Task Force 4
Digital Transformation

Policy brief

PROMOTING GLOBAL FINANCIAL RESILIENCE AGAINST CYBER THREATS THROUGH AN OPERATIONAL COLLABORATION MODEL

SEPTEMBER 2021

Erica D. Borghard Carnegie Endowment for International Peace

T20 NATIONAL COORDINATOR AND CHAIR
ISPI

T20 CO-CHAIR
IAI

T20 SUMMIT CO-CHAIR
Università Bocconi MILANO

THINK20 ITALY 2021

G20 ITALIA 2021

ABSTRACT

This policy brief explores the challenge of how to promote the cyber resilience of the global financial system through operational collaboration. It focuses on promoting the resilience both of individual financial institutions and the global financial system. Cyber resilience entails the ability to anticipate and prepare; withstand and recover; respond; and learn in the wake of disruptive events. Operational collaboration is a model for implementing a resilience-based approach. It goes beyond information-sharing, to incorporate meaningful, routine, institutionalized collaboration, where stakeholders work together on shared threats (Borghard 2018; Maurer and Nelson 2020). Collaboration is important due to the scope of the cyber threat to financial services; the interdependence of the system itself, such that an incident in one part could have cascading effects; and the diversity of stakeholders across the regulatory/supervisory, government and industry communities that play a role in the system's resilience. However, these factors also present hurdles to collaboration-particularly the global nature of the challenge and the sometimes competing or imperfectly aligned nature of the actors involved. Therefore, the G20, including through the Financial Stability Board (FSB) established by the G20 in 2009, is uniquely positioned to play a key role in helping to surmount these hurdles and promote an operational collaboration approach.

While there is an emerging consensus across governmental organizations, regulatory entities, international bodies and industry that cyber resilience for financial institutions should be prioritized, gaps remain with respect to defining an overarching framework that can help drive the development of common standards and achieve agreement on prioritization and implementation. Given the diverse work that already exists on cyber resilience for the financial sector, this policy brief articulates a resilience framework based on the logic of operational collaboration to help foster consensus across diverse stakeholders and drive implementation of resilience approaches for financial services.

CHALLENGE

The threat in this space is diverse, multifaceted and growing. Over 30 countries are purported to have offensive cyber capabilities, in addition to the growing proliferation of criminal actors, proxy groups and opportunists. Both state and non-state actors have routinely demonstrated a capability and willingness to target the international financial system for economic gain or strategic purposes. This has included disruptive attacks, theft of digital currencies and intellectual property, data integrity attacks, ransomware attacks, and so on.

Additionally, the evolving nature of financial services is creating new risks. Several examples of these new technologies illustrate the scale of this policy challenge. For instance, innovations in financial technologies (FinTech) and the increasing digitization of financial services and institutions – ranging from cryptocurrencies that exist outside the scope of traditional financial institutions and markets, to central bank digital currencies and digital payments systems – are expanding the scope of actors and creating new risks. The cybersecurity risks posed by digital assets remain understudied. Moreover, migration to the cloud, while in some ways a positive development for resilience, is also generating concerns about third-party risk and the potential downstream effects of cyber incidents targeting cloud service providers, and is spurring debates about appropriate governance regimes for cloud service providers. The growing use of artificial intelligence and machine learning tools, where the financial sector has been a pioneering force, is raising questions among the regulatory and supervisory communities about how these tools are being employed. These trends underscore the importance of operational collaboration. As the stakeholders involved in the resilience of the financial system grow and become more diverse, and as the risks multiply and become more complex, it becomes more important for actors to work together to address common challenges and cultivate the resilience of the financial system.

Promoting the resilience of the financial system is an inherently global task. Because global finance is a complex, interdependent system, disruptive events targeting a single entity could have broader, negative consequences for the system itself. And this interdependence, coupled with the reality that capabilities can widely vary across financial institutions, means that incidents targeting small- to medium-sized firms are likely to have broader consequences for the global financial system. Moreover, given the integral role the financial services sector plays in the global economy – starkly demonstrated by the consequences of the 2008 financial crisis – cyber threats to financial institutions pose broader international economic and strategic risks. Indeed, in a recent interview, Jerome Powell, Chairman of the Federal Reserve, identified cyber-related risks as the top threat to the international financial system, more than the events that triggered the 2008 crisis (Fung 2021).

Several ongoing efforts across relevant international stakeholders are aimed at cultivating the resilience of the financial system. For example, regulatory entities and standards-setting bodies, such as United States regulators, the Bank of England, Monetary Authority of Sin-

gapore, the European Central Bank, the Financial Stability Board and the Bank for International Settlements have issued different recommendations and best practices to promote resilience. At the same time, industry has driven efforts, such as Sheltered Harbor, to protect financial data in the event of a major cyber attack, as well as working with governments to conduct recurring table-top exercises to identify gaps and improve collaboration, such as the Hamilton Series exercises and exercises held by the Financial Services Information Sharing and Analysis Center (FS-ISAC) on cyber threats to the payments system. International bodies, including the Organization for Security and Cooperation in Europe (OSCE), G7 and G20, as well as some governments, have emphasized the development of confidence-building measures to promote transparency, as well as norms to protect the financial services sector, particularly against cyber attacks that target data integrity. There have also been efforts to promote capacity-building to increase the resilience of the overall system by raising the cybersecurity of small- to medium-sized institutions.

However, despite these important initiatives, adoption of resilience-based approaches remains inconsistent. A number of factors likely contribute to this outcome. However, the absence of a coherent and consistent conceptual framework that clarifies how to implement a resilience-based approach, remains a critical gap. Therefore, there is an opportunity for G20 to assume a leadership role in this area, providing a strategic anchor to guide and promote ongoing resilience work.

G20 has already made important progress in promoting cyber resilience, especially through the work of the FSB, which makes the G20 ideally positioned to play a key role in this area. For instance, in response to a request by the G20 Finance Ministers and Central Bank Governors, in 2017 the FSB published a report, "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices," which details existing regulatory and supervisory practices and guidelines (Financial Stability Board, 2017). Furthermore, in November 2018 the FSB published a cyber lexicon containing 50 key terms to cultivate common definitions and understandings among constituencies in the financial services ecosystem (Financial Stability Board, 2018). Moreover, in October 2020 the FSB published an extensive report on cyber resilience that features a toolkit for organizations to evaluate cybersecurity and resilience best practices (Financial Stability Board, 2020). Therefore, G20 tasking FSB to take the lead on promoting operational collaboration across member countries would build on the existing foundation of the FSB's work in this area.

PROPOSAL

Improving the cyber resilience of the financial sector based on a model of operational collaboration shifts existing strategic framing away from an emphasis on deterrence – which is largely grounded in preventing unwanted actions both through the threat of retaliation (typically the purview of governments) and by improving defenses (predominantly the responsibility of industry) to make cyber breaches and attacks more difficult – toward a recognition that a certain level of malicious cyber activity, particularly against financial services, is inevitable. This distinction is not merely academic. The conceptual frameworks that explicitly or implicitly guide policymaking around the resilience of the financial sector affect how stakeholders define threats and risks, and prioritize investment in controls and other mitigations.

Government, industry, the regulatory and supervisory community and international bodies are all galvanized to improve the cyber resilience of the financial sector. This includes cyber resilience efforts through the G20 and the FSB. To achieve more coherence around existing initiatives, gaining consensus around a common conceptual framework to guide the efforts of diverse stakeholders toward a common objective would be a positive development. Diverse stakeholders agree that protecting the cyber resilience of the global financial system is essential, but there are varying approaches to resilience and differences in conceptual framing. Therefore, even while specific resilience practices may vary by organization and constituencies, achieving general consensus on the appropriate components of a resilience-based approach to financial sector cybersecurity is crucial. This policy memo aims to provide a foundation for doing so. Specifically, it argues that the cyber resilience of the financial sector should be grounded in the concept of operational collaboration.

Operational collaboration involves more meaningful, institutionalized cooperation at an operational level between financial sector stakeholders and governments on a day-to-day basis. It includes information-sharing at a minimum, but also incorporates a range of other activities. Emergent models of operational collaboration have developed in the United States, such as the Analysis and Resilience Center (ARC, formerly the Financial Sector Analysis and Resilience Center) and United Kingdom, particularly the Financial Sector Cyber Collaboration Centre (FSCCC) (Maurer and Nelson 2020). The G20, through the FSB, could provide a forum for sharing best practices and insights about these approaches that could be extended to other member states.

This policy brief organizes operational collaboration according to four elements: anticipate and prepare; withstand and recover; respond; and learn. These components are meant to be cyclical and iterative, rather than linear. Lessons learned and insights gleaned feed back into helping stakeholders better anticipate, recover from and respond to cyber incidents. Temporally, these elements are distinguished by those that take place prior to a disruptive event (anticipate and prepare); during the course of the disruptive event (withstand and

recover); and following the event (respond and learn). Moreover, across the four elements, the roles and responsibilities of different stakeholders will vary. Figure 1, below, depicts the relationship between these elements.

FIG. 1 - OPERATIONAL COLLABORATION TO PROMOTE CYBER RESILIENCE

ANTICIPATE AND PREPARE

Because it is inevitable that malicious actors will continue to target the financial sector for strategic and financial gain, anticipating and preparing for these events will help to reduce their impact at both firm and systemic level.

Anticipation is analogous to the concept of strategic warning. With proper strategic warning, individual firms could leverage indicators and warnings of impending cyber incidents to shore up their own monitoring and network defenses in anticipation of adverse events to mitigate their consequences. Government intelligence organizations could play a critical role in enabling strategic warning by providing more useful and timely information to private-sector entities that are likely to be affected, based on intelligence collection and analysis that could only be conducted by leveraging unique governmental intelligence capabilities and authorities. Furthermore, for government intelligence collection and analysis against threats to financial services to be useful, industry would have to be incorporated into the intelligence cycle, so that it can provide input on how collection requirements are defined, in order to ensure that they are in line with how malicious actors actually target the financial sector.

However, at present, strategic warning capabilities are nascent and are challenged by the fact that, while threat actors target across multiple verticals in the financial services sector, vital information about the threat environment and evolving adversary capabilities and in-

tent is fragmented across different stakeholders. This fragmentation occurs across different lines and to varying degrees in different G20 member nations. Among governments, as well as between governments and firms, there is a hesitance to share intelligence pertaining to cyber threats to the financial system, given concerns about revealing sensitive national security information. Among firms, there is a reluctance to share threat intelligence information within the sector, given the business consequences of potential exposure and the competitive nature of any market environment.

There are several areas in the context of strategic warning where G20 could play a leadership role, especially through the FSB:

- G20 member states could agree to work through the FSB to promote more meaningful information-sharing among member states about cyber threats to the financial system.

- G20 could encourage member states to work toward a consensus position that cyber threats to the financial system represent a national security threat, and that intelligence agencies should play a role in collecting against those threats.

- G20 could task the FSB to encourage member states to evaluate existing models of intelligence collaboration around strategic warning between industry and government to assess how those models might be implemented within individual countries.

Beyond anticipating adverse events, being prepared to address them if and when they occur is essential for resilience, so that stakeholders are not adjudicating roles and responsibilities and working together for the first time in the midst of a crisis or contingency. Recognizing this, a number of different financial-sector-oriented exercises and simulations are already taking place, some on a recurring basis, which is a positive development that should be sustained. However, there are two areas where G20 could play a leadership role in terms of enhancing the impact of ongoing exercise initiatives, as well as moving beyond exercises toward the development of sector-specific playbooks.

- G20 could task the FSB to help to foster thought leadership around developing consistent methodologies for how the scenarios that inform financial sector cyber exercises are developed, as well as develop consensus around clear and consistent processes for how the lessons learned from exercises and simulations are incorporated into policy, plans and procedures, and how they inform investments in controls.

- Moving beyond exercises, G20 could task FSB to encourage member states to work with industry and other stakeholders to develop financial-sector-specific playbooks that are informed by ongoing exercises and simulations. These playbooks should clarify roles, responsibilities, and actions – as transparently as possible – for various scenarios and contingencies. In particular, transparency around potential government courses of action will be important for informing industry risk assessments.

WITHSTAND AND RECOVER

During the course of a disruptive event and in its immediate aftermath, the resilience of affected entities is a function of the speed with which they can restore critical functions and services, and the extent to which they can minimize damage stemming from the event. Therefore, governments and international bodies have promulgated different regulatory regimes or recommended best practices concerning the resilience of the financial sector, especially with respect to cyber threats. In particular, there is significant focus on the forthcoming passage of the European Commission's Digital Operational Resilience Act, which will create new risk management and resilience requirements for firms operating in the European Union.

- G20 should task the FSB to update resilience guidelines and best practices in light of an evolving regulatory and supervisory landscape, and to help promote clarity about different standards.

RESPOND

Response actions to cyber incidents that undermine the resilience of the financial system are important for reinforcing, clarifying and enforcing what constitutes norms of acceptable behavior. Over time, consistent and transparent responses can contribute to the overall resilience of the system. However, sector-specific norms for financial services have met with varying success. On the one hand, states have largely refrained from conducting cyber attacks that target the integrity of financial data; but on the other hand, there have been disruptive cyber incidents conducted against financial institutions, as well as financial theft.

Government responses have historically spanned a range of different actions, including public attribution, diplomatic measures, the imposition of sanctions and other economic measures, law enforcement actions and, in some cases, military responses. Therefore, while governments play a leading role in the response aspect of resilience, industry also has a stake in government responses in two ways. The first is governments' use of financial institutions to implement sanctions and other economic measures as part of government responses to malicious cyber behavior (including malicious behavior against financial institutions as well as a wide range of other targets). The second is that financial institutions often find themselves to be targets of cyber threat actors in response to changing geopolitical circumstances. This could occur directly as threat actors target financial institutions as a direct response to sanctions and other measures, such as law enforcement or even military action, or indirectly as government responses affect firms' risk exposure across a range of areas. Therefore, even in this area, where the government is the lead actor, operational collaboration is important because the overall resilience of the financial system in some ways depends on transparency and awareness by both parties of how government action may affect risks to the financial sector.

- G20 should issue a statement that promotes the concept of sector-specific norms of behavior in cyberspace, and specifically endorses a norm against cyber attacks that target financial stability and integrity (Maurer and Nelson 2020). Rather than defining general forms of malicious behavior in cyberspace, sector-specific norms are tailored to the specific and unique challenges of particular critical infrastructure sectors. Given the shared interest of G20 members in the stability and integrity of the global financial system, and given emergent state practice around refraining from conducting cyber attacks that aim to undermine it, a public statement would help reinforce and strengthen an existing implicit norm.

- G20 should task the FSB to serve as a hub for sharing information and promoting transparency about expectations around appropriate responses for norms violations, and potentially to coordinate or share information about responses and information to aid in mitigation and incident response.

LEARN

Finally, cultivating resilience is an inherently iterative process, particularly in a dynamic environment. Therefore, learning from experiences and incorporating lessons learned into ongoing practices is important for sustaining resilience over time.

- G20 could task the FSB to be a central repository for lessons learned and to iteratively solicit input for and publish reports on best practices and insights, to help institutionalize and sustain ongoing efforts and support continued maturity around resilience.

.

REFERENCES

Borghard, E. D., "Protecting Financial Institutions against Cyber Threats," *Carnegie Endowment for International Peace*, 1 September 2018 https://carnegieendowment.org/2018/09/24/protecting-financial-institutions-against-cyber-threats-national-security-issue-pub-77324

Financial Stability Board, *Stocktake of Publicly Released Cybersecurity Regulation, Guidance and Supervisory Practices*, 13 October 2017 https://www.fsb.org/wp-content/uploads/P131017-2.pdf

Financial Stability Board, *Cyber Lexicon*, 12 November 2018 https://www.fsb.org/2018/11/cyber-lexicon/

Financial Stability Board, *Effective Practices for Cyber Incident Response and Recovery*, 19 October 2020 https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery-final-report/

Fung, B., "Cyberattacks are the number-one threat to the global financial system," *CNN Business*, 12 April 2021 https://www.cnn.com/2021/04/12/business/jerome-powell-cyberattacks-global-threat/index.html

Maurer, T. and A. Nelson, "International Strategy to Better Protect the Financial System Against Cyber Threats", *Carnegie Endowment for International Peace*, 2020 https://carnegieendowment.org/2020/11/18/international-strategy-to-better-protect-financial-system-against-cyber-threats-pub-83105

New York Cyber Task Force, "Enhancing Readiness for National Cyber Defense through Operational Collaboration", *Columbia University*, February 2021 https://www.sipa.columbia.edu/ideas-lab/tech-policy/readiness-operational-collaboration

ABOUT THE AUTHOR

Erica D. Borghard Carnegie Endowment for International Peace, Washington DC (USA)

Senior fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace. Erica also continues to serve as a senior director on the U.S. Cyberspace Solarium Commission, a Congressional commission established to develop a comprehensive national strategy to defend the United States in cyberspace.