CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

APRIL 2020

Cyber Policy Initiative Working Paper Series | "Cybersecurity and the Financial System" #6

Cyber Mapping the Financial System

Jan-Philipp Brauchle, Matthias Göbel, Jens Seiler, and Christoph von Busekist

Cyber Mapping the Financial System

Jan-Philipp Brauchle, Matthias Göbel, Jens Seiler, and Christoph von Busekist

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

Cybersecurity and the Financial System

Carnegie's working paper series 'Cybersecurity and the Financial System' is designed to be a platform for thought-provoking studies and in-depth research focusing on this increasingly important nexus. Bridging the gap between the finance policy and cyber policy communities and tracks, contributors to this paper series include government officials, industry representatives, and other relevant experts in addition to work produced by Carnegie scholars. In light of the emerging and nascent nature of this field, these working papers are not expected to offer any silver bullets but to stimulate the debate, inject fresh (occasionally controversial) ideas, and offer interesting data.

If you are interested in this topic, we also invite you to sign up for Carnegie's FinCyber newsletter providing you with a curated regular update on latest developments regarding cybersecurity and the financial system: CarnegieEndowment.org/subscribe/fincyber.

If you would like to learn more about this paper series and Carnegie's work in this area, please contact Tim Maurer, Co-director of the Cyber Policy Initiative, at tmaurer@ceip.org.

Papers in this Series:

- "Lessons Learned and Evolving Practices of the TIBER Framework for Resilience Testing in the Netherlands" Petra Hielkema and Raymond Kleijmeer, October 2019
- "Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment" Lincoln Kaffenberger, Emanuel Kopp, September 2019
- "Cyber Resilience and Financial Organizations: A Capacity-building Tool Box," Tim Maurer and Kathryn Taylor, July 2019
- "The Cyber Threat Landscape: Confronting Challenges to the Financial System" Adrian Nish and Saher Naumaan, March 2019
- "Protecting Financial Institutions Against Cyber Threats: A National Security Issue" Erica D. Borghard, September 2018
- "Toward a Global Norm Against Manipulating the Integrity of Financial Data" Tim Maurer, Ariel (Eli) Levite, and George Perkovich, March 2017

About the Authors

Jan-Philipp Brauchle, Matthias Göbel, Jens Seiler, and Christoph von Busekist work in the Directorate General Financial Stability at Deutsche Bundesbank.

Introduction

Cyber risks present a growing threat for individual agents in the financial system: banks, insurers, central counterparties, and the like. However, cyber events may also have the potential to destabilize the financial system as a whole. While dedicated microprudential regulatory and supervisory regimes are in place or are being developed to manage cyber risks especially at credit institutions, what is lacking is a systemic view of cyber risks that particularly sheds light on concentrations and contagion channels that are material to the financial system.

In consideration of the foregoing, this qualitative analysis aims to offer a systemic perspective on cyber risks, one that can be regarded as both contrary and thus complementary to the rather micro-prudential (bottom-up) view on cyber risk until now. Furthermore, this approach complements the existing macroprudential analysis that focuses on structural and cyclical systemic risk emanating from the financial sector—such as credit and liquidity risk—by adding a new perspective on, among other things, concentration risk and contagion channels that are "cyber specific." In order to visualize the systemic peculiarities inherent to cyber risks, this paper differentiates between two networks, the financial network and the cyber network, proposed by these authors. Whereas the term "financial network" refers to the elements of the financial system (or financial sector), the term "cyber network" encompasses those elements of information and communication technology (ICT) that represent the underlying infrastructure for all the operational processes in the financial network. As this paper shows, such a two-network approach examines both the unique character of cyber risks in terms of risk formation, concentration, and spillovers within the cyber network and—far more important to financial stability—the interdependencies between these two networks, illustrating in particular how cyber risks can cause systemic risk in the financial sector.

Building on this integrative two-network approach, the paper formulates a conceptual methodology (called "cyber mapping") to reveal the pertinent cyber risk structures a financial system can be exposed to, including structures that may subject it to an additional degree of vulnerability aside from financial stability risks emanating from the financial network itself (see table 1).

Resting upon the concept of the two networks, our approach starts by identifying the systemically important actors in the financial network. This step is necessary because, as a rule, the prerequisite for a systemic cyber event in the financial sector is a large enough cyber attack on a systemically important institution (fulfilling the criteria of size, substitutability, and interconnectedness) with potentially severe consequences for the whole financial system.[1] In order to identify systemically important actors in the financial system, this paper draws on international or national conventions as well as expert judgment. Next, it elaborates that not every cyber event impacting a systemically important actor may be regarded as a systemic cyber event. After this clarification, it identifies the elements in the cyber network that are systemically important for the financial sector and the risk they pose for financial institutions. By means of a generic scenario analysis, this analysis focuses on the interdependence between both networks and their relevant players to reveal

TABLE 1

Network spillovers and financial stability risk

Spillover . . .	. . . to Financial network	. . . to Cyber network
. . . from Financial network . . .	Endogenous systemic risk to financial stability caused by, for example, systemic credit and liquidity risk within the financial network	No systemic risk to financial stability
. . . from Cyber network . . .	Exogenous systemic cyber risk to financial stability caused by, for example, concentration risk in the cyber network that can spill over to and destabilize the financial system	No systemic risk to financial stability

critical nodes and risks at a systemic level that could potentially threaten financial stability. In this context, financial stability can be defined as a state in which the key macroeconomic functions, that is, the allocation of financial resources and risks as well as the settlement of payment transactions, are performed efficiently—particularly during unforeseen events, stress situations, and periods of structural adjustment.[2] The qualitative approach's results may serve as a theoretical blueprint for deepened empirical analysis of systemic cyber risks. While there is broad consensus on the identity of systemically important actors in the financial network, systemically important actors and parts of the cyber network have not yet been comprehensively identified. Hence, the need for further data on the cyber network is evident. With regard to cyber incidents, this study deploys a set of necessary and supplementary conditions to define a systemically important cyber incident and provides a potential classification system for systemically important cyber incidents. Further, the analysis identifies characteristics of systemic cyber incidents. While some of them, such as cyber attacks' independence from financial cycles, are similar to attributes of operational risks, others are distinct.

Literature on Systemic Cyber Risks

In recent years, several researchers and institutions have taken a system-wide perspective on cyber risks as a potential threat to financial stability.[3] For example, as a contribution to the Organization for Economic Cooperation and Development (OECD) project Future Global Shocks, Sommer and Brown state that although very few cyber-related events could cause a global disruption, governments need to prepare to withstand and recover from such accidents or attacks.[4] This study is

notable for investigating the impact of these global shocks with a view not limited to the financial system, but rather to society as a whole. In contrast, Kopp, Kaffenberger, and Wilson describe cyber risk as a threat to financial stability and a textbook example of systemic risk.[5] They identify the exposure to access vulnerabilities, concentration risk, correlation risk, and contagion risk as the main sources for this. Only a few authors challenge the view of cyber risk as a systemic one. Danielsson, Fouché, and Macrae, for example, claim that almost all cyber risk is microprudential and that a cyber attack would have to coincide with other noncyber events in order to have a systemic impact.[6]

In terms of how systemic cyber risks might materialize, the literature focuses on various scenarios and transmission channels. Most authors examine the potential disruption of services of a systemically important institution or of a critical function of the financial system as a potential threat to financial stability.[7] The Institute of International Finance further looks at the consequences of leakage, of loss or compromised integrity of data, and of the failure of general infrastructure utilities such as transport, electricity, or telecoms.[8] In terms of transmission channels, the Bank of England views the interconnectedness of the financial system as a possible damage amplifier for transmitting a successful attack on a systemically important institution into the financial system as a whole.[9] Possible transmission channels of a cybersecurity event in the financial system are also the focus of a paper by the Office of Financial Research.[10] Here, the authors suggest three channels of transmission, namely lack of substitutability, loss of confidence, and the loss of data integrity.

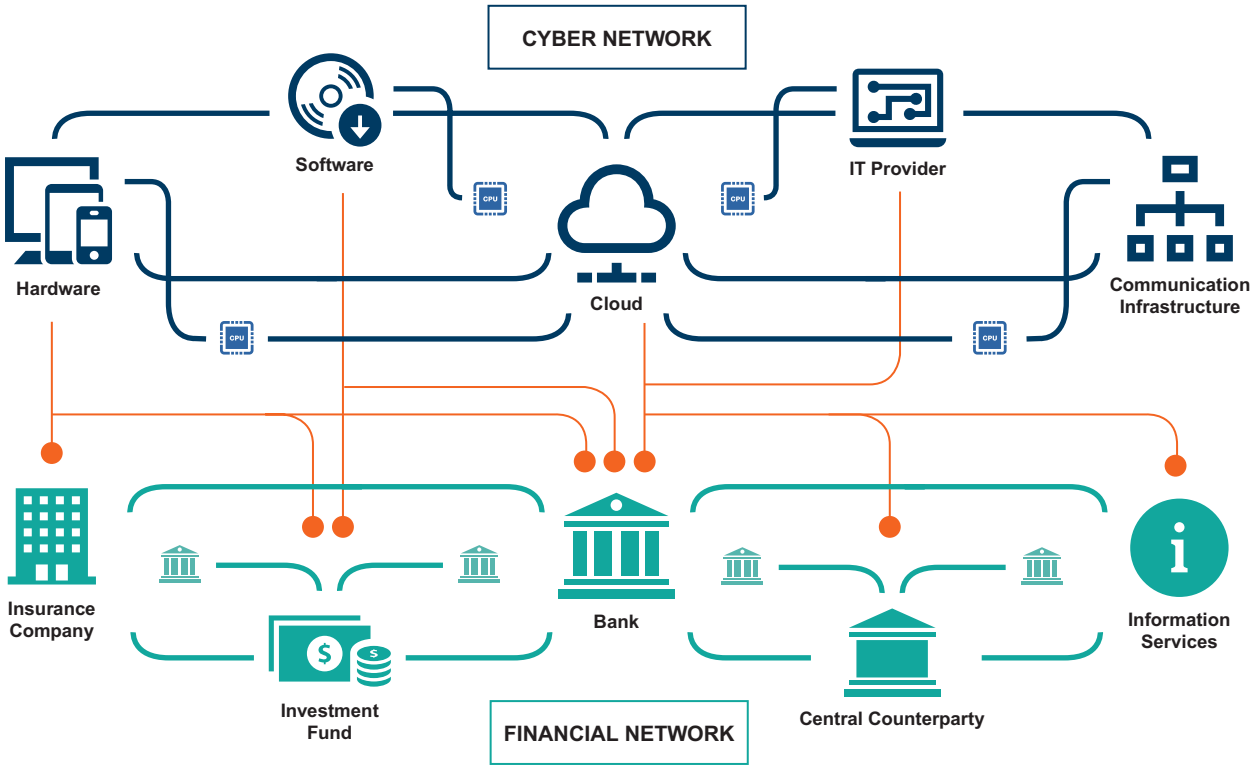
While the present analysis builds on existing literature, it develops a different systematic approach to systemic cyber risks applied to the financial system. In order to do this, a new perspective on systemic cyber risk is introduced by distinguishing between the so-called cyber network and the financial network (also known as the financial system). Taking a separate look at the cyber network allows analysts to carve out its specific functions for the financial system from a systemic risk perspective. This provides the conceptual groundwork for shedding light on risk concentrations and transmission channels conveyed across the whole financial system. In addition, the present analysis goes further in elaborating on the conditions that define a systemic cyber incident.

Exploring Cyber Risks

Unlike conventional analyses of financial stability, which in many cases explore credit, market, and liquidity risks; their concentration; and financial contagion channels, cyber risks are located on a different analytical stratum. In the present analysis, one could say that the cyber network is separated from but connected to the financial network representing the financial system (see figure 1).

FIGURE 1

Interaction Between Cyber and Financial Networks (Schematic Diagram)



This figure was developed by the authors and represents some of the relationships between cyber and financial networks. It is not intended as a complete description of the full network.

= representative of broader network components

Figure 1 shows in principle and on aggregate how the financial (for example, lending) relationships between the individual agents in the financial system and with other sectors (nonfinancial corporations, households, general government) are mapped technically by a cyber network and flanked by communicative connections. Here, the term "cyber network" encompasses those elements of information and communication technology (ICT such as software, hardware, and communication service providers) that represent the underlying infrastructure for all the operational processes in the financial network. Some nodes directly connect both networks—for example, nodes where credit institutions use certain software products or insurers enlist the services of information technology (IT) service providers. These nodes are important because they are the potential points of entry where cyber risks can materialize in the financial system. For example, IT service providers performing core functions of financial institutions in an outsourcing capacity by providing their services to a critical mass of financial system agents or to a systemically important financial institution may

destabilize the financial system once hit by a severe cyber attack. Similar effects are conceivable regarding software products being used as off-the-shelf solutions in the whole financial system—not just for individual participants but potentially for participants in their entirety as well—if what are known as exploits take widespread advantage of security gaps and software malfunctions.[11] Besides these risks, any analysis of cyber risks from a financial stability vantage point also needs to consider threat scenarios that mainly involve the communicative element of the cyber network. In times of fake news, cyber attacks can be used to disseminate manipulated information across social media or to infiltrate the systems of data providers (for example, exchanges and market data providers) in the financial system, almost in real time. In combination with automated trading processes such as algorithmic trading, this could be a source of market disruption, at least temporarily.

Cyber risks exhibit certain characteristics and propagate differently to conventional economic risks within the financial network, for example, because their effects are nonlinear. As a case in point, a cyber attack can rapidly transmit stress impulses to a multitude of recipients simultaneously (including recipients that are not linked to each other economically, such as by means of financial relationships), potentially destabilizing not just parts of the financial system but all of it, at least for a period. The impact of cyber attacks can be multiplied not just by targeting more than one victim but also by mounting multiple attacks simultaneously. At the same time, cyber risks can also go undetected for months and inflict damage (to the detriment of financial stability) in victims' systems. These examples show that cyber risks can materialize regardless of typical (namely, economic or financial) cycles in the financial system or its structural characteristics or particular sectoral makeup. Furthermore, what is inherent to cyber risk is a degree of intent that is not known to a similar extent in the context of conventional economic risk and that materializes in the case of purposeful cyber attacks.

The resilience of the cyber network ("cyber resilience") is key to financial system stability. A cyber network is said to be resilient in financial stability terms if it prevents destabilizing cyber attacks on the financial system. Key framework conditions for cyber resilience include the technical state of IT equipment in a more general sense. Outdated IT equipment tends to be more vulnerable to today's cyber attacks than a state-of-the-art IT setup. Another condition is the technological protection against cyber risks provided, for example, by running antivirus programs and keeping them up to date. One further condition for cyber resilience consists in its regulatory framework conditions and compliance with them. These conditions can stipulate compliance with technical standards or organizational and risk management considerations (for example, International Organization for Standardization/International Electrotechnical Commission norm ISO/IEC 27001). Awareness of cyber risks among employees in the financial network likewise has a bearing on financial system resilience. One final point worth raising in this inexhaustive account of the factors impacting cyber resilience is the capability to detect and fend off cyber attacks. Where cyber attacks have been successful, it is crucial to contain their impact as much as possible—for example, by switching to emergency systems—and to be able to resume the normal functioning of IT operations (business continuity).

Financial Network: Identifying Critical Financial System Agents

Cyber mapping begins by taking an aggregate bird's-eye view of the financial sector. Identifying systemically important players in the financial network is a precondition for analyzing potential destabilizing spillovers from the cyber network to the financial network. This is because one successful cyber attack that hits just one of these systemically important agents can evolve into a direct threat for the financial system as a whole. In effect, the process of identifying systemically important agents is derived from regulatory conventions and expert judgment (see table 2).

However, a cyber attack on a critical number of nonsystemically important agents can likewise present a risk to financial stability. That critical mass does not necessarily need to consist of elements from one and the same sector. To this effect, an attack could conceivably be made on a group of heterogeneous agents that belong to different sectors but all use the same off-the-shelf software or cloud provider. Thus, even though the financial system can be broken down into individual sectors, the topic of cyber risks should always be considered from an intersectoral perspective as well.

TABLE 2

Systemically Important Agents in the Financial Network

Sector	Systemic Importance
Banks	Global Systemically Important Banks according to the assessment methodology developed by the Basel Committee on Banking Supervision (BCBS)[12] and Other Systemically Important Institutions according to the guidelines of the European Banking Authority (EBA)[13]
Insurers	Global Systemically Important Insurers according to the assessment methodology by the International Association of Insurance Supervisors (IAIS)[14]
Financial market infrastructures	Assumed to be systemically important according to international standards outlined in the Principles for Financial Market Infrastructures[15]
Asset managers/investment funds	Not systemically important based on expert judgment
Central banks	Assumed to be systemically important
External Credit Assessment Institutions (rating agencies)	The so-called big three assumed to be systemically important based on expert judgment
Information service providers	Assumed to be systemically important depending on reach/market control
External sector	Assumed to be systemically important depending on external trade links

Categorizing Systemic Importance

Not every targeted cyber attack or cyber event affecting the aforementioned systemically critical elements of the financial network will be systemically important. Rather, the question of whether a cyber event at a systemically important financial institution or at multiple financial institutions will indeed destabilize the financial system will depend above all on which functions or services are disrupted or disabled at the institutions affected. Bearing this in mind, the institutional stock-taking exercise described and carried out in table 2 needs to be augmented by a functional perspective that identifies the system-critical functions and services rendered by those entities. A cyber attack on these functions could well destabilize the financial system (functional channel). The present analysis refrains initially from grading functions according to their systemic importance and instead proceeds based on the general and simplified working hypothesis that a cyber attack on one or more agents identified as being systemically important to the financial system will per se also have a destabilizing effect, regardless of which particular functionalities are impacted by that kind of attack.

Even if the above conditions—namely, that a cyber attack is carried out on systemically important financial market agents, their functions, or their services—are met, that does not suffice to identify an event as being systemically important. Supplementary conditions characterizing the attack itself and its repercussions also need to be met and include the following.

Event Duration

While short-term disruptions or failures of systemically important agents or services may impair the financial system, it should normally be possible to bypass them by applying robust business continuity plans. For example, the Principles for Financial Market Infrastructures state that "an FMI [financial market infrastructure] should have a business continuity plan that addresses events posing a significant risk of disrupting operations, including events that could cause a wide-scale or major disruption. The plan should incorporate the use of a secondary site and should be designed to ensure that critical (IT) systems can resume operations within two hours following disruptive events. The plan should be designed to enable the FMI to complete settlement by the end of the day of the disruption, even in case of extreme circumstances. The FMI should regularly test these arrangements."[16]

Bearing this in mind, then, one could draw the concrete conclusion that when considering the systemic importance of a cyber event, any disruption of financial market infrastructure that lasts more than two hours and/or prevents settlement by the end of the day could arguably be considered systemically important. It would appear reasonable to apply this consideration to other systemically important agents since they, too, are often expected to provide their services within similarly short deadlines during normal operations. In this sense, a disruption period that impairs or prevents end-of-day settlement should be deemed systemically important.

Financial Loss

Another supplementary condition for a systemic cyber incident and possible transmission channel of a cyber shock to the whole financial system is the minimum financial loss caused by a cyber event (financial channel). Here again, the thinking goes that not every financial loss caused by a cyber event, including indirect losses, will necessarily be of systemic proportions. What is basically needed, then, is a definition of financial dimensions for loss events that, if exceeded because of a cyber event, can be deemed systemically important. Regarding banks, for example, the level of capital can be regarded as a threshold that, when absorbed or exceeded by losses incurred due to a cyber event, can turn a nonsystemic cyber incident into a systemically important one.

Loss of Confidence

Cyber events that impair critical functions of the financial system but are remedied quickly and cause only a minor financial loss can nevertheless be of systemic proportions if such events or a burst of similar events—even if they individually have negligible implications—erode confidence in the proper functioning of the financial system (confidence channel).[17] A similar impact via the confidence channel can be caused by using communication tools (such as Twitter) to unsettle the public regarding the functionality of the financial system or parts of it.

Naturally, it will probably be difficult to categorize a cyber event as systemically important because of its impact via the confidence channel. It might be helpful to use qualitative classifications based on surveys, for example, that determine which events in the financial system had impaired confidence among market participants. To solve this issue pragmatically, these authors suggest taking a cyber event's media coverage as a proxy for the impact via the confidence channel. For example, the number of newspapers, the duration, and the range of media coverage (such as cross-regional or cross-country) may give an impression of the potential destabilizing impact of a cyber event via the confidence channel.

Elements of the Cyber Network

After analyzing the circumstances in which a cyber event that impacts the financial sector could be deemed systemically important (at least potentially), this paper looks closer at the cyber network as the origin of these kinds of cyber events. The term "cyber network" encompasses those ICT elements that form the underlying infrastructure for all operational processes in the financial network. Due to limited publicly available data, the elements of the cyber network were only identifiable on an abstract level. The key technical components of IT infrastructure are software, hardware, and built-in devices used to operate applications software. The provision of such infrastructure is increasingly being outsourced to third-party IT service providers or delivered by means of cloud computing on

the internet or a dedicated link service. In addition, the analysis attributes a central role in the cyber network to a global provider of secure financial news and payment services, the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Finally, not only IT but also state-of-the-art communications infrastructures, especially social media, play a significant role when analyzing cyber risks. This section briefly outlines the risks to the financial system posed by elements of the cyber network.

- **Software**: The decisive factor, both actively and passively, at work in the overwhelming majority of cyber attacks is software. Actively, hackers use all manner of malicious software to infiltrate and damage systems. Passively, vulnerabilities in a company's software represent the main point of entry for cyber attacks. The extent and intensity of software-related cyber risks depend considerably on whether the software is off-the-shelf or customized, with off-the-shelf software used by a multitude of financial institutions presenting a larger surface for large-scale cyber attacks.
- **Hardware**: Hardware can be manipulated, for instance, by modifying it using additional structural components, changing existing circuits, tampering with chips, or modifying firmware. Tampering with automated teller machines (ATMs), point-of-sale systems, and credit cards or electronic cash (EC) cards are cases specific to the financial sector. Centralized hardware, such as in computer centers, often poses the hazard of concentration risk where the hardware is used by multiple enterprises.
- **Cloud Computing**: The National Institute of Standards and Technology (NIST) lists resource pooling as one of the essential characteristics of cloud services. The provider's resources are pooled to serve multiple customers using a multi-tenant model. This means that, by definition, the various users of cloud services depend on a cloud service provider and its IT infrastructure to function properly. This dependence gives rise to heightened concentration risk. Considerable problems include not only impaired cloud service availability but also threats to data confidentiality or integrity caused by attacks on cloud services.
- **IT Outsourcing**: IT outsourcing includes surrendering the power to control and monitor organizational areas that have high operational relevance and that are frequently closely interlinked with other material organizational areas. In that vein, failure of computer centers or ATMs and self-service machines, disruptions in the core banking system, or the loss or corruption of sensitive customer data during cyber attacks on the IT service provider can, if inadequate precautions have been taken, evolve into a major risk to the firm, prevent the performance of system-critical functions, or cause long-term reputational damage.
- **SWIFT**: Banks, insurers, market infrastructures, and businesses are interlinked globally by the services SWIFT provides, especially by the shared use of this platform and by uniform communication standards. This makes SWIFT an enticing target for potential cyber attacks. SWIFT occupies a unique position in the international payments segment, especially in

correspondent banking. More than 11,000 financial institutions in more than 200 countries and territories can directly exchange payment instructions via the SWIFT network, a coverage no other service provider can offer.

- **Social Media**: Inadequate oversight of social media leaves open massive scope for manipulation and influencing at various levels. Thus, fake news can be spread easily via social networks, in a targeted and unfiltered manner, reaching numerous users virtually in real time without impartial review. Social bots masquerading as fake profiles that unleash masses of comments on a topic, thereby influencing the public debate or spreading fake news, may serve as potential catalysts. These communication stimuli can sap the public's confidence in the functioning of the financial system or parts of it, for example, the creditworthiness of a single credit institution. They can also be amplified in the financial system through, for instance, automated trading algorithms that scan the internet and social media for certain keywords and make transaction decisions within seconds based thereupon, which can then lead to considerable price fluctuations known as "flash crashes."

Cyber Risks to Financial Stability

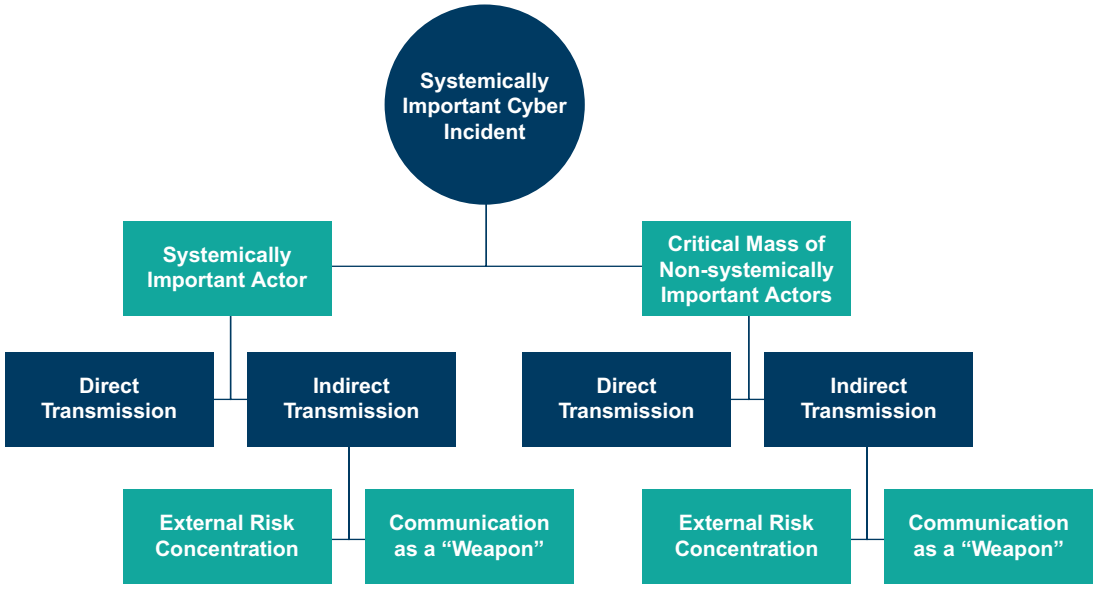
Based on the considerations so far, the connection of the financial and cyber networks reveals new critical nodes and risks at a systemic level that could potentially threaten financial stability. In other words, interfaces between the cyber network and financial network open up new channels of risk transmission capable of destabilizing the financial system.

Essentially, one can differentiate between direct and indirect transmission of cyber incidents (see figure 2).

Direct Transmission

The classification "direct transmission" of a cyber incident comprises all attacks that directly impact the IT infrastructure of an individual systemically important agent or a critical mass of nonsystemically important agents of the financial network. The attacker can act either individually or in a group. Methods of attack vary (for example, they can be advanced persistent threats, denials of service, or ransomware)[18] and can be targeted at any and all components of the IT infrastructure of one or more financial network agents. Exploiting vulnerabilities in software products represents an effective way of striking a group of financial market agents at the same time. Through such vulnerabilities, attackers can infiltrate computer systems and tamper with them. Owing to the widespread use of off-the-shelf software the number of potential victims is staggeringly high. Moreover, such attacks are simple to carry out (by means of phishing e-mails), very successful, and scalable ad infinitum.[19]

FIGURE 2
Classification of Systemically Important Cyber Incidents



SOURCE: Bundesbank

Indirect Transmission

The classification "indirect transmission" of a cyber incident comprises all attacks that do not directly impact the IT infrastructure of an individual systemically important agent or a critical mass of nonsystemically important agents of the financial network, but rather use technological or communicative leverage to impact them. In addition, two scenario categories can be distinguished: an attack on a third-party service provider (for example, a cloud service provider) or via the malicious use of communication infrastructure (communication as a weapon).

External Risk Concentration

The increasing tendency in the financial sector to outsource IT entails further potential risks to financial stability. One is that an attack on a cloud or IT service provider could also cause problems for a systemically important institution that has outsourced certain services. Another is that outsourcing certain processes or services to either a cloud or an IT service provider helps to create new networks between financial system agents and cyber network agents. IT service providers assume a pivotal role within these networks, acting as nodes and thus creating concentration risk between their individual clients: financial system agents. A successful attack on the availability of a cloud service provider or an IT service provider would send a shockwave through the network and could,

Data as a Target in Need of Protection

Data is one of the most valuable assets in the digital world. This also makes it one of the assets most worthy of protection. A common goal of cyber attacks is the so-called CIA triad of information security. This triad comprises the confidentiality, integrity, and availability of data. A severe attack on the CIA triad of critical information could have systemic consequences in multiple ways. For one, such an attack could hinder the affected institution's operations or cause financial losses. Further, a large-scale misuse of a critical mass of data could lead to a significant loss of confidence in the affected institutions even if the financial or operational consequences for them are negligible. This might be achieved by a cyber attack that destroys the integrity of multiple banks' critical data. Integrity can be compromised by manipulating the data in such a way that it is impossible to tell if and which data was falsified. If such a case were made public, it could have severe consequences for the confidence in these banks, the interbank market, and even the financial system as a whole. Similar consequences could arise from a massive leak of confidential—for example, prudential—information on a group of financial institutions. This breach of confidentiality could impact the reputation of the affected financial institutions, the prudential authority, and the system as a whole.

in a single blow, deny multiple users of these services (for example, multiple financial system agents) access to the outsourced services or functions. The more monopolistic the service provider is in the cyber network, the more impact this attack would have, because it might not be possible, despite the available technology, to switch to an alternative service provider. Depending on the length and severity of the disruption, this could cause considerable turmoil among the affected customers. In this case, the shock of the cyber attack would transmit to the financial system through a functional channel and consequently could threaten financial stability.[20] This makes cloud service providers and IT service providers external risk nodes for the financial network according to the two-tier network approach of this analysis.

The risk posed by cloud or IT service providers presents two parallels to structures that came under increasing scrutiny by regulators following, among other things, the 2008 financial crisis. One was that agents important to financial stability (such as insurers or money market funds) exist, a fact that had not been identified by supervisors until then. In response to the financial crisis, these entities came under tightened regulation and oversight following 2008. It is necessary to analyze whether cloud service providers and IT service providers could potentially play a similar role in the financial network. Another is that, particularly in the aftermath of the collapse of Lehman Brothers, people's eyes were opened to the opaqueness of certain markets, especially in

trading with over-the-counter (OTC) derivatives, and to the great dangers this created. In the case of IT service providers, too, it would be advisable from a regulatory perspective to assign financial system agents directly and by name to their respective cloud or IT service providers. This would enable the network structure to be disclosed, which is necessary to identify connections, nodes, and risk points.

Communication as a Weapon

The risks that fake news and data leaks pose for businesses can be transposed to the financial system at large. On a sufficiently large scale, such attacks could also unleash massive turmoil throughout the financial system—for example, via the confidence channel—thus threatening financial stability.[21] A widespread disclosure of confidential—for example, prudential—information on a group of financial agents could have a similar effect. Reputational losses for the affected companies and the financial system at large would also be at play here. Looking at the potential proliferation of fake tweets, the rapid repudiation of such tweets as a bogus post may help soothe the jitters on the markets. Besides, automated communication protocols and responses to such attacks may be an effective way of repudiating such fake news quickly and credibly.

Conclusion

This qualitative study has underscored the need to take a systemic view of cyber risks, one that augments the microprudential coverage of these risks as a subset of the operational risk of individual entities by adding the potential for those risks to jeopardize the stability of the financial system as a whole. By linking the concept of the cyber network introduced in this analysis with the financial network, the study identified various potential scenarios of systemically important cyber events and their properties. It then subdivided the aforementioned scenarios into various categories of systemic cyber risk and described the key transmission channels (functional, financial, and confidence channels) between the cyber network and the financial system.

The study lays the conceptual groundwork for an extensive cyber map showing which systemically important functions of the financial network can be mapped to which specific elements of the cyber network.[22] The next steps will involve fleshing out this approach by, first of all, specifically identifying the agents and structures of the cyber network, namely its systemically important agents for the financial system. In addition, cyber events need to be systematically monitored on the basis of a uniform taxonomy, the results of which could then be input into a cyber register.

Looking ahead, it would make sense to integrate systemic cyber risks into the structured macroprudential analysis of other financial stability risks (for example, credit, market, and liquidity risk) in order to, among other things, better understand the interplay between these categories of risk.

It would also need to be clarified, for instance, which factors are relevant to diagnosing a systemic cyber shock (such as duration and impact) and where to place the threshold above which a systemically important cyber shock is deemed to exist. A further step would be to discuss the extent to which quantitative simulations of cyber shocks (called "cyber stress tests") and their impact on the financial system are possible and how they differ from the modeling of conventional shocks.

Notes

[1] It should be mentioned here that a financial stability risk could also arise from an attack on various individually nonsystemically important financial actors that add up to a systemically important mass of actors.

[2] Deutsche Bundesbank, "Financial Stability Review 2017," November 2017.

[3] World Economic Forum (WEF), "Understanding Systemic Cyber Risk," Global Agenda Council on Risk & Resilience, October 2016.

[4] Peter Sommer and Ian Brown, "Reducing Systemic Cybersecurity Risk," Organisation for Economic Cooperation and Development (OECD), January 2011.

[5] Emanuel Kopp, Lincoln Kaffenberger, and Christopher Wilson, "Cyber Risk, Market Failures, and Financial Stability," International Monetary Fund Working Paper no. 17/185, 2017.

[6] Jon Danielsson, Morgane Fouché, and Robert Macrae, "Cyber Risk as Systemic Risk," VoxEU.org, August 2016, https://voxeu.org/article/cyber-risk-systemic-risk.

[7] Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO), "Guidance on Cyber Resilience for Financial Market Infrastructures," June 2016; Danmarks Nationalbank, "Financial Stability 1st Half 2016," May 2016.

[8] Martin Boer and Jaime Vazquez, "Cyber Security & Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System," Institute of International Finance, September 2017, https://www.iif.com/Portals/0/Files/IIF%20Cyber%20Financial%20Stability%20Paper%20Final%2009%2007%202017.pdf?ver=2019-02-19-150125-767.

[9] Bank of England, "Financial Stability Report," no. 37, July 2015, https://www.bankofengland.co.uk/-/media/boe/files/financial-stability-report/2015/july-2015.pdf?la=en&hash=DFC8B08B2EAB1ECE3A77939A41A914C6297C0F12.

[10] Office of Financial Research (OFR), "Cybersecurity and Financial Stability: Risks and Resilience," OFR Viewpoint 17-01, February 15, 2017, https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf.

[11] Exploits are small pieces of malicious code that infiltrate software by taking advantage of security gaps and malfunctions in auxiliary or application programs in order to manipulate PC activity (such as admin rights) or disable internet servers.

[12] Basel Committee on Banking Supervision (BCBS), "Global Systemically Important Banks: Revised Assessment Methodology and The Higher Loss Absorbency Requirement," July 2018, https://www.bis.org/bcbs/publ/d445.pdf.

[13] European Banking Authority (EBA), "Guidelines On The Criteria To Determine The Conditions of Application of Article 131(3) of Directive 2013/36/EU (CRD) in Relation to The Assessment of Other Systemically Important Institutions (O-SIIs)," December 16, 2014, https://eba.europa.eu/sites/default/documents/files/documents/10180/930752/964fa8c7-6f7c-431a-8c34-82d42d112d91/EBA-GL-2014-10%20(Guidelines%20on%20O-SIIs%20Assessment).pdf.

[14] International Association of Insurance Supervisors (IAIS), "Global Systemically Important Insurers: Updated Assessment Methodology," June 16, 2016, https://www.iaisweb.org/page/supervisory-material

/financial-stability-and-macroprudential-policy-and-surveillance/file/61179/updated-g-sii-assessment-methodology-16-june-2016.

[15] Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO), "Principles for Financial Market Infrastructures," April 2012.

[16] Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO), "Principles for Financial Market Infrastructures," Principle 17, Key Consideration 6, 2012. CPMI and IOSCO, "Guidance on Cyber Security for Financial Market Infrastructures," 2016.

[17] An example of this phenomenon can be found in Office of Financial Research, "2016 Financial Stability Report," page 41: "Malicious actors often target customer account information. Although unfortunate, so far most of these hacks have been one-off events, hurting just the victim firm and its customers. A wide-reaching theft, however, could cause a broader loss of confidence. This occurred in South Korea in 2014. Customer names, credit card data, and phone numbers were stolen from a consumer credit rating firm, the Korea Credit Bureau. The news triggered a run on the country's banks, and many people cancelled credit cards. However, reaction to the breach did not grow into a full-blown crisis."

[18] For a brief description of potential methods of attack, see Bally, "The Big Cyber Threats Breakdown: Types of Cyber Attacks," Cybertraining 365 Blog, March 24, 2017, http://blog.cybertraining365.com/2017/03/24/big-cyber-threats-breakdown-types-cyber-attacks/.

[19] The global cyber attack by the WannaCry malware program, which infected over 230,000 computers in 150 countries in May 2017, is a cautionary example of what can happen. The malware exploited a security vulnerability in Microsoft Windows, encrypted certain user data after infecting a computer, and demanded a ransom in order to release the files (known as a ransomware attack). The program then independently sought out further computers in the network in order to infect them. This caused the attack to spread quickly and uncontrollably to various countries; its victims came in all types (individuals, business enterprises, the public sector). See European Union Agency for Cybersecurity (ENISA), "WannaCry Ransomware Outburst," May 15, 2017, https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst.

[20] A case in point (though the financial sector was not the focus of the attack) was the glitch that knocked out the server infrastructure of Amazon Web Services (AWS) in Northern Virginia, United States, on February 28, 2017. An incorrect input by a software technician disabled many servers for several hours, denying AWS customers access to their data and preventing them from executing transactions. This affected fifty-four of the one hundred largest U.S. online retailers, along with firms such as Dropbox, Coca-Cola, and Spotify. The outage is estimated to have caused losses of $150 million among S&P 500 companies alone. See Nick Wingfield, "Miscue Calls Attention to Amazon's Dominance in Cloud Computing," *New York Times*, March 2017, https://www.nytimes.com/2017/03/12/business/amazon-web-services-outage-cloud-computing-technology.html.

[21] One example of this was the attack on the Associated Press (AP) news agency's Twitter account on April 23, 2013. Hackers issued a fake tweet to AP's over 1.9 million followers reporting an explosion in the White House and injuries to then U.S. president Barack Obama. Despite the fact that AP responded immediately and reported the tweet as false, the Dow Jones and S&P 500 indices dropped considerably within just a few minutes (a time span in which, for instance, high-frequency traders can instrumentalize

the plummeting stock prices to their own ends). Although the markets recovered their losses very quickly, the event shows the potential implications of such an attack. See Tim Bradshaw, Arash Massoudi, and Kara Scannell, "Bogus terror tweet sparks shares blip," *Financial Times*, April 2013, https://www.ft.com/content/33685e56-ac3d-11e2-a063-00144feabdc0.

[22] Such mapping would provide answers to the question of, for instance, which systemically important financial system agents are using which specific software and hardware solutions, cloud providers, and IT service providers.

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org