, "Customer Security Programme Terms and Conditions," June 30, 2017, https://www2.swift.com/uhbonline/books/public/en_uk/cst_sec_prog_trm_cond/index.htm.

240 Bill Gates, "Bill Gates: Trustworthy Computing," *Wired*, January 17, 2002, https://www.wired.com/2002/01/bill-gates-trustworthy-computing/.

241 Dennis Fisher, "Era Ends With Break Up of Trustworthy Computing Group at Microsoft," ThreatPost, accessed January 14, 2020, https://threatpost.com/era-ends-with-break-up-of-trustworthy-computing-group-at-microsoft/108404/.

242 Paul Beckett and Rebecca Buckman, "Citigroup, Microsoft Will Allow Users to Send Money Transfers - WSJ," *Wall Street Journal*, accessed January 16, 2020, https://www.wsj.com/articles/SB988669484896586123.

243 Craig Mundie et al., "Trustworthy Computing, Microsoft White Paper," Microsoft Corporation, revised version 2002, http://download.microsoft.com/documents/australia/about/trustworthy_comp.doc. *Emphasis added by author.*

Priority #3: Collective Response

244 Saul Hansell, "Citibank Fraud Case Raises Computer Security Questions," *New York Times*, August 19, 1995, https://www.nytimes.com/1995/08/19/business/citibank-fraud-case-raises-computer-security-questions.html.

245 U.S. Federal Bureau of Investigation, "A Byte Out of History: $10 Million Hack," accessed July 20, 2020, https://www.fbi.gov/news/stories/a-byte-out-of-history-10-million-hack.

246 Matthew Noyes, "Countering COVID-19 Related Fraud" (panel discussion, Center for Strategic and International Studies, June 5, 2020), https://www.youtube.com/watch?v=Ms-e-4TFsyI&feature=emb_title.

247 U.S. Department of Justice, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," March 24, 2016, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.

248 "Bangladesh Bank Heist Was 'State-Sponsored': U.S. Official," Reuters, March 29, 2017, https://www.reuters.com/article/us-cyber-heist-philippines/bangladesh-bank-heist-was-state-sponsored-u-s-official-idUSKBN1700TI.

249 U.S. Treasury, "Sanctions Related to Significant Malicious Cyber-Enabled Activities," accessed July 20, 2020, https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx.

250 Europol, "Law Enforcement Agencies Across the EU Prepare for Major Cross-Border Cyber-Attacks," March 2019, https://www.europol.europa.eu/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks.

251 ENISA, "CyLEEx19: Inside a Simulated Cross-Border Cyber-Attack on Critical Infrastructure," October 31, 2019, https://www.enisa.europa.eu/news/enisa-news/test-1.

252 Fabio Panetta, "Protecting the European Financial Sector: The Cyber Information and Intelligence Sharing Initiative," https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200227~7aae128657.en.html.

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

254 Chris Bing, "Project Indigo: The Quiet Info-Sharing Program Between Banks and U.S. Cyber Command," CyberScoop, May 21, 2018, https://www.cyberscoop.com/project-indigo-fs-isac-cyber-command-information-sharing-dhs/.

255 Paul Nakasone, "Statement of General Paul M. Nakasone, Commander, United States Cyber Command, before the Senate Committee on Armed Services" (Hearing on United States Special Operations Command and United States Cyber Command, U.S. Senate, 2019), https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf.

256 "Cybercom Media Roundtable," May 7, 2019, https://www.cybercom.mil/Portals/56/Documents/FOIA%20Reading%20Room%20Docs/2019-05-07_CYBERCOM_Media_Roundtable_Transcript.pdf?ver=2020-01-24-095943-620.

257 Hannah McGrath, "UK Banks to Set Up Cyber Security Centre," FStech, October 19, 2018, https://www.fstech.co.uk/fst/UK_Banks_Insurers_To_Set_Up_Cybersecurity_Centre.php.

258 Katherine Griffiths, "Banks Man the Barricades to See Off Cyberattacks," *The Times*, October 2018, https://www.thetimes.co.uk/article/banks-man-the-barricades-to-see-off-cyberattacks-qz63v5wwk.

259 Moody's, "BoE Releases Findings of Cyber Simulation Exercise in Financial Sector," Moody's Analytics, September 2019, https://www.moodysanalytics.com/regulatory-news/sep-27-19-boe-releases-findings-of-cyber-simulation-exercise-in-financial-sector.

260 ANSSI, "Coopération entre l'Agence Nationale de la Sécurité des Systems d'Information (ANSSI) et ;'Autorité de Contôle Prudentiel (ACPR)," https://www.ssi.gouv.fr/actualite/cooperation-entre-lagence-nationale-de-la-securite-des-systemes-dinformation-anssi-et-lautorite-de-controle-prudentiel-acpr/.

261 Anna Isaac, "U.K. Examines if Cyberattack Triggered London Stock Exchange Outage," *Wall Street Journal,* January 5, 2020, https://www.wsj.com/articles/u-k-examines-if-cyberattack-triggered-london-stock-exchange-outage-11578232800.

262 Jeremy Fleming, "Director GCHQ's Speech at CYBERUK 2019", (CYBERUK 2019, Glasgow, April 24, 2019), https://www.gchq.gov.uk/speech/director-s-speech-at-cyberuk-2019.

263 World Economic Forum, "Recommendations for Public-Private Partnership Against Cybercrime," World Economic Forum, January 2016, http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf; World Economic Forum, "Partnership Against Cybercrime," accessed July 20, 2020, https://www.weforum.org/projects/partnership-against-cybercime/.

264 Third Way, "Announcing the Third Way Cyber Enforcement Initiative," October 29, 2018, https://www.thirdway.org/memo/announcing-the-third-way-cyber-enforcement-initiative.

265 Juan Zarate and Tim Maurer, "Protecting the Financial System Against the Coming Cyber Storms," *Hill*, May 18, 2020, https://thehill.com/opinion/cybersecurity/498244-protecting-the-financial-system-against-the-coming-cyber-storms.

266 Joyce Hakmeh and Allison Peters, "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet," Council on Foreign Relations, January 13, 2020, https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.

267 U.S. Federal Bureau of Investigation, "A Byte Out of History."

268 Europol, "Joint Cybercrime Action Taskforce (J-CAT)," accessed July 22, 2020, https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce.

269 Tuesday Reitano, Troels Oerting, and Marcena Hunter, "Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce (J-CAT)," Studying Group on Organised Crime, 2015, https://standinggroups.ecpr.eu/sgoc/innovations-in-international-cooperation-to-counter-cybercrime-the-joint-cybercrime-action-taskforce-j-cat/.

270 Founding institutions include Barclays, Standard Chartered, Deutsche Bank, and Banco Santander. Other members now include Bank of Ireland, Allied Irish Banks, Lloyds Banking Group, and Metro Bank. See, "Banks Join Forces to Crack Down on Fraudsters," *Financial Times*, August 8 2017, https://www.ft.com/content/6c9030ca-7937-11e7-90c0-90a9d1bc9691.

271 Europol, "The Cyber Defence Alliance and Europol Step Up Cooperation in the Fight Against Fraudsters," October 2018, https://www.europol.europa.eu/newsroom/news/cyber-defence-alliance-and-europol-step-cooperation-in-fight-against-fraudsters.
272 Cheri McGuire, A True Risk "Partner," interview by Corporate Counsel Business Journal, March 2, 2018, https://ccbjournal.com/articles/true-risk-partner.
273 Bill Nelson, "FS-ISAC Testimony Before the Committee on Banking, Housing and Urban Affairs" (Hearing on Cybersecurity: Risks to Financial Services Industry and Its Preparedness, U.S. Senate, 2019), https://www.fsisac.com/hubfs/Resources/FS-ISAC-Testimony_BillNelson-2018-FIN.pdf.
274 FS-ISAC, "About FS-ISAC," accessed July 28, 2018, https://www.fsisac.com/about.
275 FS-ISAC, "CERES Forum Marks One-Year Anniversary With 10th Country Addition," July 10, 2019, https://www.fsisac.com/newsroom/ceres_forum_one_year.
276 FS-ISAC and Monetary Authority of Singapore, "FS-ISAC and MAS Establish Asia Pacific (APAC) Intelligence Centre for Sharing and Analysing Cyber Threat Information," Press Release, December 1, 2016, https://www.nas.gov.sg/archivesonline/data/pdf-doc/20161201006/Media%20Release_FS-ISAC%20and%20MAS%20Establish%20Asia%20Pacific%20%28APAC%29%20Intelligence%20Centre%20for%20sharing%20and%20analysing%20cyber%20threat%20information%20%28SGPC%29.pdf.
277 FS-ISAC, "About FS-ISAC," accessed July 28, 2018, https://www.fsisac.com/about.
278 FS-ISAC, "CERES Forum Marks One-Year Anniversary With 10th Country Addition."
279 FS-ISAC, "FS-ISAC and CSA Partner to Enhance Cybersecurity in Singapore," Press Release, July 18, 2018, https://www.fsisac.com/newsroom/fs-isac-and-csa-partner-to-enhance-cybersecurity-in-singapore.
280 FS-ISAC, "FS-ISAC and Europol Partner to Combat Cross-Border Cybercrime," Press Release, September 19, 2019, https://www.fsisac.com/newsroom/fsisac-europol-mou.
281 "About FS-ISAC," FS-ISAC, accessed July 28, 2018, https://www.fsisac.com/about.
282 U.S. Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," April 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.
283 Executive Office of the President, "National Cyber Strategy for the United States of America," September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
284 U.S. Department of State, "Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats," U.S. Department of State, May 31, 2018, https://www.state.gov/s/cyberissues/eo13800/282011.htm.
285 U.S. Department of State, "Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats," U.S. Department of State, May 31, 2018, https://www.state.gov/s/cyberissues/eo13800/282011.htm.
286 U.S. Department of State, "Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats," May 31, 2018, https://www.state.gov/s/cyberissues/eo13800/282011.htm.
287 "Joint Statement on Advancing Responsible State Behavior in Cyberspace," U.S. Department of State, September 23, 2019, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.
288 For more details see Uri Friedman, "Smart Sanctions: A Short History," April 23, 2012, https://foreignpolicy.com/2012/04/23/smart-sanctions-a-short-history/; and John Ikenberry, "Smart Sanctions: Targeting Economic Statecraft," September 2002, https://www.foreignaffairs.com/reviews/capsule-review/2002-09-01/smart-sanctions-targeting-economic-statecraft.
289 Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (Public Affairs, 2013).
290 Barack Obama, "Executive Order 13694 of April 1, 2015, Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," 2015, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf.
291 U.S. Department of the Treasury, "Treasury Targets Supporters of Iran's Islamic Revolutionary Guard Corps and Networks Responsible for Cyber-Attacks Against the United States," Press Release, September 14, 2017, https://www.treasury.gov/press-center/press-releases/Pages/sm0158.aspx.

292 U.S. Department of the Treasury, "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups | U.S. Department of the Treasury," Press Release, September 19, 2019, https://home.treasury.gov/news/press-releases/sm774; U.S. Department of the Treasury, "Treasury Targets North Korea for Multiple Cyber-Attacks," Press Release, September 14, 2017, https://home.treasury.gov/news/press-releases/sm473.

293 U.S. Department of the Treasury, "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware."

294 Katriina Härmä and Tomáš Minárik, "European Union Equipping Itself Against Cyber Attacks With the Help of Cyber Diplomacy Toolbox," *NATO Cooperative Cyber Defence Centre of Excellence* (blog), accessed July 20, 2020, https://ccdcoe.org/incyder-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/.

295 European Union, "Implementing Regulation (EU) 2019/796 Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union of Its Member States," Official Journal of the European Union, July 30, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020R1125&from=EN.

296 "Cyber-attacks: Council Is Now Able to Impose Sanctions," Council of the European Union, May 17, 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/.

297 "EU Imposes the First Ever Sanctions Against Cyber-Attacks," Council of the European Union, July 30, 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

298 In the United States, the U.S. Department of the Treasury has taken aim at Iranian targets engaged in distributed denial of service attacks against financial institutions, North Korean actors targeting cryptocurrency exchanges and ATMs to generate revenue, and Chinese actors engaged in money-laundering on behalf of North Korean groups. The European Union's action targeted a North Korean company for aiding in cyberattacks affecting the Polish Financial Supervision Authority, Bangladesh Bank, and Vietnam Tien Phong Bank. See, "Treasury Targets Supporters of Iran's Islamic Revolutionary Guard Corps and Networks Responsible for Cyber-Attacks Against the United States," U.S. Department of the Treasury, September 14, 2017, https://www.treasury.gov/press-center/press-releases/Pages/sm0158.aspx; "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups," U.S. Department of the Treasury, September 13, 2019, https://home.treasury.gov/news/press-releases/sm774; "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group," U.S. Department of the Treasury, March 2, 2020, https://home.treasury.gov/news/press-releases/sm924; Council Implementing Regulation (EU) 2020/1125 of July 30, 2020, implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 2020 O.J. (246) 4, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020R1125&from=EN.

299 Dursun Peksen, "When Do Imposed Economic Sanctions Work? A Critical Review of the Sanctions Effectiveness Literature," *Defence and Peace Economics* 30, no. 6 (May 2019): 635–47, https://doi.org/10.1080/10242694.2019.1625250.

300 For a specific overview on the use of sanctions for deterring financial motivated cyber crime, see Zachary K. Goldman and Damon McCoy, "Economic Espionage: Deterring Financially Motivated Cybercrime," *Journal of National Security Law & Policy* 8, no. 3 (July 2016): 595–619, https://jnslp.com/wp-content/uploads/2017/10/Deterring-Financially-Motivated-Cybercrime_2.pdf.

301 This categorization builds upon the scholarship of Garrett Hinck and Tim Maurer regarding the purposes of criminal charges against malicious cyber actors. Garrett Hinck and Tim Maurer, "Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity," *Journal of National Security Law and Policy* 10, no. 3 (2020): 531–4, https://jnslp.com/wp-content/uploads/2020/05/Criminal-Charges-as-a-Response-to-Nation-State-Malicious-Cyber-Activity.pdf.

302 Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/17): 56, https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266; for general background, see also Daniel Drezner, "Targeted Sanctions in a

World of Global Finance," *International Interactions* 41, no. 4 (2015): 760–1, https://doi.org/10.1080/03050629.2015.1041297; Henry Farrell and Abraham L. Newman, "Weaponized Interdependence," *International Security* 44, no. 1 (Summer 2019): 65–70, https://doi.org/10.1162/isec_a_00351.

303 Ibid, 76; Peter D. Feaver and Eric Lorber, "Coercive Diplomacy and the New Financial Levers: Evaluating the Intended and Unintended Consequences of Financial Sanctions," Legatum Institute, November 2010, 46–47, https://lif.blob.core.windows.net/lif/docs/default-source/publications/2010-publications-coercive-diplomacy.pdf?Status=Temp&sfvrsn=2. "Chinese Banks Urged to Switch Away From SWIFT as U.S. Sanctions Loom," Reuters, July 29, 2020, https://www.reuters.com/article/us-china-banks-usa-sanctions/chinese-banks-urged-to-switch-away-from-swift-as-u-s-sanctions-loom-idUSKCN24U0SN.

304 Brian Krebs, "U.S. Secret Service: 'Massive Fraud' Against State Unemployment Insurance Programs — Krebs on Security," *KrebsOnSecurity* (blog), May 16, 2020, https://krebsonsecurity.com/2020/05/u-s-secret-service-massive-fraud-against-state-unemployment-insurance-programs/.

305 BAE Systems, "Follow the Money: Understanding the Money Laundering Techniques That Support Large-Scale Cyber-Heists," 2020, https://www.swift.com/sites/default/files/files/swift_bae_report_Follow-The%20Money.pdf.

306 Shannon Vavra, "Secret Service Merging Electronic and Financial Crime Task Forces to Combat Cybercrime," CyberScoop, July 9, 2020, https://www.cyberscoop.com/secret-service-reorganization-task-force-cybercrime-financial-crime/.

307 United States Secret Service, "Secret Service Announces the Creation of the Cyber Fraud Task Force," Press Release, July 9, 2020, https://www.secretservice.gov/data/press/releases/2020/20-JUL/Secret-Service-Cyber-Fraud-Task-Force-Press-Release.pdf.

308 UK Finance, "Staying Ahead of Cyber Crime," April 2018, https://www.ukfinance.org.uk/system/files/Staying-ahead-of-cyber-crime.pdf.

309 Salim Hasham, Shoan Joshi, and Daniel Mikkelsen, "Financial Crime and Fraud in the Age of Cybersecurity," McKinsey & Company, October 2019.

310 "FinCEN Realigns Division to Increase Strategic Capabilities," Financial Crimes Enforcement Network, November 25, 2019, https://www.fincen.gov/news/news-releases/fincen-realigns-division-increase-strategic-capabilities.

311 "Public Safety Committee on Jan. 28th, 2019," Open Parliament, January 28, 2019, https://openparliament.ca/committees/public-safety/42-1/145/?page=2.

312 Fajar Pebrianto, "PPATK Probes Alleged Money Laundering in Skimming Case," *Dukung Indepensi Tempo,* March 2018, 18, https://en.tempo.co/read/916736/ppatk-probes-alleged-money-laundering-in-bri-skimming-case.

313 Tracfin, "Tracfin Annual Report 2018," Ministère de l'Action et des Comptes Publics, 2018, https://www.economie.gouv.fr/files/files/directions_services/tracfin/Rapport%20Activit%C3%A9%20_2018_Ang.pdf.

314 Financial Intelligence Centre, "Annual Report 2018/19," July 31, 2019, https://www.masthead.co.za/wp-content/uploads/2019/11/FIC-Annual-Report-2018-2019.pdf.

315 U.S. Department of the Treasury, "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware," Press Release, December 5, 2019, https://home.treasury.gov/news/press-releases/sm845.

316 National Police Agency, "Annual Report 2019," Government of Japan, 2019, https://www.npa.go.jp/sosikihanzai/jafic/en/nenzihokoku_e/data/jafic_2019e.pdf.

317 Anton Moiseienko and Olivier Kraft, "From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime," Royal United Services Institute, November 2018, https://rusi.org/sites/default/files/20181129_from_money_mules_to_chain-hopping_web.pdf.

318 Anton Moiseienko and Olivier Kraft, "From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime," Royal United Services Institute, November 2018, https://rusi.org/sites/default/files/20181129_from_money_mules_to_chain-hopping_web.pdf.

319 Directive (EU) 2018/1673 of the European Parliament and of the Council on combating money laundering by criminal law, October 23, 2018, https://eur-lex.europa.eu/eli/dir/2018/1673/oj.

Priority #4: Cybersecurity Workforce Challenges

320 "Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)2 Cybersecurity Workforce Study 2019," 2019, https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7.

321 Sabine Lautenschläger, "Towards a More Cyber Secure Financial System: The Role of Central Banks" (Speech, G7 2019 conference on "Cybersecurity: Coordinating Efforts to Protect the Financial Sector in the Global Economy", Paris, May 10, 2019), https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190510_1~5803aca48c.en.html.

322 Financial Stability Board, "Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices."

323 Financial Services Sector Coordinating Council, "The Financial Services Sector Cybersecurity Profile," October 25, 2018, https://fsscc.org/files/galleries/Financial_Services_Sector_Cybersecurity_Profile_Overview_and_User_Guide_2018-10-25.pdf.

324 For more details, see: "Timeline of Cyber Incidents Involving Financial Institutions," Carnegie Endowment for International Peace, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

325 Cynet, "2020 Cybersecurity Salary Survey Results," 2020, https://go.cynet.com/hubfs/2020-Salary-Survey-Report.pdf.

326 Aspen Cybersecurity Group, "Principles for Growing and Sustaining the Nation's Cybersecurity Workforce," Aspen Institute, November 2018.

327 ITWeb Africa, "Internships Key to Addressing Cyber Security 'Brain Drain,'" *ITWeb Africa* (blog), July 18, 2019, https://itweb.africa//content/Kjlyr7w1NGAqk6am.

328 Paul Makin, interview by authors, January 2020.

329 Robyn Ziegler, "Zurich Insurance Launches Cyber Security Apprenticeship to Address Growing Demand for Cyber Security Professionals," Zurich Insurance Group, September 18, 2018, https://www.zurichna.com/about/news/news-releases/2018/zurich-insurance-launches-cyber-security-apprenticeship.

330 iQ4 Corp., "IQ4 Corp. Launches Virtual Apprenticeship Challenge With Global Public, Private and Educational Sector Backing to Create Skilled and Qualified Cyber-Savvy Workforce," Press Release, Markets Insider, October 8, 2019, https://markets.businessinsider.com/news/stocks/iq4-corp-launches-virtual-apprenticeship-challenge-with-global-public-private-and-educational-sector-backing-to-create-skilled-and-qualified-cyber-savvy-workforce-1028584152.

331 Melana Carollo, "JPMorgan Chase Donates $150,000 to University of South Florida Cybersecurity Center," *Tampa Bay Times*, February 25, 2019, https://www.tampabay.com/business/jpmorgan-chase-donates-150000-to-university-of-south-florida-cybersecurity-center-20190225/.

332 Capital One, "Capital One Launches $500,000 Grant Program to Build Workforce Technology Skills," Press Release, January 22, 2015, https://www.3blmedia.com/News/Capital-One-Launches-500000-Grant-Program-Build-Workforce-Technology-Skills.

333 "Top Companies Team Up With Federal Agencies and Nonprofit to Launch First-of-its-kind Cyber Talent Initiative to Protect Against Cyberattacks," *Partnership for Public Service* (blog), April 8, 2019, accessed March 9, 2020, https://ourpublicservice.org/publications/cybersecurity-talent-initiative-launch/.

334 US Bank, "U.S. Bank Announces 2018 Cybersecurity Scholarship Recipients," Press Release, November 13, 2018, https://www.usbank.com/newsroom/stories/us-bank-announces-2018-cybersecurity-scholarship-recipients.html.

335 Lauren Weber, "Why Companies Are Failing at Reskilling," *Wall Street Journal,* April 19, 2019, https://www.wsj.com/articles/the-answer-to-your-companys-hiring-problem-might-be-right-under-your-nose-11555689542.

336 Barclays, "Barclays Partners With Cyber Security Challenge UK to Attract Cyber Talent | Barclays," Press Release, July 2018, https://home.barclays/news/press-releases/2018/07/barclays-partners-with-cyber-security-challenge-uk-to-attract-cy/.

337 Eileen Yu, "Singapore Banks Offered $21M in Funds to Boost Cybersecurity Capabilities," ZDNet, accessed January 6, 2020, https://www.zdnet.com/article/singapore-banks-offered-21m-in-funds-to-boost-cybersecurity-capabilities/.

338 This section is based on a memo written by Laura Bate for Carnegie's FinCyber Working Group on Cybersecurity Workforce.
339 Justin Falk, "Comparing the Compensation of Federal and Private-Sector Employees, 2011 to 2015," U.S. Congressional Budget Office, April 2017.
340 Partnership for Public Service and Booz Allen Hamilton, "Cyber In-Security II: Closing the Federal Talent Gap," April 2015, https://ourpublicservice.org/wp-content/uploads/2015/04/5a6ae63596cc99f7039b9e409c70891a-1429280031.pdf#page=26.
341 (ISC)2, "Hiring and Retaining Top Cybersecurity Talent," (ISC)2, 2018, https://www.isc2.org/-/media/Files/Research/ISC2-Hiring-and-Retaining-Top-Cybersecurity-Talent.ashx#page=11.
342 ISACA, "State of Cyber 2020, Part 1: Workforce Efforts and Resources," ISACA, 2020, https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpsc201.
343 Center for Strategic and International Studies, "Hacking the Skills Shortage Report," McAfee, 2016, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf#page=12.
344 Rachel Thomas et al., "Women in the Workplace," McKinsey & Company & LeanIn.org, 2019, 10, https://wiw-report.s3.amazonaws.com/Women_in_the_Workplace_2019.pdf#page=10.
345 Megan Caposell, Chris Paris, and Matt Isnor, "Interagency Federal Cyber Career Pathways Initiative" (NICE 2019 Conference & Expo, Phoenix, Arizona, November 16, 2019), https://niceconference.org/uploads/2019/InteragencyFederalCyberCareerPathwaysInitiative.pdf; NICE, "Cybersecurity Career Pathway," CyberSeek, accessed July 22, 2020, https://www.cyberseek.org/pathway.html.
346 Gary C. Peters, "Federal Rotational Cyber Workforce Program Act of 2019," Pub. L. No. S. 406 (2019), https://www.congress.gov/116/bills/s406/BILLS-116s406rfh.pdf.
347 National Security Agency, "Development Programs," accessed July 22, 2020, https://www.intelligencecareers.gov/nsa/nsadevprograms.html.
348 National Security Agency.
349 Jackson Barnett, "'Rigid' Pay System Blamed for Federal Cyber Reskilling Academy Struggles," FedScoop, January 22, 2020, https://www.fedscoop.com/cyber-reskilling-federal-workers/.
350 CIO Council, "Federal Cyber Reskilling Academy," CIO.gov, accessed July 22, 2020, https://www.cio.gov/programs-and-events/reskilling/.
351 Center for Strategic and International Studies, "Hacking the Skills Shortage Report," McAfee, 2016, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf#page=12.
352 North Carolina Department of Information Technology, "Five Veterans Graduate From Cybersecurity Apprenticeship; 10 Vets to Join Program," *NC DIT* (blog), November 15, 2018, https://it.nc.gov/blog/2018/11/15/five-veterans-graduate-cybersecurity-apprenticeship-10-vets-join-program.
353 Jacqueline Thomsen, "Dem Introduces Bill to Create Federal Cybersecurity Apprenticeship Program," *Hill*, September 13, 2018, https://thehill.com/policy/cybersecurity/406577-dem-introduces-bill-to-create-federal-cybersecurity-apprenticeship.
354 Jon Ashton, "Cyber Apprenticeship Scheme: Open for Applications," *Government Security* (blog), May 3, 2018, https://securityprofession.blog.gov.uk/2018/05/03/cyber-apprenticeship-scheme-open-for-applications/.
355 Chief Information Officer of the U.S. Department of Defense, "DoD Cyber Excepted Service (CES) Personnel System," accessed July 22, 2020, https://dodcio.defense.gov/Cyber-Workforce/CES.aspx.
356 Mark Cancian, "Blue-Haired Soldiers? Just Say No," *War on the Rocks* (blog), January 18, 2018, https://warontherocks.com/2018/01/blue-haired-soldiers-just-say-no/.
357 AustCyber, "About Us," accessed July 22, 2020, https://www.austcyber.com/about-us.
358 Cybersecurity Talent Initiative, "About," accessed July 22, 2020, https://cybertalentinitiative.org/about/.
359 Office of the Under Secretary of Defense for Acquisition and Sustainment, "Public-Private Talent Exchange (PPTE) Program," accessed July 22, 2020, http://www.hci.mil/dodcareers.html.

360 U.S. Government Accountability Office, "Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas," High-Risk Series (U.S. Government Accountability Office, March 6, 2019), https://www.gao.gov/highrisk/govwide_security_clearance_process/why_did_study.
361 National Initiative for Cybersecurity Education (NICE), "The NICE Cybersecurity Workforce Framework," U.S. National Institute for Standards and Technology, August 2017, https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center/current.
362 Based on input from senior officials at the Bank of England.
363 Based on input from senior officials at the Bank of England.
364 Based on input from officials at the Monetary Authority of Singapore.
365 Monetary Authority of Singapore, "New S$30 Million Grant to Enhance Cybersecurity Capabilities in Financial Sector," Press Release, December 3, 2018, https://www.mas.gov.sg/news/media-releases/2018/new-30-million-grant-to-enhance-cybersecurity-capabilities-in-financial-sector.
366 Monetary Authority of Singapore, "Landmark Partnership to Level Up Skills for Singaporeans to Seize FinTech Jobs," Press Release, November 16, 2017, https://www.mas.gov.sg/news/media-releases/2017/landmark-partnership-to-level-up-skills-for-singaporeans-to-seize-fintech-jobs.
367 FS-ISAC, "FS-ISAC & MAS to Strengthen Cyber Info Sharing Across Nine Countries."
368 Monetary Authority of Singapore, "Annual Report 2008/2009," Monetary Authority of Singapore, 2009, https://www.mas.gov.sg/annual_reports/annual20082009/56_pro.html.
369 Based on input from Italian financial authorities.
370 Bank for International Settlements (BIS), "Cyber Resilience: Range of Practices."
371 This section is based on conversations with central bank officials, including officials from the Bank of England, the Italian Financial Authorities, and the European Central Bank.
372 Based on conversations with central bank officials, including officials from the Bank of England, the Italian Financial Authorities, and the European Central Bank.
373 Lyndon Nelson (Bank of England), interview by the authors, May 2020.
374 Based on conversations with central bank officials, including officials from the Bank of England, the Italian Financial Authorities, and the European Central Bank.
375 Based on input from officials at the European Central Bank.
376 Based on input from former officials at the Reserve Bank of India.
377 Based on conversations with central bank officials, including officials from the Bank of England, the Italian Financial Authorities, and the European Central Bank.
378 Mirko Hohmann, Alexander Pirang, and Thorsten Benner, "Advancing Cybersecurity Capacity Building," Global Public Policy Institute, March 2017, https://www.gppi.net/media/Hohmann__Pirang__Benner__2017__Advancing_Cybersecurity_Capacity_Building.pdf.
379 Global Cyber Security Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations," University of Oxford, May 31, 2016, https://gcscc.web.ox.ac.uk/files/cmmrevisededition090220171pdf.
380 Mirko Hohmann, Alexander Pirang, and Thorsten Benner, "Advancing Cybersecurity Capacity Building."
381 Global Cybersecurity Capacity Program, "Lessons Learned and Recommendations Towards Strengthening the Program," World Bank Group, 2019, http://documents1.worldbank.org/curated/en/947551561459590661/pdf/Global-Cybersecurity-Capacity-Program-Lessons-Learned-and-Recommendations-towards-Strengthening-the-Program.pdf.
382 Norwegian Institute of International Affairs, "Cybersecurity Capacity Building," 2015, http://nupi_eng/About-NUPI/Projects-centers/Cybersecurity-Capacity-Building.
383 Zine Homburger, "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace," *Global Society* 33, no. 2 (April 3, 2019): 224–42, https://doi.org/10.1080/13600826.2019.1569502.
384 United Nations Office on Drugs and Crime, "Global Programme on Cybercrime," accessed July 22, 2020, http://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html; World Bank Group, "Combatting Cybercrime," accessed July 22, 2020,

http://www.combattingcybercrime.org/; World Bank Group and United Nations and International Bank for Reconstitution and Development, "Combatting Cybercrime: Tools and Capacity Building for Emerging Economies," 2017, http://documents1.worldbank.org/curated/en/355401535144740611/pdf/129637-WP-PUBLIC-worldbank-combating-cybercrime-toolkit.pdf.

385 United Nations Institute for Disarmament Research, "UNIDIR Cyber Policy Portal," Cyber Policy Portal, accessed July 22, 2020, https://cyberpolicyportal.org/en/; "Cybersecurity for Financial Inclusion: Framework & Risk Guide," Alliance for Financial Inclusion, October 2019, https://www.afi-global.org/sites/default/files/publications/2019-11/AFI_GN37_DFS_AW_digital_0.pdf.

386 Amazon Web Services, Inc., "AWS Educate," accessed July 22, 2020, https://aws.amazon.com/education/awseducate/.

387 World Economic Forum, "Partnership Against Cybercrime," accessed July 20, 2020, https://www.weforum.org/projects/partnership-against-cybercime/.

388 Third Way, "Announcing the Third Way Cyber Enforcement Initiative," October 29, 2018, https://www.thirdway.org/memo/announcing-the-third-way-cyber-enforcement-initiative.

389 Committee on Payments and Market Infrastructures and The Board of the International Organization of Securities Commissions, "Guidance on Cyber Resilience for Financial Market Infrastructures. "

390 David Lipton, "Cybersecurity Threats Call for a Global Response," *IMF Blog* (blog), January 13, 2020, https://blogs.imf.org/2020/01/13/cybersecurity-threats-call-for-a-global-response/.

391 Financial Stability Board, "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices"; Financial Stability Board, "Cyber Lexicon."

392 Bank for International Settlements (BIS), "Cyber Resilience: Range of Practices."

393 World Bank, "Financial Sector Cyber Resilience Workshop" (Workshop, Mexico City, November 6, 2019), https://www.worldbank.org/en/events/2019/11/06/financial-sector-cyber-resilience-workshop.

394 Cyber Security Program of the Inter-American Committee against Terrorism, "State of Cybersecurity in the Banking Sector in Latin America and the Caribbean."

395 FinCyber Project, "Cyber Resilience and Financial Organizations: A Capacity-Building Tool Box," Carnegie Endowment for International Peace, accessed July 22, 2020, https://carnegieendowment.org/specialprojects/fincyber/guides.

396 Global Cyber Alliance, "Cybersecurity Toolkit for Small Business," accessed July 22, 2020, https://www.globalcyberalliance.org/gca-cybersecurity-toolkit/.

397 "Customer Security Programme (CSP)," SWIFT, accessed July 22, 2020, https://www.swift.com/myswift/customer-security-programme-csp.

398 Cyber Risk Insitute, "About Cyber Risk Institute," accessed July 22, 2020, https://cyberriskinstitute.org/about/.

399 FS-ISAC, "FS-ISAC Summits," accessed July 22, 2020, https://www.fsisac.com/events#summits.

400 Amazon Web Services, Inc., "AWS Education," accessed July 22, 2020, https://aws.amazon.com/education/awseducate/.

401 United Nations Institute for Disarmament Research, "UNIDIR Cyber Policy Portal."

402 UN Office for Disarmament Affairs, "CyberDiplomacy," accessed July 22, 2020, https://cyberdiplomacy.disarmamenteducation.org/home/.

403 United Nations Office for Disarmament Affairs, "Developments in the Field of Information and Telecommunications in the Context of International Security," UN.org, accessed July 22, 2020, https://www.un.org/disarmament/ict-security/.

404 OSCE, "Cyber/ICT Security," accessed July 22, 2020, https://www.osce.org/cyber-ict-security.

405 Organization of American States, "Cyber Security," OAS.org, accessed July 22, 2020, https://www.oas.org/en/topics/cyber_security.asp.

406 NATO Cooperative Cyber Defence Centre of Excellence, "ASEAN Regional Forum Reaffirming the Commitment to Fight Cyber Crime," accessed July 22, 2020, https://ccdcoe.org/incyder-articles/asean-regional-forum-reaffirming-the-commitment-to-fight-cyber-crime/.

407 Global Forum on Cyber Expertise, "Cybil Portal," accessed July 22, 2020, https://cybilportal.org/.
408 Microsoft, "Cyber Crime & Security Content Hub," accessed July 22, 2020, https://www.microsoft.com/en-us/cybersecurity/content-hub; "CyberPeace Institute - Home."
409 DiploFoundation, "Cybersecurity," accessed July 22, 2020, https://www.diplomacy.edu/cybersecurity.
410 ICT4Peace, "Promotion of a Secure and Peaceful Cyberspace," June 1, 2016, https://ict4peace.org/what-we-do/.
411 United Nations Office on Drugs and Crime, "Cybercrime," accessed July 22, 2020, https://www.unodc.org/unodc/en/cybercrime/index.html.
412 World Bank Group, "Combatting Cybercrime."
413 Council of Europe, "Worldwide Capacity Building," accessed July 22, 2020, https://www.coe.int/en/web/cybercrime/capacity-building-programmes.
414 Europol, "Training and Capacity Building," accessed July 22, 2020, https://www.europol.europa.eu/activities-services/services-support/training-and-capacity-building.
415 INTERPOL, "Capacity Building Projects," accessed July 22, 2020, https://www.interpol.int/en/How-we-work/Capacity-building/Capacity-building-projects.
416 African Union, "First African Forum on Cybercrime" (Addis Ababa, October 16, 2018), https://au.int/en/newsevents/20181016/first-african-forum-cybercrime.
417 The National Cyber-Forensics and Training Alliance, "NCFTA," accessed July 22, 2020, https://www.ncfta.net/.
418 Anomali Inc, "Cyber Defence Alliance (CDA) Partners With Anomali to Better Enable Sharing of Threat Intelligence Among Banking Members," GlobeNewswire News Room, March 5, 2020, http://www.globenewswire.com/news-release/2020/03/05/1995533/0/en/Cyber-Defence-Alliance-CDA-partners-with-Anomali-to-better-enable-sharing-of-Threat-Intelligence-among-banking-members.html.
419 Chris Bing, "Project Indigo: The Quiet Info-Sharing Program Between Banks and U.S. Cyber Command," CyberScoop, May 21, 2018, https://www.cyberscoop.com/project-indigo-fs-isac-cyber-command-information-sharing-dhs/.
420 "Cybersecurity for Financial Inclusion: Framework & Risk Guide," Alliance for Financial Inclusion, October 2019, https://www.afi-global.org/sites/default/files/publications/2019-11/AFI_GN37_DFS_AW_digital_0.pdf.
421 UNSGSA Fintech Sub-Group, "Briefing on Cybersecurity," United Nations Secretary-General's Special Advocate for Inclusive Finance for Development, 2017, https://www.unsgsa.org/files/2815/3575/0134/Cybersecurity.pdf.
422 World Economic Forum, "World Economic Forum Convenes New Consortium to Address Fintech Cybersecurity," March 6, 2018, https://www.weforum.org/press/2018/03/world-economic-forum-convenes-new-consortium-to-address-fintech-cybersecurity/.
423 Nicholas Nhede, "Cybersecurity Innovation: Enel, Mastercard Announce a New Lab in Israel," *Smart Energy International* (blog), May 15, 2020, https://www.smart-energy.com/industry-sectors/cybersecurity/enel-mastercard-announce-a-new-cybersecurity-innovation-lab-in-israel/.
424 Citi, "Global Citizenship Report," 2018, https://www.citigroup.com/citi/about/citizenship/download/Global-Citizenship-Report-2018.pdf.
425 Foreign, Commonwealth & Development Office, "UIK Commonwealth Chair-in-Office Report 2018-2020," September 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/916018/UK-Commonwealth-Chair-in-Office-Report-2018-2020.pdf.
426 Monetary and Capital Markets Department, "Technical Assistance Annual Report 2018," International Monetary Fund, 2018, https://www.imf.org/en/Publications/Technical-Assistance-Annual-Reports/Issues/2018/10/12/technical-assistance-annual-report-2018.
427 Monetary and Capital Markets Department, "Technical Assistance Annual Report 2018," International Monetary Fund, 2018, https://www.imf.org/en/Publications/Technical-Assistance-Annual-Reports/Issues/2018/10/12/technical-assistance-annual-report-2018.
428 The ten regional technical assistance centers are: AFRITAC Central (Gabon), AFRITAC South (Mauritius), AFRITAC West (Côte d'Ivoire), AFRITAC West II (Ghana), East AFRITAC

(Tanzania), Pacific Financial Technical Center (Fiji), South Asia Regional Training and Technical Assistance Center (India), Middle East Regional Technical Assistance Center (Lebanon), Caribbean Regional Technical Assistance Center (Barbados), Central America, Panama and the Dominican Republic Regional Technical Assistance Center (Guatemala).

429 Detailed plans for the concept drawn from interviews with senior CGAP leadership and "Regional Cybersecurity Resource Centers for Financial Inclusion," Business Concept, CGAP, June 2020. More details also available at: Silvia Baur-Yazbeck and Jean-Louis Perrier, "Regional Centers Can Help Low-Income Countries Build Cyber Resilience," CGAP (blog), July 8, 2020, https://www.cgap.org/blog/regional-centers-can-help-low-income-countries-build-cyber-resilience.

430 Silvia Baur-Yazbeck, Judith Frickenstein, and David Medine, "Cyber Security in Financial Sector Development: Challenges and Potential Solutions for Financial Inclusion," Consultative Group to Assist the Poor, November 2019, https://www.findevgateway.org/sites/default/files/publications/files/cyber_security_paper_november2019.pdf.

431 Based on input from CGAP representatives.

432 Financial Sector Advisory Center, "Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision," World Bank, February 24, 2018, https://www.worldbank.org/en/topic/financialsector/brief/cybersecurity-cyber-risk-and-financial-sector-regulation-and-supervision.

433 Finance, Competitiveness & Innovation Global Practice, "Finance, Competitiveness & Innovation," World Bank, accessed July 22, 2020, https://www.worldbank.org/en/about/unit/fci.

434 Aquiles A. Almansi and Yejin Carol Lee, "Financial Sector's Cybersecurity: A Regulatory Digest," World Bank Group, Financial Sector Advisory Center, July 2020, http://pubdocs.worldbank.org/en/361881595872293851/CybersecDigest-v5-Jul2020-FINAL.pdf.

435 World Bank, "Financial Sector Cyber Resilience Workshop."

436 Aquiles Almansi, Yejin Carol Lee, and Emiko Todoroki, "World Bank Crisis Simulation Exercises: What Is at Stake in Coordinating and Making Decisions in a Crisis," World Bank Group, October 2016, https://openknowledge.worldbank.org/bitstream/handle/10986/25192/109243.pdf?sequence=4; Aquiles Almansi and Yejin C. Lee, "Cybersecurity: A Simulation Exercise" (FIGI Symposium 2019: Capacity Building Sessions, Cairo, Egypt, January 22, 2019), https://www.itu.int/en/ITU-T/extcoop/figisymposium/2019/Pages/Programme-2401.aspx.

437 United Nations Office on Drugs and Crime, "Global Programme on Cybercrime"; World Bank Group, "Combatting Cybercrime"; World Bank Group and United Nations and International Bank for Reconstitution and Development, "Combatting Cybercrime: Tools and Capacity Building for Emerging Economies."

438 Financial Services Sector Coordinating Council, "Financial Sector Cybersecurity Profile."

439 Global Financial Markets Association and Institute of International Finance, "Discussion Draft Principles Supporting the Strengthening of Operational Resilience Maturity in Financial Services," October 2019, https://www.gfma.org/wp-content/uploads/2019/10/discussion-draft-iif-gfma-operational-resilience-principles-october-2019.pdf.

440 Cyber Risk Institute, "The Profile," accessed July 22, 2020, https://cyberriskinstitute.org/the-profile/.

441 Cyber Risk Institute, "The Financial Services Cybersecurity Profile: Ongoing Activity and the Road Ahead," May 5, 2020.

442 Cyber Risk Institute, "Press Releases," https://cyberriskinstitute.org/news-events/.

443 Global Forum on Cyber Expertise, "About the GFCE," accessed July 22, 2020, https://thegfce.org/about-the-gfce/.

444 Global Forum on Cyber Expertise, "About the GFCE," accessed July 22, 2020, https://thegfce.org/about-the-gfce/.

445 Global Forum on Cyber Expertise, "About the GFCE," accessed July 22, 2020, https://thegfce.org/about-the-gfce/.

446 Global Forum on Cyber Expertise, "Initiatives Overview," accessed July 22, 2020, https://thegfce.org/initiatives-overview/.

447 Global Forum on Cyber Expertise, "Preventing and Combating Cybercrime in Southeast Asia—Global Forum on Cyber Expertise," accessed July 22, 2020, https://thegfce.org/initiatives/preventing-and-combating-cybercrime-in-southeast-asia/.

448 Global Forum on Cyber Expertise, "Critical Information Infrastructure Protection Initiative," accessed July 22, 2020, https://thegfce.org/initiatives/critical-information-infrastructure-protection-initiative/.
449 Global Forum on Cyber Expertise, "Cybil Portal," https://cybilportal.org/about-the-gfce/.
450 Global Partnership for Financial Inclusion, "GPFI," accessed July 20, 2020, https://www.gpfi.org/; Global Infrastructure Hub, "Funders and Strategic Partners," accessed July 20, 2020, https://www.gihub.org/about/funders-and-strategic-partners/.
451 Global Infrastructure Hub, "Funders and Strategic Partners," accessed July 20, 2020, https://www.gihub.org/about/funders-and-strategic-partners/.
452 Global Partnership for Financial Inclusion, "GPFI," accessed July 20, 2020, https://www.gpfi.org/; William Hague, "Foreign Secretary William Hague Addressed the London Conference on Cyberspace on 1 November" (Speech, London Conference on Cyberspace, London; UK, November 1, 2011), https://www.gov.uk/government/speeches/foreign-secretary-opens-the-london-conference-on-cyberspace.
453 FinCyber Project, "Cyber Resilience and Financial Organizations: A Capacity-building Tool Box," Carnegie Endowment for International Peace, https://carnegieendowment.org/specialprojects/fincyber/guides.

Priority #6: Digital Transformation and Financial Inclusion

454 "Disruptive Technologies in the Credit Information Sharing Industry: Developments and Implications," Fintech Note, World Bank, 2019, http://documents.worldbank.org/curated/en/587611557814694439/pdf/Disruptive-Technologies-in-the-Credit-Information-Sharing-Industry-Developments-and-Implications.pdf.
455 "Data | GPFI," accessed January 26, 2020, https://www.gpfi.org/data.
456 Nir Kshetri, "Cybercrime and Cybersecurity in Africa," *Journal of Global Information Technology Management* 22, no. 2 (April 3, 2019): 77–81, https://doi.org/10.1080/1097198X.2019.1603527.
457 Kiarie Njoroge, "Treasury Report Reveals Fears Over M-Pesa's Critical Role in Economy," *Business Daily Africa*, November 30, 2016, https://www.businessdailyafrica.com/markets/Treasury-report-reveals-fears-on-M-Pesa-critical-role-in-economy/539552-3469802-2v2gjcz/index.html.
458 John Walubengo, "M-Pesa Is a Critical Resource That Should Never Fail," *Daily Nation* (blog), December 10, 2018, https://www.nation.co.ke/kenya/blogs-opinion/blogs/dot9/walubengo/m-pesa-is-a-critical-resource-that-should-never-fail-117234.
459 Silvia Baur-Yazbeck, Judith Frickenstein, and David Medine, "Cyber Security in Financial Sector Development: Challenges and Potential Solutions for Financial Inclusion," Consultative Group to Assist the Poor, November 2019.
460 Silvia Baur-Yazbeck, Judith Frickenstein, and David Medine, "Cyber Security in Financial Sector Development: Challenges and Potential Solutions for Financial Inclusion," Consultative Group to Assist the Poor, November 2019.
461 Serianu, "Africa Cybersecurity Report 2017: Demystifying Africa's Cyber Security Poverty Line," 2017, https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf.
462 Paul Makin, "Cybersecurity for Mobile Financial Services," CGAP, August 2018, https://www.cgap.org/blog/cybersecurity-mobile-financial-services-growing-problem.
463 Paul Makin, "Cybersecurity for Mobile Financial Services," CGAP, August 2018, https://www.cgap.org/blog/cybersecurity-mobile-financial-services-growing-problem.
464 "Cybersecurity for Financial Inclusion: Framework & Risk Guide," Alliance for Financial Inclusion, October 2019, https://www.afi-global.org/sites/default/files/publications/2019-11/AFI_GN37_DFS_AW_digital_0.pdf.
465 Silvia Baur-Yazbeck, Judith Frickenstein, and David Medine, "Cyber Security in Financial Sector Development: Challenges and Potential Solutions for Financial Inclusion," November 2019.
466 Nir Kshetri and Jeffrey Voas, "Trusting Pirated Software," *Computer* 52, no. 3 (March 2019): 87–90, https://doi.org/10.1109/MC.2019.2898719.
467 "Economic Impact of Cybercrime," accessed January 27, 2020, https://www.csis.org/analysis/economic-impact-cybercrime.

468 "Kaspersky Lab Sees Spike In Mobile Cyberattacks," *PYMNTS.Com* (blog), May 23, 2019, https://www.pymnts.com/news/security-and-risk/2019/kaspersky-lab-malware-mobile-banking/.
469 Nir Kshetri, "Cybercrime and Cybersecurity in Africa," *Journal of Global Information Technology Management* 22, no. 2 (April 3, 2019): 77–81, https://doi.org/10.1080/1097198X.2019.1603527.
470 Symantec, "Cyber Crime and Cyber Security Trends in Africa," November 2016.
471 Serianu, "Africa Cybersecurity Report 2017: Demystifying Africa's Cyber Security Poverty Line."
472 Symantec, "Cyber Crime and Cyber Security Trends in Africa"; "Cybersecurity for Financial Inclusion: Framework & Risk Guide," Alliance for Financial Inclusion, October 2019, https://www.afi-global.org/sites/default/files/publications/2019-11/AFI_GN37_DFS_AW_digital_0.pdf.
473 Paul Makin, "Cybersecurity for Mobile Financial Services," CGAP, August 2018, https://www.cgap.org/blog/cybersecurity-mobile-financial-services-growing-problem.
474 Hildah Nduati, "Cyber Security in Emerging Financial Markets," Consultative Group to Assist the Poor, May 2018, https://www.findevgateway.org/library/cyber-security-emerging-financial-markets.
475 Alliance for Financial Inclusion, "AFI Holds Regulatory Training on Cybersecurity Challenges and Resilience Management," August 2, 2017, https://www.afi-global.org/news/2017/08/afi-holds-regulatory-training-cybersecurity-challenges-and-resilience-management.
476 United Nations Secretary-General's Special Advocate for Inclusive Finance for Development, Fintech Sub-Group on Cybersecurity, "Briefing on Cybersecurity," accessed January 22, 2020, https://www.unsgsa.org/files/2815/3575/0134/Cybersecurity.pdf.
477 Alliance for Financial Inclusion, "Cybersecurity for Financial Inclusion: Framework & Risk Guide," October 2019, https://www.afi-global.org/sites/default/files/publications/2019-11/AFI_GN37_DFS_AW_digital_0.pdf.
478 Silvia Baur-Yazbeck, Judith Frickenstein, and David Medine, "Cyber Security in Financial Sector Development: Challenges and Potential Solutions for Financial Inclusion," November 2019.
479 Gates Foundation, "Grant Awards," accessed July 22, 2020, https://www.gatesfoundation.org/ns/500.html.
480 Digital Financial Services Observatory, "The DFS Observatory at Columbia University," https://dfsobservatory.com/, accessed September 26, 2020.
481 Digital Financial Services Observatory, "The DFS Observatory at Columbia University," https://dfsobservatory.com/, accessed September 26, 2020.
482 Financial Stability Board, "2016 List of Global Systemically Important Insurers (G-SIIs)," November 21, 2016, https://www.fsb.org/wp-content/uploads/2016-list-of-global-systemically-important-insurers-G-SIIs.pdf.
483 Financial Stability Board, "2019 List of Global Systemically Important Banks (G-SIBs)," November 22, 2019, https://www.fsb.org/wp-content/uploads/P221119-1.pdf.
484 Kirstjen M. Nielsen, "National Cybersecurity Summit Keynote Speech" (Speech, National Cybersecurity Summit, New York City, New York, July 31, 2018), https://www.dhs.gov/news/2018/07/31/secretary-kirstjen-m-nielsen-s-national-cybersecurity-summit-keynote-speech.
485 Michael A. Pompeo, "The United States Concerned by Threat of Cyber Attack Against the Czech Republic's Healthcare Sector," Press Statement, April 17, 2020, https://www.state.gov/the-united-states-concerned-by-threat-of-cyber-attack-against-the-czech-republics-healthcare-sector/.
486 "Malicious Cyber Activity Against Healthcare Services and Facilities: Joint OEWG Report Proposal From Australia, Czech Republic, Estonia, Japan, Kazakhstan and United States of America," Open Ended Working Group, Spring 2020, https://www.dfat.gov.au/sites/default/files/joint-oewg-proposal-protection-health-infrastructure.pdf.
487 African Union, "First African Forum on Cybercrime" (Addis Ababa, October 16, 2018), https://au.int/en/newsevents/20181016/first-african-forum-cybercrime.
488 Alliance for Financial Inclusion, "About Us - AFI," accessed July 22, 2020, https://www.afi-global.org/about-us.
489 Alliance for Financial Inclusion, "Global Policy Forum," accessed July 22, 2020, https://www.afi-global.org/global-policy-forum.

490 Alliance for Financial Inclusion, "Cybersecurity for Financial Inclusion: Framework & Risk Guide," October, 2019.
491 Asia Securities Industry & Financial Markets Association, "ASIFMA," accessed July 22, 2020, https://www.asifma.org/.
492 Emmanuel LaMarois, "Cybersecurity Needs to Be a Global and Coordinated Effort," AFME, December 5, 2017, https://www.afme.eu/News/Views-from-AFME/Details/cybersecurity-needs-to-be-a-global-and-coordinated-effort.
493 NATO Cooperative Cyber Defence Centre of Excellence, "ASEAN Regional Forum Reaffirming the Commitment to Fight Cyber Crime."
494 AustCyber, "About Us," accessed July 22, 2020, https://www.austcyber.com/about-us.
495 Australian Signals Directorate, "Cyber Security," accessed July 22, 2020, https://www.asd.gov.au/cyber.
496 Australian Prudential Regulation Authority, "APRA Finalises Updated Guidance on Information Security | APRA," Press Release, June 25, 2019, https://www.apra.gov.au/news-and-publications/apra-finalises-updated-guidance-on-information-security.
497 AUSTRAC, "AUSTRAC Overview," accessed July 22, 2020, https://www.austrac.gov.au/about-us/austrac-overview.
498 Council of Financial Regulators, "Cyber Security—Financial Stability," Australia, accessed July 22, 2020, https://www.cfr.gov.au/financial-stability/cyber-security.html.
499 AUSTRAC, "Fintel Alliance," accessed July 22, 2020, https://www.austrac.gov.au/about-us/fintel-alliance.
500 Reserve Bank of Australia, "Financial Stability Review," October 2018, Australia, https://www.rba.gov.au/publications/fsr/2018/oct/box-d.html.
501 Bank for International Settlements (BIS), "Cyber Resilience: Range of Practices."
502 Committee on Payments and Market Infrastructures, "Payment, Clearing and Settlement Operators Meet on Global Cyber-Resilience."
503 Committee on Payments and Market Infrastructures and The Board of the International Organization of Securities Commissions, "Guidance on Cyber Resilience for Financial Market Infrastructures."
504 Bank for International Settlements (BIS), "Innovation BIS 2025: Shaping the Bank for Tomorrow," June 2019, https://www.bis.org/about/innovation_bis_2025/index.htm.
505 Better Than Cash Alliance, "About the Better Than Cash Alliance," accessed July 22, 2020, https://www.betterthancash.org/about.
506 Better Than Cash Alliance, "Toolkits," accessed July 22, 2020, https://www.betterthancash.org/tools-research/toolkits.
507 Bill and Melinda Gates Foundation, "Financial Services for the Poor Strategy Overview," July 2012, https://docs.gatesfoundation.org/Documents/fsp-strategy-overview.pdf.
508 Bill and Melinda Gates Foundation, "Financial Services for the Poor Strategy Overview," July 2012, https://docs.gatesfoundation.org/Documents/fsp-strategy-overview.pdf.
509 Bank of Canada, "2019-2021 Cyber Security Strategy: Reducing Risk, Promoting Resilience," 2019, https://www.bankofcanada.ca/wp-content/uploads/2019/06/cyber-security-strategy-2019-2021.pdf.
510 Bank of Canada, "2019-2021 Cyber Security Strategy: Reducing Risk, Promoting Resilience," 2019, https://www.bankofcanada.ca/wp-content/uploads/2019/06/cyber-security-strategy-2019-2021.pdf.
511 Siemens, "Siemens and Partners Sign Joint Charter on Cybersecurity," press release, May 17, 2017, https://www.siemens.com/press/en/feature/2018/corporate/2018-02-cybersecurity.php.
512 Samm Sacks, Qiheng Chen, and Graham Webster, "Five Important Takeaways From China's Draft Data Security Law," *DigiChina Project* (blog), July 9, 2020, http://newamerica.org/cybersecurity-initiative/digichina/blog/five-important-take-aways-chinas-draft-data-security-law/.
513 US-China Business Council, "China Banking and Insurance Regulatory Commission," December 19, 2018, https://www.uschina.org/sites/default/files/cbirc_2018.12.19.pdf.
514 China Banking Regulatory Commission, "Guidelines on the Risk Management of Commercial Banks' Information Technology," accessed July 22, 2020, https://wenku.baidu.com/view/71d9dbc48bd63186bcebbc1b.html.

515 Yan Luo and Zhijing Yu, "China Releases Personal Financial Information Protection Technical Specification," *Inside Privacy* (blog), March 2, 2020, https://www.insideprivacy.com/international/china/china-releases-personal-financial-information-protection-technical-specification/.
516 International Organization of Securities Commissions, "About IOSCO," https://www.iosco.org/about/?subsection=about_iosco.
517 Committee on Payments and Market Infrastructures and the Board of the International Organization of Securities Commissions, "Guidance on Cyber Resilience for Financial Market Infrastructures."
518 Detailed plans for the concept drawn from interviews with senior CGAP leadership and "Regional Cybersecurity Resource Centers for Financial Inclusion," Business Concept, CGAP, June 2020.
519 Cybersecurity Tech Accord, "Eleven New Companies Join Pledge to Fight Cyberattacks, Promise Equal Protection for Customers Worldwide," press release, June 20, 2018, https://cybertechaccord.org/eleven-new-companies-join-pledge-to-fight-cyberattacks-promise-equal-protection-for-customers-worldwide/.
520 DFS Observatory, "About the Digital Financial Services Observatory," May 19, 2016, https://dfsobservatory.com/content/about-digital-financial-services-observatory.
521 Sam Meredith, "Microsoft Calls for 'New Digital Geneva Convention' After Spate of High-Profile Cyberattacks," CNBC, January 26, 2018, https://www.cnbc.com/2018/01/26/microsoft-calls-for-new-digital-geneva-convention-after-spate-of-high-profile-cyberattacks.html.
522 Europol, "New Initiative Brings Together Law Enforcement and Europe's Largest Financial Infrastructures," Press Release, February 27, 2020, https://www.europol.europa.eu/newsroom/news/new-initiative-brings-together-law-enforcement-and-europe%E2%80%99s-largest-financial-infrastructures.
523 ENISA, "CyLEEx19: Inside a Simulated Cross-Border Cyber-Attack on Critical Infrastructure," October 31, 2019, https://www.enisa.europa.eu/news/enisa-news/test-1.
524 European Banking Authority, "EBA Guidelines on ICT and Security Risk Management," https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management.
525 European Banking Authority, "EBA Guidelines on ICT and Security Risk Management," https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management.
526 European Banking Authority, "Guidelines on Outsourcing Arrangements," https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements.
527 European Banking Federation, "Cybersecurity," accessed July 22, 2020, https://www.ebf.eu/priorities/cybersecurity-innovation/cybersecurity/.
528 European Commission, "Consultation Document: Digital Operational Resilience Framework for Financial Services: Making the EU Financial Sector More Secure."
529 European Union Agency for Cybersecurity, "Financial Fraud in the Digital Space," November 2018, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/financial-fraud-in-the-digital-space.
530 Europol, "EC3 Partners," accessed July 22, 2020, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners.
531 Council of Europe, "Global Action on Cybercrime Extended (GLACY)+," accessed July 22, 2020, https://www.coe.int/en/web/cybercrime/glacyplus.
532 "First FATF Report on the Extent and Nature of the Money Laundering Process and FATF Recommendations to Combat Money Laundering," Financial Action Task Force, July 2, 1990, http://www.fatf-gafi.org/media/fatf/documents/reports/1990%20ENG.pdf.
533 "About FS-ISAC," FS-ISAC, accessed July 28, 2018, https://www.fsisac.com/about.
534 "FSB Publishes Stocktake on Cybersecurity Regulatory and Supervisory Practices."
535 "FSB Publishes Stocktake on Cybersecurity Regulatory and Supervisory Practices."
536 FINCA Microfinance Global Services LLC, "Products and Services - FINCA Impact Finance," accessed July 22, 2020, https://www.fincaimpact.com/solutions/products-and-services/.

537 FINCA, "Fintech: Innovations and Technology," accessed July 22, 2020, https://www.fincaimpact.com/solutions/fintech-innovations-technology/.
538 Forum of Incident Response and Security Teams, "FIRST - Improving Security Together," accessed July 22, 2020, https://www.first.org/.
539 Banque de France, "French Presidency G7 2019 - « Cybersecurity."
540 Banque de France, "The Banque de France and the Monetary Authority of Singapore Strengthen Financial Cooperation," Press Release, November 12, 2019, https://www.banque-france.fr/en/communique-de-presse/banque-de-france-and-monetary-authority-singapore-strengthen-financial-cooperation.
541 Aquiles A. Almansi and Yejin Carol Lee, "Financial Sector's Cybersecurity: A Regulatory Digest," 92.
542 Chris Ott, "What You Should Know About the 24/7 Cybercrime Network," Davis Wright Tremaine LLP, June 28, 2018, https://www.dwt.com/files/uploads/documents/publications/What%20You%20Should%20Know%20About%20The%2024.pdf.
543 European Central Bank, "Cybersecurity for the Financial Sector," n.d., https://www.ecb.europa.eu/paym/pol/shared/pdf/qa_cybersecurity.pdf.
544 White House Office of the Press Secretary, "G-8 Action on the Deauville Partnership With Arab Countries in Transition," Fact Sheet, May 19, 2012, https://obamawhitehouse.archives.gov/the-press-office/2012/05/19/fact-sheet-g-8-action-deauville-partnership-arab-countries-transition.
545 Deauville Partnership, "Deauville Partnership Action Plan for Financial Inclusion" (G7 Germany 2015), accessed July 22, 2020, https://www.afi-global.org/sites/default/files/publications/2015-04-30-deauville-aktionsplan.pdf.
546 G7 Information Centre, "G7/8 Finance Ministers," accessed July 22, 2020, http://www.g7.utoronto.ca/finance/index.htm.
547 G20 Finance Ministers and Central Bank Governors, "Communiqué," March 17, 2017, Carnegie Endowment for International Peace, https://carnegieendowment.org/files/g20-communique.pdf.
548 Deutsche Bundesbank, "Financial Stability Review 2018" (Frankfurt am Main, Germany, 2018), https://www.bundesbank.de/resource/blob/766586/f9d675a9f6a50562291589f7f3409f5a/mL/2018-finanzstabilitaetsbericht-data.pdf.
549 Aquiles A. Almansi and Yejin Carol Lee, "Financial Sector's Cybersecurity: A Regulatory Digest," World Bank Group, Financial Sector Advisory Center, November 2019, 55, http://pubdocs.worldbank.org/en/940481575300835196/CybersecDIGEST-NOV2019-FINAL.pdf.
550 Global Cyber Alliance, "Cybersecurity Toolkit for Small Business," accessed July 22, 2020, https://www.globalcyberalliance.org/gca-cybersecurity-toolkit/.
551 Global Financial Markets Association, "A Framework for the Regulatory Use of Penetration Testing in the Financial Services Industry"; GFMA and IIF, "Discussion Draft Principles Supporting the Strengthening of Operational Resilience Maturity in Financial Services."
552 Global Forum on Cyber Expertise, "About the GFCE," accessed July 22, 2020, https://thegfce.org/about-the-gfce/.
553 Global Forum on Cyber Expertise, "About the GFCE," accessed July 22, 2020, https://thegfce.org/about-the-gfce/.
554 G20 Leaders, "The G20 Seoul Summit Leaders' Declaration November 11 - 12, 2010," Press Statement, November 12, 2010, http://www.g20.utoronto.ca/2010/g20seoul.pdf.
555 Global Partnership for Financial Inclusion, "GPFI," accessed July 20, 2020, https://www.gpfi.org/.
556 GSMA, "About the GSMA," accessed July 22, 2020, https://www.gsma.com/aboutus/.
557 GSMA, "GSMA Inclusive Tech Lab," accessed July 22, 2020, https://www.gsma.com/mobilefordevelopment/mobile-money/gsma-inclusive-tech-lab/.
558 GSMA, "GSMA Launches Inclusive Tech Lab," Press Release, September 24, 2019, https://www.gsma.com/newsroom/press-release/gsma-launches-inclusive-tech-lab/.
559 Aquiles A. Almansi and Yejin Carol Lee, "Financial Sector's Cybersecurity: A Regulatory Digest," 61.
560 Institute for Development and Research in Banking Technology, "Cyber Security Checklist," Reserve Bank of India, July 2016, https://www.idrbt.ac.in/assets/publications/Best%20Practices/CSCL_Final.pdf.

561 Reserve Bank of India, "Cyber Security Frameworks in Banks" (Notification, June 2, 2016), https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0.

562 Jaime Vazquez and Martin Boer, "Addressing Regulatory Fragmentation to Support a Cyber-Resilience Global Financial Services Industry," n.d., https://www.iif.com/portals/0/Files/private/iif_cyber_reg_04_25_2018_final.pdf.

563 INTERPOL, "INTERPOL-Led Action Takes Aim at Cryptojacking in Southeast Asia," Press Release, January 8, 2020, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-led-action-takes-aim-at-cryptojacking-in-Southeast-Asia; Michael Ouma, "INTERPOL Meeting of Cybercrime Unit Chiefs to Develop Response to WannaCry Attack," aptantech, June 7, 2017, http://aptantech.com/2017/06/interpol-meeting-of-cybercrime-unit-chiefs-to-develop-response-to-wannacry-attack/.

564 International Finance Corporation, "The Partnership for Financial Inclusion," accessed July 22, 2020, https://www.ifc.org/wps/wcm/connect/REGION__EXT_Content/IFC_External_Corporate_Site/Sub-Saharan+Africa/Priorities/Financial+Inclusion/za_ifc_partnership_financial_inclusion.

565 Monetary and Capital Markets Department, "Technical Assistance Annual Report 2018," International Monetary Fund, 2018, https://www.imf.org/en/Publications/Technical-Assistance-Annual-Reports/Issues/2018/10/12/technical-assistance-annual-report-2018.

566 Monetary and Capital Markets Department, "Technical Assistance Annual Report 2018," International Monetary Fund, 2018, https://www.imf.org/en/Publications/Technical-Assistance-Annual-Reports/Issues/2018/10/12/technical-assistance-annual-report-2018.

567 International Telecommunication Union, "Digital Financial Inclusion," accessed July 22, 2020, https://www.itu.int/en/mediacentre/backgrounders/Pages/digital-financial-inclusion.aspx.

568 Kevin Butler et al., "Security Aspects of Digital Financial Services (DFS)," Focus Group Technical Report (International Telecommunication Union, January 2017).

569 Supervisor of Banks, "Cyber Defense Management," Proper Conduct of Banking Business Directive, Bank of Israel, March 2015, https://www.boi.org.il/en/BankingSupervision/SupervisorsDirectives/ProperConductOfBankingBusinessRegulations/361_et.pdf.

570 "FC3—Finance and Cyber Continuity Center: Israel's National Financial CERT," Senior officials from the Israeli Ministry of Finance in written correspondence with the authors, April 16, 2020.

571 Banca d'Italia, "Cybersecurity: A Strategy for the G7 Financial Sector," Press Release, October 11, 2016, https://www.bancaditalia.it/media/notizia/cybersecurity-a-strategy-for-the-g7-financial-sector.

572 CONSOB, "Consob and the Bank of Italy Have Agreed a Common Strategy to Strengthen the Cyber Security of the Italian Financial Sector," CONSOB Weekly Newsletter, January 2020, http://www.consob.it/web/consob-and-its-activities/newsletter/documenti/english/en_newsletter/2020/year_26_n-02_20_january_2020.html.

573 CONSOB, "Consob and the Bank of Italy Have Agreed a Common Strategy to Strengthen the Cyber Security of the Italian Financial Sector," CONSOB Weekly Newsletter, January 2020, http://www.consob.it/web/consob-and-its-activities/newsletter/documenti/english/en_newsletter/2020/year_26_n-02_20_january_2020.html.

574 Leika Kihara, "BOJ Warns of Cyber-Attack Vulnerability Ahead of Olympic Games," Reuters, January 31, 2020, https://www.ibtimes.sg/boj-warns-cyber-attack-vulnerability-ahead-olympic-games-38619.

575 Financial Services Agency, "The Policy Approaches to Strengthen Cyber Security in the Financial Sector (Summary)," Presentation, July 2, 2015, https://www.fsa.go.jp/en/news/2015/20151105-1/01.pdf.

576 Japan Cybercrime Control Center, "Establishment of 'Japan Cybercrime Control Center,' a New Organization for Fighting Cybercrime," Press Release, November 13, 2014, https://www.jc3.or.jp/media/pdf/pressreleaseEnglish.pdf.

577 Europol, "Joint Cybercrime Action Taskforce (J-CAT)," accessed July 22, 2020, https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce.

578 "DNB Publishes Hacking Guide for Cyber Security Exercises," Central Banking, November 20, 2017, https://www.centralbanking.com/node/3322436.

579 G Odinot et al., "Organised Cybercrime in the Netherlands," The Ministry of Justice and Security of the Netherlands, 2017.
580 Government of the Netherlands, "Investigation and Prosecution of Criminals," Ministerie van Algemene Zaken, December 14, 2011, https://www.government.nl/topics/crime-and-crime-prevention/investigation-and-prosecution-of-criminals.
581 G Odinot et al., "Organised Cybercrime in the Netherlands," The Ministry of Justice and Security of the Netherlands, 2017.
582 G Odinot et al., "Organised Cybercrime in the Netherlands," The Ministry of Justice and Security of the Netherlands, 2017.
583 Nigeria Electronic Fraud Forum, "2016 Annual Report," Central Bank of Nigeria, July 5, 2016, https://www.cbn.gov.ng/documents/NeFFar.asp.
584 North Atlantic Treaty Organization, "Collective Defence - Article 5," November 25, 2019, http://www.nato.int/cps/en/natohq/topics_110496.htm.
585 NATO Cooperative Cyber Defence Centre of Excellence, "CCDCOE - About Us," accessed July 22, 2020, https://ccdcoe.org/about-us/.
586 North Atlantic Treaty Organization, "Cyber Defence," accessed July 22, 2020, http://www.nato.int/cps/en/natohq/topics_78170.htm.
587 G20/OECD Task Force on Financial Consumer Protection, "G20/OECD Policy Guidance on Financial Consumer Protection Approaches in the Digital Age," G20/OECD Policy Guidance, OECD, 2018, http://www.oecd.org/daf/fin/financial-education/G20-OECD-Policy-Guidance-Financial-Consumer-Protection-Digital-Age-2018.pdf.
588 OSCE, "Cyber/ICT Security," accessed July 22, 2020, https://www.osce.org/cyber-ict-security.
589 Organization of American States, "Welcome to the Inter-American Cooperation Portal on Cyber-Crime," accessed July 22, 2020, https://www.oas.org/juridico/english/cyber.htm.
590 France Diplomatie, "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace," https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.
591 Central Bank of Russia, "Guidelines for the Advancement of Information Security in the Financial Sector for 2019-2021," http://www.cbr.ru/Content/Document/File/103460/onrib_2021_e.pdf.
592 Central Bank of Russia, "Guidelines for the Advancement of Information Security in the Financial Sector for 2019-2021," 3, http://www.cbr.ru/Content/Document/File/103460/onrib_2021_e.pdf.
593 Central Bank of Russia, "Financial Cybersecurity: Bank of Russia Report," October 10, 2019, http://www.cbr.ru/eng/press/event/?id=3937.
594 Central Bank of Russia, "Guidelines for the Advancement of Information Security in the Financial Sector for 2019-2021."
595 SANS Institute, "Cyber Workforce Academy Maryland," accessed July 22, 2020, https://www.sans.org/cybertalent/cyber-workforce-academy-maryland.
596 SANS Institute, "Introduction to the Cyber Retraining Academy," accessed July 22, 2020, https://www.sans.org/ukcyberacademy.
597 SIFMA, "Cybersecurity Exercise: Quantum Dawn V."
598 Alex Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased," *CFRBlog* (blog), November 15, 2018, https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.
599 FS-ISAC, "FS-ISAC and CSA Partner to Enhance Cybersecurity in Singapore."
600 Aquiles A. Almansi and Yejin Carol Lee, "Financial Sector's Cybersecurity: A Regulatory Digest."
601 "Consultation Paper on Proposed Revisions to Business Continuity Management Guidelines."
602 SWIFT, "Customer Security Programme Terms and Conditions," June 30, 2017, https://www2.swift.com/uhbonline/books/public/en_uk/cst_sec_prog_trm_cond/index.htm.
603 "Huge Data Theft Hits South Korea," BBC News, January 20, 2014, https://www.bbc.com/news/technology-25808189.

604 Korean Institute of Criminology, *Cybercrime in the Republic of Korea II: Criminal Justice and International Coopeeration for Cybercrime Prevention* (Seoul, Republic of Korea: KyungSung Publishing, 2014), https://eucyberdirect.eu/wp-content/uploads/2019/10/cybercrime-in-the-republic-of-korea-ii.pdf.

605 Christine Kim, "North Korea Hacking Increasingly Focused on Making Money More Than Espionage: South Korea Study," Reuters, July 28, 2017, https://www.reuters.com/article/us-northkorea-cybercrime-idUSKBN1AD0BO.

606 GEANT, "TF-CSIRT: Computer Security Incident Response Teams - GÉANT," accessed July 20, 2020, https://www.geant.org:443/People/Community_Programme/Task_Forces/Pages/TF-CSIRT.aspx.

607 Bank of England and Financial Conduct Authority, "Building the UK Financial Sector's Operational Resilience."

608 Bank of England, "CBEST Implementation Guide."

609 Founding institutions include Barclays, Standard Chartered, Deutsche Bank and Banco Santander. Other members now include Bank of Ireland, Allied Irish Banks, Lloyds Banking Group, and Metro Bank. See: "Banks Join Forces to Crack Down on Fraudsters," August 8 2017, https://www.ft.com/content/6c9030ca-7937-11e7-90c0-90a9d1bc9691.

610 Europol, "The Cyber Defence Alliance and Europol Step Up Cooperation in the Fight Against Fraudsters," October 2018, https://www.europol.europa.eu/newsroom/news/cyber-defence-alliance-and-europol-step-cooperation-in-fight-against-fraudsters.

611 Bank of England and Financial Conduct Authority, "Building the UK Financial Sector's Operational Resilience," July 2018, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf.

612 Katherine Griffiths, "Banks Man the Barricades to See off Cyberattacks," *The Times*, October 2018, https://www.thetimes.co.uk/article/banks-man-the-barricades-to-see-off-cyberattacks-qz63v5wwk.

613 Robert Hannigan, "Organising a Government for Cyber: The Creation of the UK's National Cyber Security Centre," Occasional Paper, Royal United Services Institute for Defence and Security Studies, February 2019, https://rusi.org/sites/default/files/20190227_hannigan_final_web.pdf.

614 National Cyber Security Centre, "Cyber Security Information Sharing Partnership (CiSP)."

615 Robert Hannigan, "Organising a Government for Cyber: The Creation of the UK's National Cyber Security Centre."

616 Bank of England and Financial Conduct Authority, "Building the UK Financial Sector's Operational Resilience."

617 UK Finance, "About Us | UK Finance," accessed July 22, 2020, https://www.ukfinance.org.uk/about-us.

618 UN Department of Economic and Social Affairs, "Financing for Sustainable Development," accessed July 22, 2020, https://www.un.org/esa/ffd/events/event/high-level-dialogue-on-financing-for-development.html.

619 United Nations Office on Drugs and Crime, "Cybercrime."

620 United Nations Secretary-General's Special Advocate for Inclusive Finance for Development, Fintech Sub-Group on Cybersecurity, "Briefing on Cybersecurity," accessed January 22, 2020, https://www.unsgsa.org/files/2815/3575/0134/Cybersecurity.pdf.

621 United Nations Security Council, "Letter Dated 31 July 2019 From the Panel of Experts Established Pursuant to Resolution 1874 (2009) Addressed to the Chair of the Security Council Committee Established Pursuant to Resolution 1718 (2006)."

622 Financial Services Sector Coordinating Council, "The Financial Services Sector Cybersecurity Profile," October 25, 2018, https://fsscc.org/files/galleries/Financial_Services_Sector_Cybersecurity_Profile_Overview_and_User_Guide_2018-10-25.pdf.

623 Financial Services Sector Coordinating Council, "The Financial Services Sector Cybersecurity Profile," October 25, 2018, https://fsscc.org/files/galleries/Financial_Services_Sector_Cybersecurity_Profile_Overview_and_User_Guide_2018-10-25.pdf.

624 Federal Reserve System, "Enhanced Cyber Risk Management Standards," Advance Notice of Proposed Rulemaking, Fall 2019, 7100-AE61, Office of Information and Regulatory Affairs, OMB, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201910&RIN=7100-AE61.

625 United States Secret Service, "Electronic Crimes Task Forces (ECTF)," White House Archived Web Pages, https://obamawhitehouse.archives.gov/files/documents/cyber/United%20States%20Secret%20Service%20-%20Electronic%20Crimes%20Task%20Forces.pdf.
626 United States Secret Service, "United States Secret Service Electronic Crimes Task Forces," U.S. Department of Homeland Security, accessed July 22, 2020, https://www.dhs.gov/sites/default/files/publications/USSS_Electronic-Crimes-TaskForces.pdf.
627 Shannon Vavra, "Secret Service Merging Electronic and Financial Crime Task Forces to Combat Cybercrime."
628 Cyber Readiness Institute, "Our Mission," accessed July 22, 2020, https://www.cyberreadinessinstitute.org/our-mission.
629 Service, "Top Companies Team Up With Federal Agencies and Nonprofit to Launch First-of-its-kind Cyber Talent Initiative to Protect Against Cyberattacks."
630 Frank C. Cicio, Jr., "How America Is Closing the Cybersecurity Skills Gap," *Knowledge@Wharton* (blog), August 16, 2017, https://knowledge.wharton.upenn.edu/article/america-plans-close-skills-gap-cybersecurity/.
631 Frank C. Cicio, Jr.
632 Steven T. Mnuchin, "Statement by Treasury Secretary Steven T. Mnuchin on the Introduction of Legislation to Transfer the Secret Service Back to Its Original Home at the Treasury Department," statement, Washington, DC, May 6, 2020, https://home.treasury.gov/news/press-releases/sm1004.
633 Internet Crime Complaint Center, "2019 Internet Crime Report," U.S. Federal Bureau of Investigation, 2019, https://pdf.ic3.gov/2019_IC3Report.pdf.
634 Financial and Banking Information Infrastructure Committee, "FBIIC: Members," accessed July 22, 2020, https://www.fbiic.gov/fbiic-members.html.
635 FinCEN, "What We Do," accessed July 22, 2020, https://www.fincen.gov/what-we-do.
636 U.S. Department of the Treasury, "FinCEN Realigns Division to Increase Strategic Capabilities."
637 Financial Services Sector Coordinating Council, "Financial Sector Cybersecurity Profile."
638 FS-ISAC, "FS-ISAC Announces the Formation of the Financial Systemic Analysis & Resilience Center (FSARC)."
639 Chris Bing, "Project Indigo: The Quiet Info-Sharing Program Between Banks and U.S. Cyber Command," CyberScoop, May 21, 2018, https://www.cyberscoop.com/project-indigo-fs-isac-cyber-command-information-sharing-dhs/.
640 The National Cyber-Forensics and Training Alliance, "NCFTA," accessed July 22, 2020, https://www.ncfta.net/.
641 The National Cyber-Forensics and Training Alliance, "CyFin Program," accessed July 22, 2020, https://www.ncfta.net/cyfin-program/.
642 National Initiative for Cybersecurity Education (NICE), "The NICE Cybersecurity Workforce Framework," U.S. National Institute for Standards and Technology, August 2017, https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center/current.
643 National Initiative for Cybersecurity Education (NICE), "The NICE Cybersecurity Workforce Framework," U.S. National Institute for Standards and Technology, August 2017, https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center/current.
644 New York State Department of Financial Services, "NYDFS 23 NYCRR 500," 2017, https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.
645 Sheltered Harbor, "Sheltered Harbor - About," accessed July 20, 2020, https://shelteredharbor.org/index.php/about#who.
646 Stacy Cowley, "Banks Adopt Military-Style Tactics to Fight Cybercrime," *New York Times*, May 20, 2018, https://www.nytimes.com/2018/05/20/business/banks-cyber-security-military.html.
647 United States Secret Service, "Secret Service Announces the Creation of the Cyber Fraud Task Force," press release, July 9, 2020, https://www.secretservice.gov/data/press/releases/2020/20-JUL/Secret-Service-Cyber-Fraud-Task-Force-Press-Release.pdf.

648 Juan Zarate and Tim Maurer, "Protecting the Financial System Against the Coming Cyber Storms," *Hill*, May 18, 2020, https://thehill.com/opinion/cybersecurity/498244-protecting-the-financial-system-against-the-coming-cyber-storms.

649 World Bank and United Nations, "Combatting Cybercrime: Tools and Capacity Building for Emerging Economies," 2017, http://documents.worldbank.org/curated/en/355401535144740611/pdf/129637-WP-PUBLIC-worldbank-combating-cybercrime-toolkit.pdf.

650 Finance, Competitiveness & Innovation Global Practice, "Finance, Competitiveness & Innovation," World Bank, accessed July 22, 2020, https://www.worldbank.org/en/about/unit/fci.

651 Georg Schmitt, "To Prevent a Digital Dark Age: World Economic Forum Launches Global Centre for Cybersecurity," World Economic Forum, December 19, 2019, https://www.weforum.org/press/2018/01/to-prevent-a-digital-dark-age-world-economic-forum-launches-global-centre-for-cybersecurity/.

652 World Economic Forum, "Partnership Against Cybercrime," accessed July 20, 2020, https://www.weforum.org/projects/partnership-against-cybercime/.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

The Carnegie Endowment for International Peace is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Cyber Policy Initiative

To achieve greater stability and civility in cyberspace, the Carnegie Cyber Policy Initiative develops strategies and policies in several key areas and promotes international cooperation and norms by engaging key decisionmakers in governments and industry.

CarnegieEndowment.org