CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

Executive Summary

International Strategy to Better Protect the Financial System Against Cyber Threats

TIM MAURER AND ARTHUR NELSON

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

Executive Summary

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

Summary

The global financial system is going through an unprecedented digital transformation, which is being accelerated by the coronavirus pandemic.[1] 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.[2] 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,[3] 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,[4] more than three times the amount of money it was able to generate through counterfeit activity over the previous four decades.[5] Other state-sponsored actors have targeted financial institutions, for example, with massive distributed denial-of-service (DDoS) attacks.[6] 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.[7]

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.[8] 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.[9] 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."[10]

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."[11] 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;[12] 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.[13] 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.

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.[14]

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:

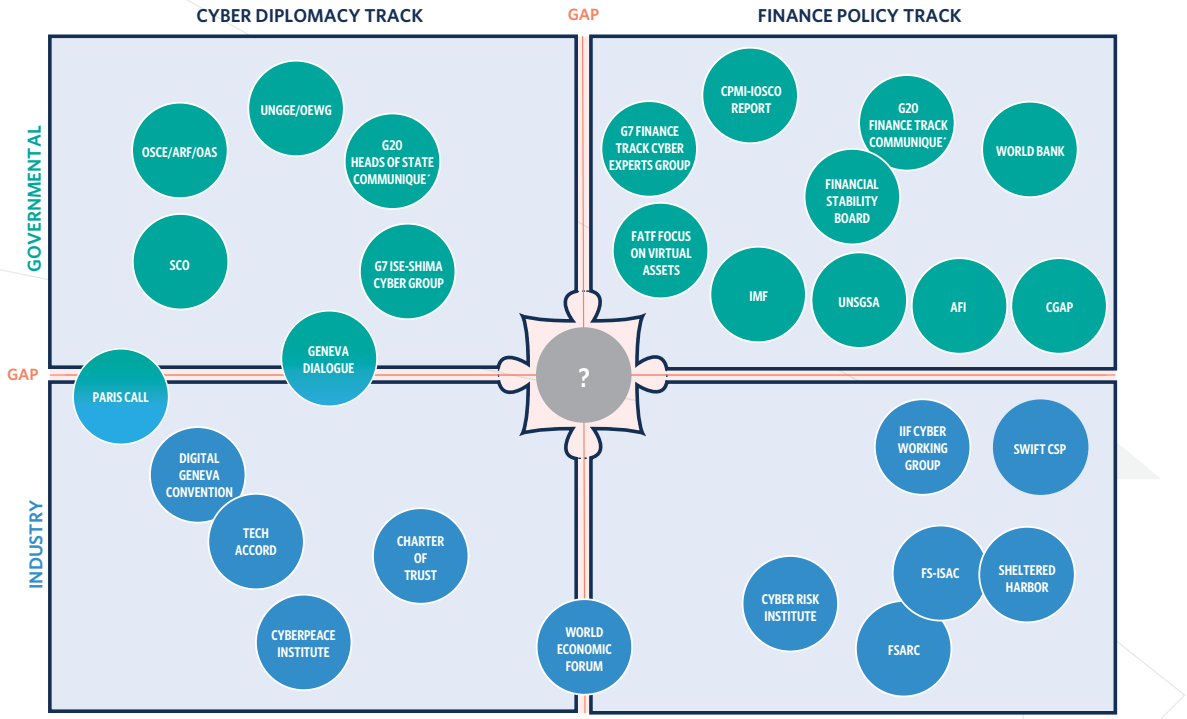
- **Greater clarity about roles and responsibilities is required.** The current fragmentation and uncertainty about roles and responsibilities weaken the international system's collective resilience, recovery, and response capabilities. Only a handful of countries have built effective domestic relationships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

- **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.

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



Note: Overlapping indicates that processes/organizations are connected.

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).[15] 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;[16] 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."[17]

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 illustrates 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.

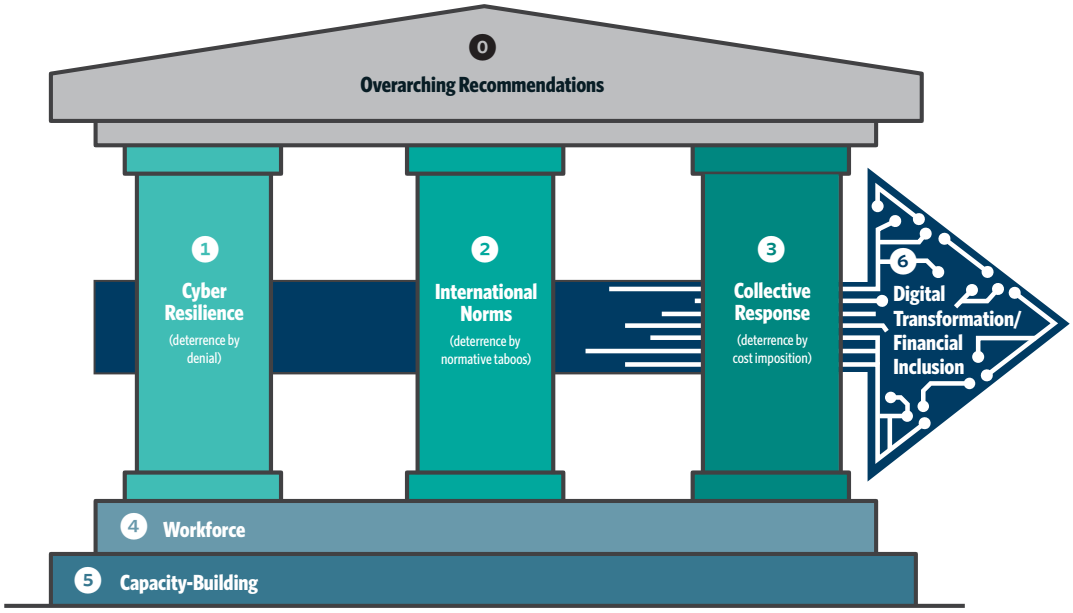
5. Crosscutting Issue #2:

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 for Better Protecting the Financial System Against Cyber Threats



OVERARCHING RECOMMENDATIONS

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.

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 include the United States and Russia.

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.

PRIORITY #1 "CYBER RESILIENCE": FOCUS ON THE UNIQUE NATURE OF CYBER THREATS

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.

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, 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 f irms 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.

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.

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.

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

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, 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.

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.

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

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 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 to 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

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

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), 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, 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

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.

NOTES

1 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.

2 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.

3 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/.

4 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.

5 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.

6 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.

7 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.

8 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/.

9 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.

10 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.

11 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/.

12 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.

13 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.

14 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/.

15 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/.

16 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.

17 "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.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

IN COLLABORATION WITH:

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

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