Cyber Securing Cross-border Financial Services: Calling for a Financial Cybersecurity Action Task Force

Keman Huang
Cybersecurity at MIT Sloan
keman@mit.edu

Stuart Madnick
MIT Sloan School of Management
smadnick@mit.edu

Abstract

Cyber risk can underlie the next financial crisis. Increasing trade policies on cross-border financial services have been implemented to manage cybersecurity concerns. Simply complying with the fragmented policies can cause unintended consequences for businesses and can even result in new cyber threats. This study develops a taxonomy to understand the effect of the trade policies for cyber-securing the cross-border financial services. The analysis reveals that a Financial Cybersecurity Action Task Force, where both public and private sectors are involved, is necessary to create and promote cyber norms to balance innovation and systematic cyber risk within cross-border financial systems.

Introduction

The global payments industry continues to deliver healthy growth and is expected to become a $2 trillion industry by 2020 (McKinsey, 2017). The ability to make international financial transactions has allowed for cross-border trade and investments. Cross-border flows have accounted for one-sixth of total transaction values of up to $200 billion globally, split between transaction fees and foreign exchange revenues; this number is increasing by six percent annually (McKinsey, 2019). However, over the last few years, the impact of cyber incidents on international financial systems, from Bangladesh Bank's missing $81 million to Banco de Chile's loss of $10 million, and from Russia's exchange market attack to Mexico's Interbank Electronic Payments network disruption, all indicate one possibility: "*the next financial crisis may well start as a cyber incident*" (Cœuré, 2019). Therefore, we need to understand what cyber risks exist within the cross-border payment services industry to reduce such risks and how such cyber risks are governing within the global environment.

Cross-border financial services are very complex and many new FinTech innovations are emerging daily intending to facilitate the adoption of such a system. In this study, we conceptualize cyber risk as the opportunity structure in digital technologies which may be exploited and result in a breach of confidential information/knowledge, which will damage the competitive advantage provided by confidentiality (Inkpen, Minbaeva, & Tsang, 2019); or violate the integrity, and/or availability which will interrupt the sufficient capability to provide essential services (Boeke, 2018). To get a systematic understanding, instead of looking into specific innovation, we turn to its process so that we can identify the key digital innovations and related cybersecurity risks through the cross-border financial service ecosystem. Inspired by the cyberspace territorialization theory (Lambach, 2019), we look into what the actors, digital innovations, and the policies can exert control on, so that we can identify the three dimensions of cyber risks from the control perspectives: the physical infrastructure, code and algorithms, and data. As an international financial system is actually a highly regulated sector and states are implementing policies to regulate it, and while there are no global rules for cybersecurity, the conflict regulation compliance is raising unique risks for this ecosystem. Furthermore, as states are implementing different trade policies intending to improve the

cybersecurity within the cross-border financial services, this results in highly diversified policy implementations. By investigating the trade policies which are or could be used to impact the cross-border financial services, we identify three main mechanisms including post-sales services requirements like localization requirement, pre-requirement for market access and foreign direct investment restrictions. This enables us to analyze whether the implemented cybersecurity-motivated trade policies are helpful for cross-border financial service ecosystem.

Unfortunately, we observed very limited positive effects in securing the cyber aspects of cross-border financial services. Actually, all the identified trade policies can be implemented in a way to increase the cyber risks, making themselves a problem. Therefore, by investigating the existing global efforts to cyber-secure the cross-border financial services, this study calls for a Financial Cybersecurity Action Task Force like the Financial Action Task Force (FATF) for Anti-money laundering and combating the financing of terrorism. Both public and private sectors should work together to create a more cybersecure cross-border financial service system to support the development of global digitization.

The remainder of this paper is organized as follows. We will discuss the process of cross-border financial services to understand different types of cross-border fintech innovations. By identifying the potential cyber risks and the related trade policies, we further analyze the effect on cybersecurity from the existing trade policies. Following with a discussion of the existing global efforts and the roadmap to build the suggested Financial Cybersecurity Action Task Force, we conclude this article.

FinTech are Reshaping the Cross-border Financial Services

How do international monetary transfers work in the digital age, when a click of a button can send money to someone thousands of miles away? How is it different from mailing a check? The answer to these questions lies within the Society of Worldwide Interbank Financial Telecommunication (SWIFT) and Single Euro Payments Area (SEPA). International bank transfers are similar to inter-bank transfers, except that the bank money is being sent to lies in another country, making the transfer process more intricate. The mechanics of SWIFT and SEPA transfers can take place in two different ways, depending on whether two banks have a direct relationship with each other. In the case that two banks have a direct relationship, meaning that Bank A has a commercial account with Bank B and vice versa, and a client from Bank A wishes to transfer money to a client in Bank B, the following would happen. First, Bank A will send a message via SWIFT/SEPA to Bank B regarding the monetary transfer. Next, once the electronic message is received, Bank A will debit the amount of money in question from the sending client's account then Bank A will credit Bank B, and Bank B will credit the receiving client's account. The direct relationship between these banks facilitates the processing of moving around funds, keeping transaction fees to a minimum. However, in the case that Bank A and Bank B do not have a direct relationship with each other, there will be intermediary players, Bank C or even a Bank D or Bank E in this process, who will assist in the transfer. The more operations behind-the-scenes leads to greater fees being deducted and longer wait times for the transfer to take place. Moreover, if there needs to be a currency transfer in the process as well, that would mean another fee for the exchange.

The long-standing inefficiencies are due to the complexity and lack of transparency in cross-border payment systems that have opened the door for financial technology (FinTech) companies to fill the gap (Agarwal, 2018). It is important to note that it is the messages being sent between banks, instead of actual monetary transfer. Therefore, nascent financial technology companies such as TransferWise, Revolut, and others are changing the way that cross-border payments can be transacted.

The development of FinTech, such as distributed ledger technologies, has been considered promising to facilitate back-end processes in cross-border payments. For example, SWIFT launched its newly minted Global Payments Innovation (GPI) network, which merges real-time payments tracking with an added certainty of same-day settlement for banks within its network. Besides, TransferWise has developed a peer-to-peer (P2P) solution for payments transfers utilizing a matching model in which money is redirected to another recipient of an equivalent transfer in the opposite direction.

New payment methods have been created over these years to advance the existing cross-border payment systems. IBM introduced the Blockchain World Wire payment system on the Stellar network in 2018, stating that the new payment network utilizing digital currency on Stellar's blockchain would *"…accelerate remittances and transform cross-border payments to facilitate the movement of money in countries that*

need it most" (Agarwal, 2018; Mourdoukoutas, 2019). In 2019, the Blockchain World Wire has expanded to 72 countries, 47 currencies, 44 banking endpoints, and more than 1,081 unique currency trading pairs. J.P. Morgan, a commercial and investment banking titan in the U.S., is set to launch its native cryptocurrency, JPM Coin, for cross-border payments (Tsakanikas, 2019). Banks such as Santander and Fidor have partnered with the blockchain-based payment network, Ripple, that can complete cross-border transactions in both a timely and transparent manner.

Financial regulation plays an essential role in reducing the systematic risk of the international financial system. However, the complex and evolving governance structures raise significant challenges for the entire industry. A technology to support the development and compliance of the regulations (RegTech) (Anagnostopoulos, 2018; Arner, Barberis, & Buckley, 2017), has been explored recently to address regulatory challenges. Examples include the electronic Know-Your-Customer (KYC) system, automated compliance monitoring and reporting, and algorithm-based reviews of trading patterns.

Cyber Risk within Cross-border Financial Services

Digital innovations for cross-border payment services using FinTechs are creating new risks, especially concerning cybersecurity. The changing nature of cyber attacks and the growth of cyber risk are driven by factors including advancing technologies, greater interconnections among financial institutions and external parties, and more significant incentives for cybercriminals to target financial bodies (Financial Stability Board, 2017a). This, combined with a lack of coordination and a set of standards among international financial bodies, leaves room for vulnerabilities.

Financial market infrastructures (FMIs), defined as a "*multilateral system among participating institutions, including the operator of the system, used for clearing, settling, or recording payments, securities, derivatives, or other financial transactions*," serve as a set of guidelines and a technical infrastructure to manage risks (Committee on Payment and Settlement Systems & International Organization of Securities Commissions, 2011). They provide participants with platforms for clearing settlements and recording financial transactions to allow for greater efficiency and reduce risks among the network of financial institutions. The business disruptions due to cyber attacks will prevent firms from conducting routine operations, resulting in an operational backlog as well as a loss of revenue. For example, the cyber attack against Banco de Chile in 2018 destroyed 9,000 workstations and 500 servers, as well as compromising endpoint handling transactions on the SWIFT network.

Algorithms behind-the-screen to automate credit approvals or advisories, facilitate regulatory compliance and fraud detection, and automate financial assets trading, play fundamental roles for cross-border payment services. However, the integrity of algorithms, the inherent vulnerability of widely-adopted algorithms, the ethical questions of self-governance (Madnick, 2019; Scharre, 2019), and such, are increasing the systemic risks within the cross-border payment system. For example, the actions of the cybercriminals that breached the Russian Regional Bank resulted in the enormous fluctuations of the ruble-dollar exchange rate in 2015 (Paganini, 2016). Given the wide adoption of algorithmic trading these days, such fluctuations could further trigger "flash crashes."(J. P. Farrell, 2019)

Using cyber operations to manipulate financial data, in particular, poses a distinct set of systemic risks, the risk of collapse of an entire financial system. For example, hackers can use the cross-border "messaging" system to send false transactions. In the 2016 Bangladesh central bank heist, hackers breached the bank's network to send fraudulent transfer requests through the SWIFT network, resulting in $81 million of direct losses (Reuters, 2016). Furthermore, the increasing number of data breach incidents are further empowering the cyber fraud market, presenting cross-border transactions as low-hanging fruit for an attacker. For example, botnets are now being used to test stolen identity credentials and expose fraudulent cross-border transactions (ThreatMetrix, 2019).

Cybersecurity Motivated Policy for Cross-border Financial Services

As discussed above, Fintechs have a growing role to play to enhance the cross-border payment system while the risks from cyber threat are emerging. "*The increasing use of these technologies, though, should be coupled with a strengthening of regulatory oversight over financial activities to safeguard financial stability, as new risks may surface […] Financial digitalization trends heighten the need for cybersecurity*

to protect financial consumers and producers ", highlighted by the IMF report submitted to G20 in 2018 (IMF, 2018). Hence, beyond implementing related regulations to protect financial systems and mitigate potential cybersecurity risks, many countries have imposed limiting cyber trade barriers, intending to reduce the cyber-attack surface area in international financial systems. Based on whether and how the related services are allowed to enter the domestic market, these trade barriers can be grouped into the following categories:

The first related trade restriction focuses on post-sales service requirements such as localization requirements which set requirements on the cross-border financial services in the market. For example, India requires that all payment data held by payment companies be placed in local facilities within the country and the data are not allowed to be exported out of the country, not even for processing (Robert E. Lighthizer, 2019). Turkey requires that payment service providers establish local entities while the information systems handling payment transactions shall also be kept within the country (Taylor, 2014).

The second restriction is related to market access, which requires that service providers meet specific requirements when applying for associated licenses to enter the market. In March 2018, the People's Bank of China (PBOC) formally opened up the gates for foreign investment in the electronic payments market in China, requiring that service providers "*must deploy business operating systems and disaster recovery systems that are secured, compliant and capable of processing payment services independently"* and the "*overseas entities (receiving or processing such information) must be required to undertake corresponding confidentiality obligations*." (Mckenzie, 2018) The EU General Data Protection Regulation (GDPR) committee will require certain information regarding the logic of the algorithm to be provided to the data subject (Kaminski, 2018). Brazil, China, and Indonesia, once either implemented or introduced policies requiring foreign firms to disclose digital source codes (such as the underlying code of business software or smartphone apps) for testing as a prerequisite to operating in those countries, although these requirements are lifted later.

Another restriction stems from the foreign direct investment perspective, given the highly sensitive nature of financial security, to control the market access. The U.S foreign investment risk review modernization act of 2018 (FIRRMA) identifies a number of factors that CFIUS should consider when evaluating national security risks, including whether the transaction will "*pose sensitive U.S. citizen data to exploitation by foreign entities and governments*" or "*exacerbates cybersecurity vulnerabilities or allows a foreign government to gain new capabilities to engage in malicious cyber activities against the U.S."*(Antón & Hemmings, 2019; Grindal, 2019). A blacklist/whitelist system can be further implemented to highlight the potential cyber risk of the provided cross-border services from different nations. The EU highlights the requirement of "*data secure status*," for third counties, where an adequate level of protection is implemented so that the data transfer to those counties is aptly permitted. For example, India currently has no access to intellectual property or other sensitive information due to its lack of data-secure status and India and EU are negotiating such issues in the EU-India free trade agreement (FTA).

Can Trade Policy Cyber-Secure Cross-border Payment Services

Though many different types of trade restrictions regarding cross-border payment services have been implemented, intending to enhance the cybersecurity level. To analyze *whether these restrictions are helpful in reducing potential cybersecurity risks for cross-border financial services in practice*, according to the taxonomy we discussed above, the question can be turned into whether the implemented trade policy can mitigate cybersecurity risks within the financial market infrastructure, algorithm and code, data, and regulation compliance risks.

Firstly, the post-sales service requirements such as the localization requirement for data and information systems does not necessarily correspond to an enhanced level of cybersecurity. Actually, this requirement can even increase the risk of cyber fraud attacks in cross-border payment services as the lack of related data will reduce the efficiency for fraud detection. Also, regarding the uneven development level of the national cybersecurity capability globally (International Telecommunication Union, 2019), the lack of sufficient protection capabilities can put the localized data in the risk of data breaches.

In light of this, there exists the requirement of cybersecurity capabilities and data protection measures for cross-border payment service providers. The purpose of these requirements is to facilitate a standardized minimum cybersecurity level given the evolving nature of cyber attacks. These requirements include

auditing cyber risk from third-party service providers, including the foreign supplier. This is considered crucial when mitigating cyber risk from supply chains (Linton, Boyson, & Aje, 2014; Relihan, 2019). In addition, testing source codes is also suggested as one of the best practices for supply chain cyber risk management. However, the disclosure of source codes can raise concerns regarding intelligent property protection, which is the comparative advantage for many international enterprises (Inkpen et al., 2019). Moreover, the baseline standard and transparency measures of the certification procedures still leave space for concerns (Koch, 2016). For example, the European Commission released the high-risk third counties and regions for money laundering in 2019. As it included four US territories, the U.S. government condemned the blacklist, referring to "*the substance of the list and the flawed process by which it was developed*". Even worse were the lack of protection measures during the testing of provided services, which can increase the risk of data breaches.

Additionally, the financial system is considered critical infrastructure and its cybersecurity is defined as part of national cybersecurity. The "*Security Exception*" is an important principle in the international trade environment, which allows governments to take action when necessary in cases of "essential security interest." (Kho & Petersen, 2019) However, this security exception is considered self-defining, or so-called "self-judging" and it is expected to remain unclear in the near future. This raises many cybersecurity conflicts among nations. For example, on May 15, 2019, the U.S. issued the "executive order on securing the information and communications technology and services supply chain", declaring a national emergency to deal with the threats from information and communication technologies (ICTs). The U.S. Department of Commerce's Bureau of Industry and Security (BIS) then added Huawei Technologies and its affiliates to the "Entity List" which bans U.S. firms from doing business with Huawei (US White House, 2019). To avoid potential investigations from the U.S. CFIUS, when Ant Financial acquired U.K. based currency exchange giant WorldFirst, WorldFirst closed its U.S. arms before the deal (Xie & Dummett, 2019).

Finally, though almost all the stakeholders from each country have implemented some regulations to enhance the cybersecurity for the cross-border financial system, given the complex nature of the related regulations implemented by different authorities, the conflicting regulatory schemes impose significant restrictions for cross-border service providers (Financial Stability Board, 2017b). For example, the payment service directive II (PSD 2) requires banks to release information regarding customer accounts and transaction data to third party providers and encourages the open-banking environment, while the GDPR imposes significant penalties for failing to protect customer data, which makes open banking implementations unattractive and risky.

Table 1 Cybersecurity Effect of Trade Policies within Cross-border Financial Services

<table>
<tr><th colspan="2">Control Perspective</th><td>Financial market infrastructures (FMIs)</td><td>Code and Algorithms</td><td>Data</td></tr>
<tr><td colspan="2">Cyber Risk</td><td>Business Disruptions due to Cyber-attacks; Espionage</td><td>Integrity of algorithms, the Inherent vulnerability of wild-adopted algorithms, Ethical questions of self-governance</td><td>Data breaches and Data Manipulation</td></tr>
<tr><td rowspan="3">Trade Restrictions</td><td>Post-sales Service Requirements like Localization Requirements</td><td>Not helpful but can result in more risk</td><td>/</td><td>Not helpful but can result in more risk</td></tr>
<tr><td>Pre-requirement for Market Access</td><td colspan="3">Positive effect is limited; can raise concerns on intelligent property and data breaches</td></tr>
<tr><td>Foreign Investment Restriction</td><td colspan="2">Not helpful; National Cybersecurity Abuse</td><td>/</td></tr>
<tr><td colspan="2">Regulation Conflict</td><td colspan="3">Not helpful; Increase Risks due to conflict requirements</td></tr>
</table>

It can be seen that although cybersecurity for cross-border payment services is vital for financial stability, current implemented trade policies have limited positive, if not negative, effects in securing the cyber aspects of cross-border financial services. Merely complying with these redundant, sometimes even

conflicting, trade regulations and policies is challenging and may cause unintended consequences such as additional investment requirements or cyber risks. Therefore, given the global and highly regulated nature of financial services, cybersecurity concerns are not just a compliance issue. Instead, business leaders need to balance financial service innovations and potential cyber threats. There is an urgent need for a global effort to harmonize the implemented cybersecurity regulations for cross-border payment services and reduce the potential financial crises due to cyber attacks.

Global Efforts to Secure Cross-border Payment Services

In addition to efforts from individual countries, as summarized in Table 1, we are observing some global efforts to enhance the cybersecurity of financial services institutions. Note that many international institutions such as United Nations (UN), International Telecommunication Union (ITU), European Union (EU), North Atlantic Treaty Organization (NATO), and Shanghai Cooperation Organization (SCO) provide related guidance to improve the cybersecurity resilience of their members. In this paper, we only focus on those global efforts related to cross-border financial services.

The G20 Finance Ministers and Central Bank Governors Meeting in 2017 highlights the cyber threat to national and international financial systems. To enhance cross-border cooperation, the Financial Stability Board (FSB) delivered a stock take of existing regulations and supervisory practices in G20 jurisdictions, as well as existing international guidance, and continued its work in 2018 by publishing a Cyber Lexicon. FSB also prioritized international collaboration in managing operational risk from third-party service providers and mitigating cyber risks. Moreover, the G7 developed the Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector in 2017 to guide and drive discussions regarding cybersecurity risks. A simulation of cyber incidents in the financial sector was hosted at the 2018 G7 Finance Ministers and Central Bank Governors' Meeting, which highlighted the importance of international coordination in response to cyber threats. The International Monetary Fund (IMF) suggested specific recommendations for effective regulatory policy by highlighting the complementary nature between high-level principles and firm-level guidance (Kopp, Kaffenberger, & Wilson, 2017), while the Institute of International Finance (IIF) identified four cyber attack scenarios affecting global financial stability (Boer, 2017). Recommendations including harmonizing international regulations, sharing a common language between the cyber and financial stability communities, understanding the overlay of cyber risk on the plumbing of markets and institutions, and conducting exercise between multi-stakeholder were further emphasized by Brookings in 2018 (Healey, Mosser, Rosen, & Tache, 2018).

Table 2 Global Institutions Governing Cybersecurity within Cross-border Financial Services

GLOBAL INSTITUTION	KEY EFFORT
G20: Finance Ministers and Central Bank Governors Meeting, 2017	Advocate against the malicious use of ICT Enhancing cross-border cooperation
Financial Stability Board, 2018	Develop and promote the implementation of effective regulatory, supervisory, and other financial sector policies Cyber Lexicon; Develop effective practices relating to a financial institution's response to, and recovery from, a cyber incident
G7	The Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector Simulate "the day after" a major cyber incident in the financial sector
IMF	High-level principles and firm-level guidance: Incentivize the implementation of risk management techniques
Institute of International Finance (IIF)	Four cyber attack scenarios affecting global financial stability

Though these efforts are encouraging, the consensus is that cybersecurity within the financial sector can impact financial stability; it is essential to realize that an international organization coordinating international standards, communication, and trade policies for cybersecurity issues within cross-border financial services is nonexistent. Such organizations are urgently needed.

Call for The Financial Cybersecurity Action Task Force

To manage the systematic cybersecurity risk within the cross-border financial services, the efforts on Anti-money laundering (AML) and combating the financing of terrorism (CTF) from the Financial Action Task Force (FATF) offer successful examples.

The Financial Action Task Force (FATF) has been established since 1989 to implement and monitor effective anti-money laundering programs. It has been shown that the FATF does help in reducing money laundering activities (Johnson & Desmond Lim, 2003). FATF is said to be a guideline that "sets standards and promote[s] effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system," expecting its members to adopt such standards and measures, as well as maintain "blacklists" of jurisdictions with strategic deficiencies in their frameworks for AML/CTF. Being placed on such lists has the joint consequences of limiting the associated country's financial institutions' ability to conduct business with others, and increasing the costs of maintenance in accessing the global financial resources. These deterrents greatly assist the FATF in achieving remarkable success in generating an international policy environment to harmonize domestic regulatory policies with each other regarding AML/CTF. Furthermore, cyber launderings, which use digital payment services including e-commerce, digital currency, online games, and crowdfunding, have posed specific challenges for AML/CTF. These activities are also covered by FATF Forty Recommendations and Nine Special Recommends (FATF, 2018b). The FATF also developed a comprehensive approach to ensure a sufficient level of oversight on virtual currency activities for AM and TF (FATF, 2018a).

Though AML/CTF and cybersecurity risks are not equal, the three critical features for the success of FATF are inspiring for the efforts to cyber secure the cross-border financial service system: the success of institutional implementations, the standard assessment schema, and sanctions mechanism. Therefore, it is necessary to call for The Financial Cybersecurity Action Task Force (FCATF), to secure the cyber environment for cross-border financial services. The implementation of such organizations will offer institutional power to promote cybersecurity collaborations within global efforts, develop cybersecurity norms within cross-border financial services, and harmonize the increasingly complex regulations system.

Regarding the dynamic nature of cybersecurity risk for cross-border financial services, the standard assessment schema should consist of a consistent, continuously improving, and flexible evaluation standard and procedure, including a convergence in international taxonomies of cybersecurity and cyber attacks in the financial services sector as well as a standardized reporting method and time limit to report data breaches. Besides the maintenance of such standards, the FCATF should include the effort to implement the protection measures revealing sensitive information, and serve as a coordinator for the independent third-party services pentest service providers.

In addition, this FCATF should also implement related mechanisms, such as the blacklist/whitelist, to deter risky cybersecurity practices and reward the adoption of better cybersecurity practices. Unlike the FATF, such a blacklist shouldn't necessarily stay at the national level but can extend to the firm level to highlight those service providers offering highly risky financial services. Being listed in such blacklist should significantly impact the service providers' capability to enter the cross-border financial service market. On the other hand, this FCATF could implement related funding to support innovation in cybersecurity, enhancing technology, and improving the consumers' cybersecurity awareness for cross-border financial services. These strategies will incentivize services providers and regulators to consider cybersecurity and manage the associated cyber risks.

Leaders for The Financial Cybersecurity Action Task Force (FCATF)

To facilitate the implementation of such institution, we identified the international organizations which have significant overlap responsibility in financial services or cybersecurity, including the G20, G7, FSB, World Bank (WB), IMF, IIF, WTO (General Agreement on Trade in Services, GATS), Basel Committee on Banking Supervision, and Global Financial Innovation Network (GFIN). We further check the official purpose of these organizations, their authority representatives and the capability to act, to identify the ideal candidate for this FCATF.

As the FSB is an international forum that monitors and makes recommendations for developments regarding the global financial system, we expect that FSB can play a leading role in promoting the implementation of this organization. Given the responsibility of the FSB to "coordinate at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory, and other financial sector policies" and the impact from cyber attacks on financial stability, the FSB should take the lead and work together with other international organizations, including FATF, WB, IMF, IIF and WTO etc., to construct a global policy environment. This would include synchronizing domestic regulatory and trade policies, developing an assessment standard, reducing regulation conflict, and promoting collaboration for cyber attack detection, prevention, and response, for cross-border payment services.

Along with the FSB, the IIF should use its experience within the public-private collaboration for financial services to promote cybersecurity risk management. The IIF is an international association of financial institutions created by 38 founding banks of leading countries. Currently, it has membership from 70 countries and 450 members including financial institutions such as commercial and investment banks, asset managers, hedge funds, wealth funds, and central banks. The stated purpose is to "support the financial industry in the prudent management of risk; to develop sound industry practices; and to advocate for regulatory, financial, and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth." Additionally, the Egmont Group, a united body of 164 Financial Intelligence Units (FIUs) provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing, can add significant value to draw upon operational experience to inform policy considerations. Therefore, IIF and Egmont Group can be candidates for collaboration with the FSB to construct a set of effective practice-oriented cyber norms and the sanction/reward mechanism to incentivize the adoption of these practices.

From a private participation perspective, GFIN, a collaboration of 29 organizations including IMF and WB, aims to provide firms with a "global sandbox" in which trials of emerging cross-border FinTech solutions can take place. This sandbox allows for nations, organizations, and firms to think responsibly about the feasibility and implementation of cybersecurity perspectives and play a potential role within the FCATF to implement the blacklist and whitelist strategy, as well as the third-party evaluation service pools described in this paper.

Conclusion

Building a cyber-secure cross-border financial service system is a critical cornerstone mission for the digital society. The emerging digital innovations across financial market infrastructures (FMIs), codes and algorithms, and data are reshaping the ecosystem. However, the accompanying cybersecurity risks due to the adoption of information technologies require the balance between digital innovation and cybersecurity risk. Though states are implementing trade policies intending to improve the cybersecurity within the cross-border financial services, based on the developed framework, our analysis shows that the positive effect is insignificant. Instead, these trade policies themselves actually can raise other cyber risks, not to mention that they can have a negative impact on innovative activities and digital trade (Agrawal, Gans, & Goldfarb, 2019; Goldfarb & Tucker, 2012). The solution to manage cybersecurity risks to avoid the financial crisis may result in a financial crisis. Therefore, managing the cybersecurity concerns for cross-border financial services within the digital trading environment is not just a regulation compliance issue. It requires global collaboration, including both industry sectors and policymakers, to work together a set up a rule to manage cybersecurity risk systematically. To achieve that goal, setting up a Financial Cybersecurity Action Task Force, it is essential to reduce the possibility of financial crisis from cyber attacks. FSB, IIF, Egmont Group and GFIN can be good candidates to lead such efforts.

Importantly, the institutional arrangement and configuration behind such a Financial Cybersecurity Action Task Force to guarantee its performance (Lall, 2017) is critical to achieve its objectives in a cost-effective manner, which will open up opportunities for future work. For example, a further investigation on how to balance the national and corporate interests and achieve the de facto policy autonomy given the trend of cyberspace reterritorialization (H. Farrell & Newman, 2020; Lambach, 2019), and how to initiate the coordination among existing efforts including FATF and FSB are valuable.

Acknowledgements

The research reported herein was supported in part by the MIT Internet Research Policy Initiative, which is funded by the Hewlett Foundation, Cybersecurity at MIT Sloan, which is funded by a consortium of organizations, and MIT Policy Lab at the Center for International Studies (MIT IPL). We would like to thank the editors and reviewers for providing constructive feedback and comments on earlier versions of this article.

References

Agarwal, S. (2018). Will fintechs dominate the cross-border payments market? Retrieved August 1, 2020, from https://bankingblog.accenture.com/will-fintechs-dominate-cross-border-payments-market?lang=en_US

Agrawal, A., Gans, J., & Goldfarb, A. (2019). AI and International Trade. In *The Economics of Artificial Intelligence* (pp. 463–492). https://doi.org/10.7208/chicago/9780226613475.003.0019

Anagnostopoulos, I. (2018). Fintech and regtech: Impact on regulators and banks. *Journal of Economics and Business*, *100*, 7–25. https://doi.org/10.1016/j.jeconbus.2018.07.003

Antón, A. I., & Hemmings, J. (2019). Recognizing Vendor Risks to National Security in the CFIUS Process. Retrieved August 1, 2020, from Lawfare website: https://www.lawfareblog.com/recognizing-vendor-risks-national-security-cfius-process

Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech, regTech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law and Business*, *37*(3), 373–415.

Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance*, *31*(3), 449–464. https://doi.org/10.1111/gove.12309

Boer, M. (2017). Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system. *Institute of International Finance*, (September). Retrieved from https://www.iif.com/system/files/iif_cyber_financial_stability_paper_final_11_13_2017_clean.pdf

Cœuré, B. (2019). The new frontier of payments and market infrastructure: on cryptos, cyber and CCPs. Retrieved August 1, 2020, from https://www.bis.org/review/r181115a.html

Committee on Payment and Settlement Systems, & International Organization of Securities Commissions. (2011). *Principles for financial market infrastructures - Consultative report*. Retrieved from http://www.bis.org/cpmi/publ/d94.pdf

Farrell, H., & Newman, A. L. (2020). Choke Points. *Harvard Business Review*, (February).

Farrell, J. P. (2019). Of Flash Crashes, Hidden Actors, And Nasty Implications. Retrieved August 1, 2020, from https://gizadeathstar.com/2019/04/of-flash-crashes-hidden-actors-and-nasty-implications/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+GizaDeathStar+%28Giza+Death+Star%29

FATF. (2018a). *FATF Report to G20 Finance Ministers and Central Bank Governors*. Retrieved from www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-fm-cbg-july-2018.html

FATF. (2018b). The FATF Recommendation. Retrieved August 1, 2020, from http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF Recommendations 2012.pdf

Financial Stability Board. (2017a). *Stocktake of Publicly Released Cybersecurity Regulations , Guidance and Supervisory Practices*. (October). Retrieved from http://www.fsb.org/wp-content/uploads/P131017-2.pdf

Financial Stability Board. (2017b). *Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices*. Retrieved from http://www.fsb.org/wp-content/uploads/P131017-1.pdf

Goldfarb, A., & Tucker, C. (2012). Privacy and Innovation. *Innovation Policy and the Economy*, *12*, 65–90. https://doi.org/10.1086/663156

Grindal, K. (2019). Trade regimes as a tool for cyber policy. *Digital Policy, Regulation and Governance* , *21*(1), 19–31. https://doi.org/10.1108/DPRG-08-2018-0042

Healey, J., Mosser, P., Rosen, K., & Tache, A. (2018). The Future of Financial Stability and Cyber Risk. *Brookings Institution*, (October), 1–18.

IMF. (2018). *Future of Work: Measurement and Policy Challenges*. 1–40. Retrieved from https://www.imf.org/external/np/g20/pdf/2018/071818a.pdf

Inkpen, A., Minbaeva, D., & Tsang, E. W. K. (2019). Unintentional, unavoidable, and beneficial knowledge

leakage from the multinational enterprise. *Journal of International Business Studies*, *50*, 250–260. https://doi.org/10.1057/s41267-018-0164-6

International Telecommunication Union. (2019). Global Cybersecurity Index 2018. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Johnson, J., & Desmond Lim, Y. C. (2003). Money laundering: has the Financial Action Task Force made a difference? *Journal of Financial Crime*, *10*(1), 7–22. https://doi.org/10.1108/13590790310808556

Kaminski, M. E. (2018). The Right to Explanation, Explained. *SSRN Electronic Journal*, (July), 17–40. https://doi.org/10.2139/ssrn.3196985

Kho, S., & Petersen, T. (2019). Turning the tables: The United States, China, and the WTO national security exception. *China Business Review*, *2018*(August), 5–9.

Koch, D. D. (2016). Is the HIPAA Security Rule Enough to Protect Electronic Personal Health Information (PHI) in the Cyber Age? *Journal of Health Care Finance*, *43*(3).

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability. *IMF Working Papers*, *17*(185), 1. https://doi.org/10.5089/9781484313787.001 M4 - Citavi

Lall, R. (2017). Beyond Institutional Design: Explaining the Performance of International Organizations. *International Organization*, *71*(2), 245–280. https://doi.org/10.1017/S0020818317000066

Lambach, D. (2019). The Territorialization of Cyberspace. *International Studies Review*, 1–25. https://doi.org/10.1093/isr/viz022

Linton, J. D., Boyson, S., & Aje, J. (2014). The challenge of cyber supply chain security to research and practice - An introduction. *Technovation*, *34*(7), 339–341. https://doi.org/10.1016/j.technovation.2014.05.001

Madnick, S. (2019). The Ethics of AI: What Happens When Humans Can't Agree on What is "Right?" *The Wall Street Journal*, 1. Retrieved from https://blogs.wsj.com/experts/2019/10/17/the-ethics-of-ai-what-happens-when-humans-cant-agree-on-what-is-right/

Mckenzie, B. (2018). PBOC Announced Rules for Foreign-Invested Payment Service Providers to Operate Electronic Payment Services in China. Retrieved August 1, 2020, from https://www.bakermckenzie.com/en/insight/publications/2018/03/pboc-announced-rules

McKinsey. (2017). Global payments 2017: Amid rapid change, an upward trajectory. Retrieved August 1, 2020, from https://www.mckinsey.com/industries/financial-services/our-insights/global-payments-2017-amid-rapid-change-an-upward-trajectory

McKinsey. (2019). A vision for the future of cross-border payments. Retrieved August 1, 2020, from https://www.mckinsey.com/~/media/McKinsey/Industries/Financial Services/Our Insights/A vision for the future of cross border payments final/A-vision-for-the-future-of-cross-border-payments-web-final.ashx

Mourdoukoutas, P. (2019). Bitcoin And Stellar Get Another Boost From IBM. Retrieved August 1, 2020, from Forbes website: https://www.forbes.com/sites/panosmourdoukoutas/2019/03/19/bitcoin-and-stellar-get-another-boost-from-ibm/#141259942d80

Paganini, P. (2016). Russian Metel group manipulated ruble-dollar exchange rate with malware. Retrieved August 1, 2020, from https://securityaffairs.co/wordpress/44376/cyber-crime/metel-hackers-exchange-rate.html

Relihan, T. (2019). These Are the Cyberthreats Lurking in Your Supply Chain. *SSRN Electronic Journal*, (February), 1–6. https://doi.org/10.2139/ssrn.3370577

Reuters. (2016). Spelling Mistake Prevented Hackers Taking $1bn in Bank Heist. Retrieved from Guardian website: http://www.theguardian.com/business/2016/mar/10/spelling-mistake-prevented-bank-heist

Robert E. Lighthizer. (2019). 2018 National Trade Estimate Report on Foreign Trade Barriers. Retrieved from Office of the United States Trade Representative website: https://ustr.gov/sites/default/files/files/Press/Reports/2018 National Trade Estimate Report.pdf

Scharre, P. (2019). Killer apps: The real dangers of an AI arms race. *Foreign Affairs*, *98*(3), 135–144.

Taylor, M. (2014). Turkey Introduces New E-Payment Rules To Tackle Deficit And Terror Funding. Retrieved August 1, 2020, from PaymentsCompliance website: https://paymentscompliance.com/sites/paymentscompliance.com/files/attachments/page/Turkey Introduces New E-Payment Rules To Tackle Deficit And Terror Funding.pdf

ThreatMetrix. (2019). 9 Key Cybercrime Trends for Financial Institutions in EMEA. Retrieved August 1, 2020, from https://www.threatmetrix.com/digital-identity-blog/cybercrime/9-key-cybercrime-trends-financial-institutions-emea/

Tsakanikas, N. (2019). JP Morgan Set to Launch its Own Native Cryptocurrency for Cross-Border

Payments. Retrieved August 1, 2020, from Blokt website: https://blokt.com/news/jp-morgan-set-to-launch-its-own-native-cryptocurrency-for-cross-border-payments

US White House. (2019). Executive Order on Securing the Information and Communications Technology and Services Supply Chain.

Xie, S. Y., & Dummett, B. (2019). Ant Financial to Acquire U.K.'s WorldFirst. *The Wall Street Journal*, *Feb*. Retrieved from https://www.wsj.com/articles/alibaba-affiliate-ant-acquires-u-k-s-worldfirst-11550146173