Economic Commentary

A cyber attack can affect financial stability

Lukas Elestedt, Ulrika Nilsson and

Carl-Johan Rosenvinge

NO. 8 2021, 19 May

SVERIGES RIKSBANK

Table of contents

Economic Commentaries

Economic Commentaries are brief analyses of issues with relevance for the Riksbank. They may be written by individual members of the Executive Board or by employees at the Riksbank. Employees' commentaries are approved by their head of department, while Executive Board members are themselves responsible for the content of the commentaries they write.

Summary

Lukas Elestedt, Ulrika Nilsson and Carl-Johan Rosenvinge
The authors work in the Financial Stability Department of the Riksbank.

As the financial sector becomes increasingly digitalised, its vulnerability to cyber attacks increases. This development is taking place at the same time as advanced cyber attacks are becoming more frequent and overall this means that cyber risks for the financial sector are increasing. Cyber risk differs from other operational risks, partly because cyber attacks can come from malicious threat actors. Cyber risk is also characterised by speed and scalability, where a cyber attack has the potential to spread rapidly and widely.

The conclusion of this analysis is that a cyber attack can affect financial stability, and that cyber risk thus constitutes a systemic risk. The analysis describes how a cyber attack on the financial sector or its critical service providers can directly affect financial stability, if the agent or agents affected are sufficiently critical and the impact of the attack is sufficiently serious. Even in cases where the direct impact of the attack is limited, there is a risk that the consequences of the attack will have negative repercussions which will be exacerbated and spread further in the financial system, for example in the form of a lack of confidence in the system.

In order to limit cyber risk in the financial system, it is essential that every agent understands both what needs to be protected and what it needs to be protected against. Measures aimed at preventing and stopping cyber attacks need to be complemented by the ability to detect, respond and recover from them. In order to improve resilience, good coordination between authorities and the financial sector concerning cyber risk and long-term planning to reduce the vulnerability of the financial system are important.

The authors would like to thank Johanna Stenkula von Rosen, Kristian Jönsson, Olof Sandstedt, Caroline Jungner and Kevin Aytap for their valuable input. The views expressed in this Economic Commentary are the authors' personal opinions and are not to be regarded as the Riksbank's view in these issues.

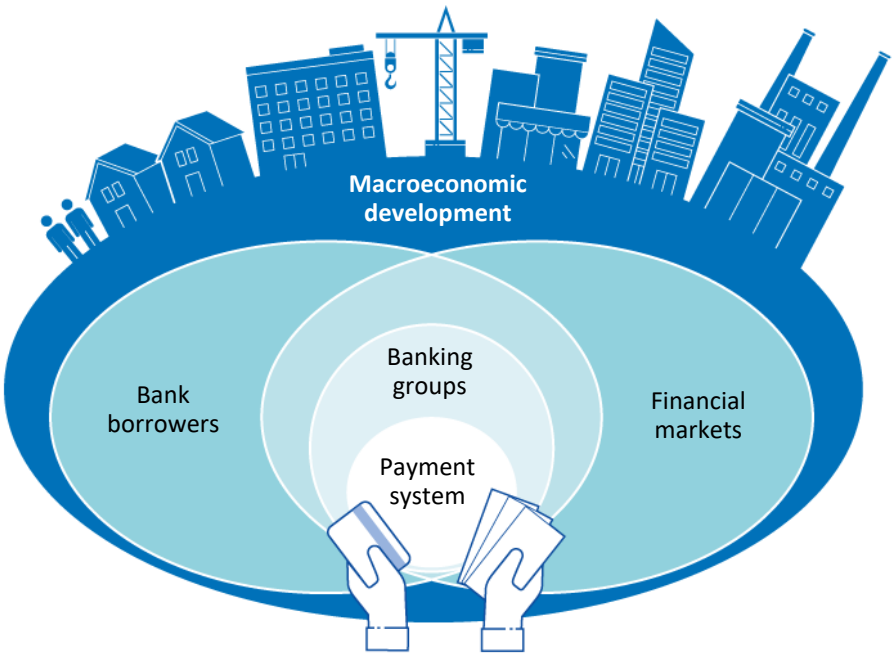
---

1 Introduction

Cyber attacks are attracting more and more attention in society. These attacks have the potential to affect authorities and companies as well as private individuals. The financial sector is no exception. According to the Bank for International Settlements (BIS), the financial sector is facing a greater number of cyber attacks than other sectors.[1]

The financial sector consists of agents operating within the financial system. These include, for example, banks and infrastructure companies whose functions are crucial for the functioning of the financial system, and ultimately of the Swedish economy. As financial companies have a special function and a special status, they are regulated in a special arrangement.[2] One way of illustrating the overall structure of the financial system and its importance for stable macroeconomic development is as in Figure 1 below.

Figure 1. Illustration of the structure of the financial system



Source: Sveriges Riksbank.

At the centre of the financial system are payment systems and other financial market infrastructures (FMIs). These are closely linked to banks, and together they form the core of the financial system. The financial infrastructure and banks form a basis for functioning financial markets and sufficient credit supply in the system. For a func-

[1] Se I. Aldasoro, L. Gambacorta, P. Giudici and T. Leach (2020), The drivers of cyber risk, *BIS Working Papers No 865*. Bank for International Settlements.

[2] See *The Riksbank and financial stability*, 2013. Sveriges Riksbank.

tioning economy, the financial system needs to carry out a wide array of key economic functions, called critical functions, in a reliable and robust manner.[3] This includes, for example, the provision of services related to such things as payments and settlement, interbank loans, transaction and savings accounts, and derivatives and securities trading. Ultimately, therefore, a functioning financial system is a prerequisite for stable macroeconomic development.

Today, the critical functions of the Swedish financial system are maintained almost exclusively by digital means. Far-reaching digitalisation has resulted in banks and FMIs now being entirely dependent on their IT environments to provide services. At the same time, these environments have grown rapidly and become increasingly interconnected and complex. This applies to the IT systems of banks and FMIs, but also to their third-party suppliers and technical infrastructure such as telecommunications and energy supply.[4] This development has increased the vulnerability of the financial system and has also occurred in combination with a widening of the threat landscape and an increase in advanced cyber attacks.[5]

This publication illustrates how a cyber attack could lead to financial instability. We also describe what cyber risk is and how it differs from other risks, the importance of understanding the threat landscape in order to adequately manage cyber risk, the role of the state and the need for coordination and collaboration between authorities and the financial sector.

2 What is cyber risk?

Cyber risk is defined by the Financial Stability Board (FSB) as the combination of the probability of cyber incidents occurring and their impact. A cyber incident is an event in an information system that jeopardizes the security of the information system or violates security policies, whether resulting from malicious activity or not.[6] The concept of risk here differs from that of companies in the financial sector, for example, which actively take risks in order to obtain a higher return. This relates to financial risks, which may include liquidity risk, market risk or credit risk, for example. However, financial companies are also exposed to operational risks, which, unlike financial risks, are not the direct result of a trade-off between risk and expected return. An operational risk can be defined as the risk of loss, disruption, interruption or damage to reputation from inadequate or failed internal processes, people, systems, or external

[3] See, for example, Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms.

[4] See, for example, *Financial Stability Report*, May 2016. Sveriges Riksbank. and F. Adelmann, J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz and C. Wilson (2020) Cyber Risk and Financial Stability: It's a Small World After All, *IMF Staff Discussion Note*. International Monetary Fund.

[5] See *National Defence Radio Establishment Annual Report 2020*, March 2021. National Defence Radio Establishment and *National Defence Radio Establishment Annual Report 2018*, January 2019. National Defence Radio Establishment.

[6] See *FSB Cyber Lexicon*, November 2018. Financial Stability Board.

events.[7] Cyber risk can be seen as part of operational risk, but often has certain characteristics that distinguish it from more traditional operational risks.

Normally, the Riksbank uses the FSB definition of cyber risk. However, in order to simplify the analysis of this economic commentary, we will instead use the concept of cyber risk for incidents that are the result of an attack initiated by malicious actors.

2.1 Cyber risk differs from traditional operational risks

The threat posed by antagonistic actors means that cyber risk is significantly different from other operational risks (apart from traditional fraud risks) faced by financial companies. In addition to this, cyber risk can be characterised by two other aspects[8]: speed and scalability. Speed means that a cyber attack can spread very quickly through affected IT environments. In many cases, the attack can be designed for just that purpose. Scalability means that many different companies around the world use similar hardware and software, and a cyber attack has the potential to spread very widely. This may be intentional but also unintentional. One example of this, outside the financial sector, is the NotPetya[9] cyber attack, which in 2017 hit a far wider circle than originally intended. For example, the Danish shipping company Maersk was hit very hard, despite probably not being the target of the attack.[10]

It is difficult to obtain reliable statistics on cyber attacks

There are estimated to be considerable hidden statistics regarding cyber risk, which makes it difficult to produce statistics in order to calculate it. The financial sector is generally used to having good access to data to calculate risks. However, when it comes to cyber risk, the lack of reliable data is a problem, especially at sectoral level. The problems of quantifying cyber risk are largely due to the weak incentives for affected companies to report serious cyber incidents to authorities, owners and other stakeholders. There is, in itself, a risk associated with being transparent and informing about it. At the same time, it is favourable for the society as a whole if more incidents are reported, so that the statistics and level of knowledge would be improved. In addition, the collection of statistics is further complicated since the advanced, and thus the most relevant, intrusions are in many cases the most difficult to detect.

In order to address the problem of data shortages, analysis is generally attempted based on data components that instil the greatest confidence. This results in, among

[7] See, for example, *Principles for Financial Market Infrastructures*, April 2012. Bank for International Settlements and the International Organization of Securities Commissions and *Principles for the Sound Management of Operational Risk*, June 2011. Bank for International Settlements.

[8] See, among others, *Systemic Cyber Risk*, February 2020. European Systemic Risk Board.

[9] NotPetya is a so-called "cryptoworm" that began to spread in 2017 and, through encryption of critical files, prevented the user from starting the operating system.

[10] See T. Gustafsson and D. Lindahl (2019), Cyber defence – skill needs practice*, FOI Memo 6867*. Swedish Defence Research Agency. And E. Zouave and M. Jaitner (2019), Säkra leverantörskedjor för styrsystem [Secure supply chains for control systems], *FOI-R—4759* In Swedish only with English summary. Swedish Defence Research Agency.

other things, the number of intrusions being a common measure of cyber risk.[11] However, from a systemic risk perspective, this is an inadequate measure, as it is the potential consequences of the intrusion that are of most importance. This type of measure also becomes very sensitive to how a cyber attack is defined. Cyber attacks can be unsophisticated and more or less automated attempts to access an organization's system, but also more sophisticated and successful in, for example, disabling an organization's critical functions. In other words, one cyber attack can be very different from another, both when it comes to the focus and procedure but also the consequences from the attack. This difference makes definitions important.

The problems with statistics described above do not, of course, directly affect the risk itself. However, it means that the risk becomes more difficult to track and affects the ability to make appropriate decisions, which can potentially affect the vulnerabilities and thus indirectly the risk.

3 A cyber attack can affect financial stability

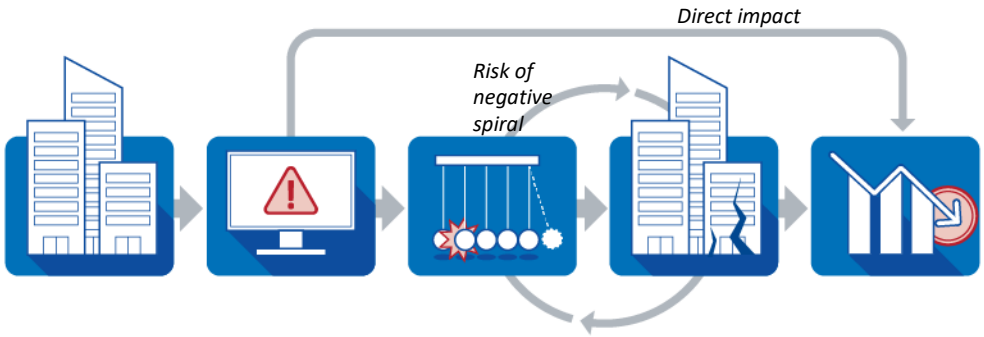
By cyber risk, we mean in this publication a combination of the probability of an incident of antagonistic origin occurring and its impact jeopardising the security of an organization's information system. As cyber attacks can affect financial market participants, they can also potentially impact financial stability and constitute a systemic risk. [12] In view of the importance of the financial system to the national economy, a cyber attack on the financial sector may ultimately pose a threat to a functioning economy.

Figure 2 below illustrates how a cyber attack can be divided into five different stages: the target of the attack, the direct impact of the attack, the potential contagion effects of the attack, the indirect impact of the attack, and the overall impact of the attack on financial stability. From a financial stability perspective, a cyber attack can be said to start when one or several agents are affected by it. These can either be financial agents or third-party suppliers to the financial sector. The next aspect is direct impact, i.e. how these agents are affected by the attack by, for example, certain services becoming unavailable. Subsequently, these effects can be spread further in the financial system, which in turn may indirectly affect the same agent even more or affect others. The final stage is when this impact on individual agents becomes so great that financial stability is also affected.

[11] See F. Adelmann, J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz and C. Wilson (2020) Cyber Risk and Financial Stability: It's a Small World After All, *IMF Staff Discussion Note*. International Monetary Fund, for a discussion on how to improve the quality and availability of data for cyber attacks.

[12] Systemic risk entails a risk of disruption to the financial system with the potential to have serious negative effects on the real economy, see for example *The Riksbank and Financial Stability*, February 2013. Sveriges Riksbank, or *Systemic Cyber Risk*, February 2020. European Systemic Risk Board.

Figure 2. How a cyber attack can affect financial stability



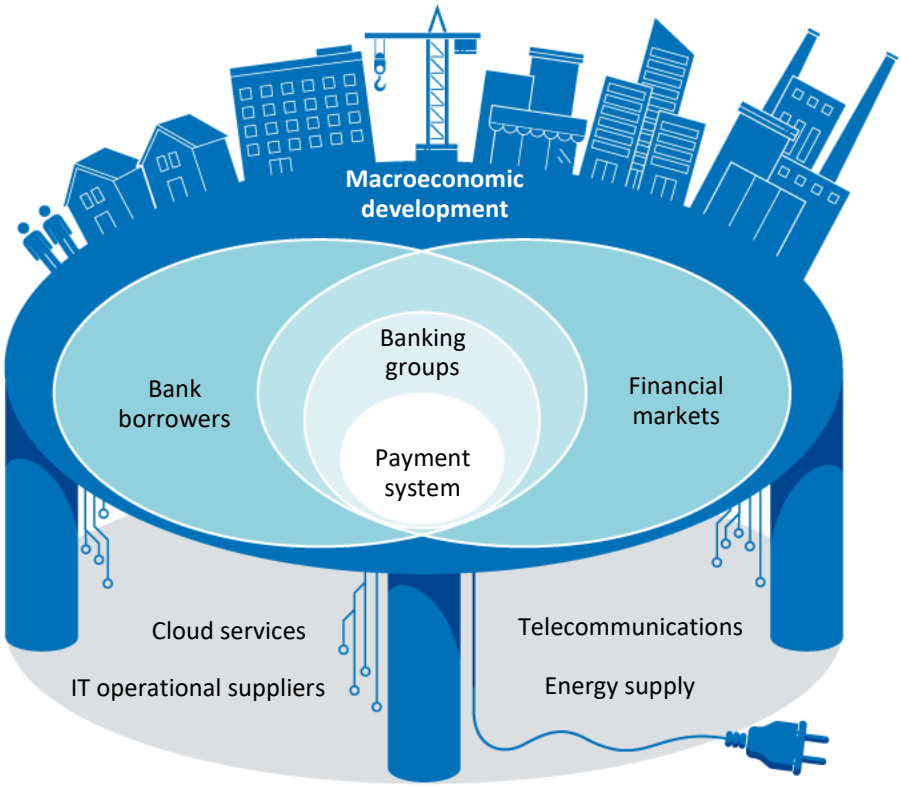
Source: The European Systemic Risk Board, the International Monetary Fund and Sveriges Riksbank.

1. Target of the attack – the starting point of the cyber attack

When analysing a cyber attack from a financial stability perspective, it can be seen as an attack starting with one or more agents being affected by it, see *Target of the attack* in Figure 2. The cyber attack is initially aimed at *one* systemically important financial company, *several* financial companies or at a third party supplier to the financial sector.[13] Third-party suppliers to the financial sector are, for example, those relating to IT operations, software, cloud services, energy supply and communication. To cover this in the illustration in Figure 1, we must extend it so that third party services are also included as critical services supporting the functions of the financial system and ultimately the macro economy, see Figure 3 below.

[13] See *Systemic Cyber Risk*, February 2020. European Systemic Risk Board.

Figure 3. Critical services support the functions of the financial system



Source: Sveriges Riksbank.

2. Direct impact – initial consequences of the cyber attack

The next step is how one or more agents hit by a cyber attack are affected by it, see *Direct impact* in Figure 2. Here we refer to what technical and operational impact a cyber attack may have initially. This stage is therefore about the consequences of a cyber attack and not the probability of one occurring.

As mentioned in the introduction, the financial system needs to carry out a number of critical functions. There are large values that move through the Swedish financial system every day, which makes the system vulnerable to disruptions. For example, around SEK 670 billion is traded daily in the Riksbank's central payment system for large-value payments, RIX.[14] The financial system relies on robust information and communication technology to perform these critical functions.

Furthermore, the financial system depends on critical information in these systems, which need to be protected. Confidentiality, integrity and availability (also known as the CIA[15]) are three key aspects that constantly recur when it comes to cyber security and protecting information. They can be defined as follows:

[14] See Sveriges Riksbank, *The Payment System - RIX*, last updated 5 March 2021. Retrieved 8 May 2021 https://www.riksbank.se/en-gb/payments--cash/the-payment-system---rix/

[15] CIA – abbreviation for Confidentiality, Integrity, Availability.

- Confidentiality: to preserve the secrecy of the information and to prevent unauthorized access to it
- Integrity: to preserve the integrity of the information and to prevent it from being altered or manipulated illegally
- Availability: To maintain access to the information to authorized persons and prevent it from being destroyed or otherwise made unavailable[16]

From the perspective of financial stability, and also from the perspective of the individual agent, one of the most critical aspects is that operations can continue. Thus, the importance of maintaining availability is central. However, it may in some cases be worse to allow operations to continue if the information of one or more financial agents has been manipulated. It is therefore also important to uphold the integrity aspect.[17] If confidentiality is affected to a large extent, it can also have a negative impact on the systemic level. Several common types of cyber attacks on an agent can affect both availability and integrity aspects. Often, a cyber attack means that several, and sometimes all, of these aspects are affected in the same attack. For companies and private individuals, this could manifest itself in many different ways, depending on the purpose, objectives and approach of the attack, for example through problems of accessing Internet or mobile banking, incorrect balance information, incorrect ownership data for securities or problems in executing transactions.

The impact of a cyber attack can also vary depending on the agent affected. For example, if there are only one or a few agents who offer certain critical functions, a cyber attack on these can lead to an important function not being possible to maintain at all. This means that *inadequate substitutability* where there are no alternatives to certain services, such as the central payment system for large-value payments[18], may affect financial stability. Disruptions in this critical function could in turn lead to knock-on effects in a large part of the financial system.[19]

3. Potential contagion effects – how the consequences of the attack can be spread and amplified

After the initial impact of the attack, its effects can spread further or be amplified, see *Potential contagion effects* in Figure 2. In the case of NotPetya, as mentioned above, the contagion occurred rapidly and on a large scale. The effects affected about 10% of Ukraine's computers and also spread far beyond the country's borders.[20]

[16] For example, see *Vägledning i säkerhetsskydd, Informationssäkerhet [Guidance in protective security, Information security*, September 2020. In Swedish only. Swedish Security Service.

[17] See *Systemic Cyber Risk*, February 2020. European Systemic Risk Board.

[18] For the Swedish financial system, this corresponds to the Riksbank's payment system, RIX.

[19] See F. Adelmann, J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz and C. Wilson (2020) Cyber Risk and Financial Stability: It's a Small World After All, *IMF Staff Discussion Note*. International Monetary Fund.

[20] See T. Gustafsson and D. Lindahl (2019), Cyber defence – skill needs practice , *FOI Memo 6867*. Swedish Defence Research Agency.

Here we describe three different channels through which the shock from a cyber attack can be amplified or spread to more agents.[21] The first is the *confidence channel*. Through this, a cyber attack can lead to a lack of confidence both in the agent affected, in other similar agents and in the financial system in general. The magnitude of the confidence effects will in part depend on the basic state of the financial system, the severity of the consequences of the attack, the duration of the impact on the agent or agents, and the number of agents affected by the attack.[22] It is important that financial markets, companies and the general public have confidence in the financial system. If confidence is lost, it could eventually lead to runs on banks or other financial companies and threaten financial stability.

The second is the *operational channel*. The financial system is closely interconnected on both the financial and the technical level. This means that operational problems at one agent can be spread to other agents. On the financial level, various central agents are closely interconnected by, among other things, payments, loans, derivatives contracts and cross-ownership. Even on the technical level, they are linked together, for example, because they use the same hardware and software and hire the same service providers for, for example, IT operations, telecommunications or cloud services. This can increase the risk of cyber attacks spreading in the financial system and thus affect financial stability. Agents in the financial system are also highly dependent on data and the same data sources, which further increases interconnectedness. Moreover, the fact that both financial and technical services are often cross-border increases the risk of the consequences of major cyber attacks spreading between countries.[23]

The third channel is the *financial channel*. Here, the focus is on the fact that the cyber attack leads to financial losses for one or more agents, either directly or indirectly via confidence effects or the operational channel. Financial losses may in turn lead to further financial losses, impaired confidence or both.[24]

4. Indirect impact – contagion effects lead to further consequences

The contagion effects that we have described above may in turn affect the same or other agents even more, see *Indirect impact* in Figure 2. This refers to effects that were not directly due to the initial attack and affect either via the contagion channels described above or confidentiality, integrity and availability just as with direct impact. This can happen to both organisations that have already been directly affected and organisations that have until then been unaffected by the initial attack. Indirect effects can be seen as a result of the contagion effects and can manifest themselves in a loss of confidence, financial losses and the risk of one or more financial organisations falling into a negative spiral of contagion effects and further indirect impact.

[21] See *Systemic Cyber Risk*, February 2020. European Systemic Risk Board.

[22] See *Systemic Cyber Risk*, February 2020. European Systemic Risk Board.

[23] See F. Adelmann, J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz and C. Wilson (2020) Cyber Risk and Financial Stability: It's a Small World After All, *IMF Staff Discussion Note*. International Monetary Fund.

[24] See *Systemic Cyber Risk*, February 2020. European Systemic Risk Board.

5. Impact on financial stability – risk of the cyber attack leading to financial instability

As described above, there are several ways that the financial stability can be affected, and this stage summarises that effect. Our conclusion from this analysis indicates that it is perfectly possible that a cyber attack can lead to a systemic crisis in the financial system. This is also in agreement with previous analyses.[25]

As we have illustrated with the arrows in Figure 2, cyber attacks can affect financial stability either directly or indirectly, or through a combination of both. It is possible that a cyber attack on financial agents or their third-party suppliers will affect critical financial functions to such an extent that the attack will have a direct impact on financial stability. It is also possible that the initial attack will only cause limited damage, but that the knock-on effects will spread and be amplified to such an extent that they will ultimately affect financial stability.

Most successful cyber attacks affect only one financial agent and cause limited damage. There are no known cases of cyber attacks that have led to systemic crises.[26] This does not mean, however, that they would not be able to do so. A successful cyber attack with sufficient resources to disrupt a key agent or spread the effects through the financial system could pose a systemic risk.[27] In this respect, the confidence channel is particularly important so that financial markets, companies and the general public have confidence in the functioning of the financial system.

4 Understanding of the threat landscape is vital for management of cyber risk

In previous sections, we have described how a cyber attack can potentially lead to financial instability. This is because agents in the financial system perform functions that are critical to financial stability, and their operations therefore need to have well-adapted protection to minimize the risk of cyber attacks. In order to achieve this, protection needs to be proportionate to both the assets of the operations[28] and the threat landscape against the organisation. Cyber risk is driven by actors with the intention and ability to affect systems or information in digital environments. An actor who initiates and is behind a cyber threat is called a threat actor and can have different goals, drivers and methods. In other words, assessing the threat landscape is necessary to know what to protect the operations against.

[25] See *Systemic Cyber Risk*, February 2020. European Systemic Risk Board, and F. Adelmann, J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz and C. Wilson (2020) Cyber Risk and Financial Stability: It's a Small World After All, *IMF Staff Discussion Note*. International Monetary Fund.

[26] See *Systemic Cyber Risk*, February 2020. European Systemic Risk Board.

[27] See F. Adelmann, J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz and C. Wilson (2020) Cyber Risk and Financial Stability: It's a Small World After All, *IMF Staff Discussion Note*. International Monetary Fund.

[28] In this context, "assets" means systems or information whose availability, integrity or confidentiality needs to be protected in order to avoid unacceptable consequences.

Assessing the threat landscape is central to being able to protect oneself

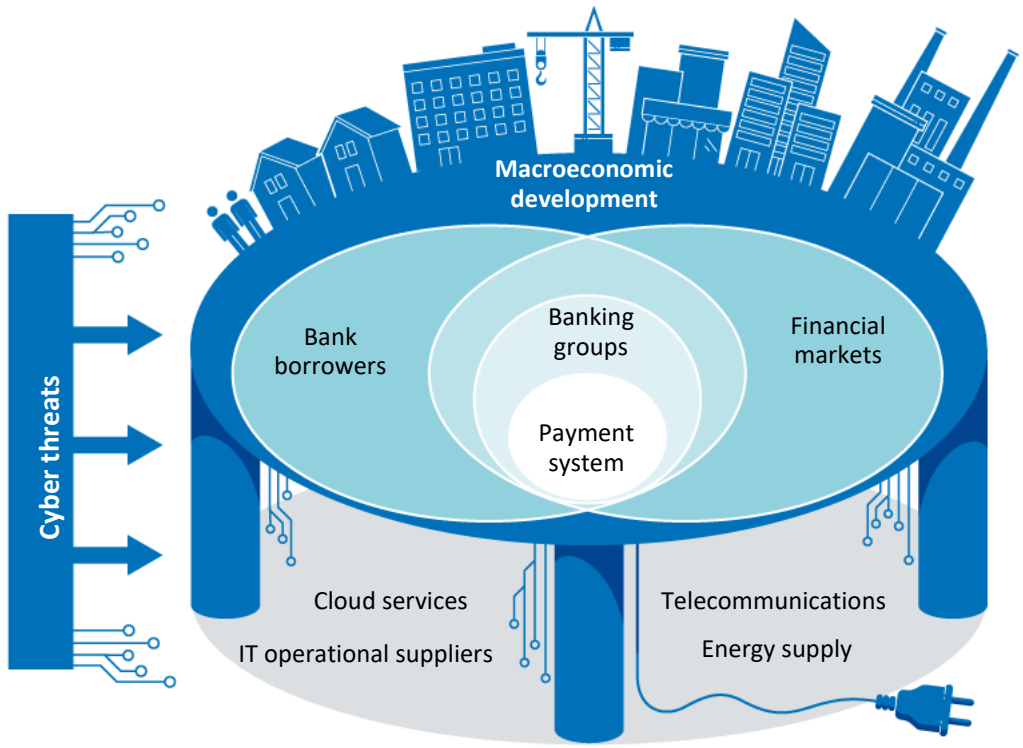
Cyber threats arise in the financial system when a threat operator has both the intention and the ability to conduct malicious actions directed against a financial agent or its third-party suppliers. These actions take place in what is known as the cyber domain or cyberspace, that is, the global information environment, which consists of interconnected IT infrastructures that are interdependent with their associated data and information.[29] However, even if a threat actor has the capability to do damage, it is generally not a threat as long as there is no intent. Similarly, a threat actor with the intent to harm does not constitute a threat, as long as it lacks capability.

Although a threat has relatively easy-to-understand elements, it is difficult to analyse the threat landscape towards a specific activity. A significant explanation for this is that threat landscapes often vary over time and can change quickly. In general, it is difficult to assess who has the necessary capability and this frequently changes within the cyber domain. Methods of manipulating, destroying and stealing information change and safeguards can never be fully relied upon. The digital tools and vulnerabilities used by a threat actor are anything but constant, while the IT environments to be defended are also constantly changing. In addition, threat actors tend to reuse the tools of other threat actors and can also buy certain capabilities.[30] Furthermore, a modern IT environment often depends on many other parties in addition to one's own organization. Moreover, there is a threat landscape towards both the financial system and its critical suppliers, as illustrated in Figure 4 below.

[29] H. Karlzén, H. Granlund and M. Wedlin (2018), Operationer i cyberdomänen - en inventering av svensk forskning [Operations in the cyber domain - an inventory of Swedish research] *FOI-R--4594*. In Swedish with an English summary. Swedish Defence Research Agency.

[30] H. Karlzén (2020), Cyberoperationer – en slutrapport [Cyber Operations – a final report], *FOI-R--5072*. In Swedish with an English summary. Swedish Defence Research Agency.

Figure 4. The cyber threat is aimed at both the financial system and its critical service providers



Source: Sveriges Riksbank.

Just as the methods and capabilities of a threat actor can develop and change over time, a threat actor's intent can also change. Changes in foreign and security policy or media attention are examples of events that may affect the intentions of a threat actors. Therefore, a threat landscape is short-term and needs to be constantly updated.[31]

The complexity of the banking, financial and insurance sectors makes it difficult to assess the threat landscape towards the sector.[32] However, the European Union Agency for Cybersecurity, ENISA, expects that cyber security risks will in general be even more difficult to assess and interpret over the next ten years due to the increasing complexity of the cyber threat and the expanding attack surface, that is, the possible access points for the attacker, resulting from continued rapid digitalisation.[33]

Protection should be adapted to the greatest threat

Threat actors have, as we have described, varied intentions and capabilities. For example, organised crime groups can initiate cyber attacks to achieve financial goals

[31] See *Vägledning i säkerhetsskydd, Säkerhetsskyddsanalys [Guidance in protective security, Protective security analysis]*, June 2020. In Swedish only. Swedish Security Service.

[32] See *ENISA Threat Landscape 2020 - Sectoral/thematic threat analysis*, October 2020. European Union Agency for Cybersecurity.

[33] See *ENISA Threat Landscape 2020 - Sectoral/thematic threat analysis*, October 2020. European Union Agency for Cybersecurity.

where financial gain is the driving force, ideologically motivated actors can initiate cyber attacks to engage in activism, and state or state-supported actors can initiate politically motivated cyber attacks, with espionage, sabotage or influence as the goal. The varied driving forces, goals and capabilities mean that different threat actors can behave very differently when it comes to how long-term, advanced, targeted or opportunistic they are in their work. This means that different threat actors require different kinds of protection to a certain extent.

The main threat to society's critical infrastructure that agents in the financial sector jointly comprise is state and state-sponsored threat actors.[34] Today, state actors try to gain foothold in digital infrastructure that is critical to Swedish society in order to be able to disable it if the intention arises.[35] In this context, the threat landscape facing Sweden has widened, become more complex and is also thought to target political, military and economic assets in parallel.[36] In other words, state or state-sponsored actors have both the intent and the ability to carry out cyber attacks that can damage central societal functions in Sweden.[37]

These are the threats that the Swedish financial system needs to adapt its protective measures to. Due to the fact that threats from state actors are more advanced and, as a rule, require greater protection than threats from other threat actors, this type of threat is what is known as the 'dimensioning threat'. For threat actors with this type of advanced capability, everything connected to the Internet is available and can be accessed. In addition, unlike many other cyber threats, these attacks are often intended not to be detected.[38] It is therefore not enough to try stopping an advanced attacker in the initial phase. Agents in the system should also individually and jointly, and as far as possible make such attacks even more difficult by developing a capacity to detect, respond and recover from them. Developing and maintaining such capacity is relatively difficult and requires time. An important organisational and cultural first step is the establishment of an 'assume breach' mentality in operations, which assumes that intrusion will take place, has already taken place and may even be taking place at the moment. In other words, measures to prevent, manage and recover from advanced cyber attacks need to include a high level of capacity to detect when existing protective measures fail, as well as a capacity to rectify both these flaws themselves and their consequences.[39]

Another important part of the work on improving resilience is good coordination regarding cyber risk and long-term planning to reduce the vulnerability of the financial system. This coordination should involve both private and public agents in the finan-

[34] It should be remembered that even attacks that are not necessarily particularly sophisticated can do considerable harm, see for example *Internet Organised Crime Threat Assessment (IOCTA)*, October 2020. Europol.

[35] See *Swedish Military Intelligence and Security Service (MUST) Annual Review 2020 [Annual Review 2020]*, March 2021. In Swedish with an English summary. Swedish Armed Forces

[36] See *MUST Annual Review 2020*, March 2021. Swedish Armed Forces

[37] See *Security Service Yearbook 2019*, March 2020. Swedish Security Service.

[38] See *National Defence Radio Establishment Annual Report 2019*, March 2020. National Defence Radio Establishment.

[39] See *Financial Stability Report*, June 2016. Sveriges Riksbank.

cial sector. In addition, both authorities with financial stability responsibilities and authorities responsible for cyber security should be involved so that the coordination leads to greater resilience.

5 Concluding comments

The conclusion of this analysis is that a cyber attack can affect financial stability, and that cyber risk thus constitutes a systemic risk.

Cyber risk differs from other operational risks, partly because cyber attacks can come from malicious threat actors. Cyber risk is also characterized by speed and scalability.

Agents in the financial system have clear incentives to deal with the cyber risk they are exposed to themselves. However, they do not take an overarching system perspective in their work, which means that there is a risk of negative external effects.[40] This entails a risk of market failure and there is therefore a natural role for the state to play.

In order for an organisation to be able to protect itself, it is essential to understand both what is to be protected and against whom protection is needed. Measures aimed at preventing and stopping cyber attacks need to be complemented by a capacity to detect when protective measures fail and a capacity to rectify such flaws and their consequences. There are several ways to improve the management of cyber risk in the financial system. Since December 2019, the Riksbank has coordinated cyber security tests according to TIBER-SE, with the aim of strengthening resilience to cyber attacks in the Swedish financial system.[41] Further, adequate and effective coordination is crucial for successfully managing cyber risk in the financial system.

[40] This assessment is shared by Finansinspektionen (FI - Swedish financial supervisory authority, see *Cyber threats and financial stability – FI's role and assignments*, March 2021. Finansinspektionen.

[41] Sveriges Riksbank, *The Riksbank coordinates cyber security tests*. News item, last updated 13 December 2019. Retrieved 9 May 2021
https://www.riksbank.se/en-gb/press-and-published/notices-and-press-releases/notices/2019/the-riksbank-coordinates-cybersecurity-tests/

References

See F. Adelmann, J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz and C. Wilson (2020). “Cyber Risk and Financial Stability: It’s a Small World After All”, *IMF Staff Discussion Note*. International Monetary Fund.

Aldasoro, I., L. Gambacorta, P. Giudici and T. Leach (2020). “The drivers of cyber risk”, *BIS Working Papers No 865*. Bank for International Settlements.

Bank for International Settlements (2,011). “Principles for the Sound Management of Operational Risk”, June.

Bank for International Settlements and the International Organization of Securities Commissions (2012). “Principles for Financial Market Infrastructures”, April.

European Union Agency for Cybersecurity (2020). “ENISA Threat Landscape 2020 - Sectoral/thematic threat analysis”, October.

European Systemic Risk Board (2020). Systemic Cyber Risk, February.

Europol (2020). “Internet Organised Crime Threat Assessment (IOCTA)”, October.

See Financial Stability Board (2018). “FSB Cyber Lexicon”, November.

Finansinspektionen (2021). “Cyber threats and financial stability – FI’s role and assignments”, March.

Swedish Defence Radio Institute (2019). “FRA Annual Report 2018”, January.

Swedish Defence Radio Institute (2020). “FRA Annual Report 2019”, February.

Swedish Defence Radio Institute (2021). “FRA Annual Report 2020”, March.

Swedish Armed Forces (2021). Swedish Military Intelligence and Security Service (MUST) Annual Review 2020 [Annual Review 2020], March. In Swedish with an English summary.

Gustafsson, T. and D. Lindahl (2019). “Cyber Defence – Skill requires Practice” *FOI Memo 6747*. Swedish Defence Research Agency.

Karlzén, H. (2020). “Cyber Operations – a final report”*, FOI-R--5072*. Swedish Defence Research Agency.

Karlzén, H., H. Granlund and M. Wedlin (2018). “Operations in the cyber domain - an inventory of Swedish research”*, FOI-R-4594*. Swedish Defence Research Agency.

Sveriges Riksbank (2013). “The Riksbank and financial stability”, February.

Sveriges Riksbank (2016 a). “The Swedish Financial Market”, August.

Sveriges Riksbank (2016b). “Article: "Cyber threats in the financial system” *Financial Stability Report*, June.

Sveriges Riksbank (2019). “The Riksbank coordinates cybersecurity tests”. News item, last updated 13 December 2019. Retrieved 9 May 2021 https://www.riksbank.se/en-gb/press-and-published/notices-and-press-releases/notices/2019/the-riksbank-coordinates-cybersecurity-tests/

Sveriges Riksbank (2021). “The Payment System - RIX”, last updated 5 March 2021. Retrieved 8 May 2021 https://www.riksbank.se/en-gb/payments--cash/the-payment-system---rix/

Swedish Security Service (2020a). “Security Service Yearbook 2019”, March.

Swedish Security Service (2020b). “Vägledning i säkerhetsskydd, Säkerhetsskyddsanalys [Guidance in protective security, Protective security analysis]”, June. In Swedish only.

Swedish Security Service (2020c). “Vägledning i säkerhetsskydd, Informationssäkerhet [Guidance in protective security, Information security]”, September.

Zouave, E. and M. Jaitner (2019). ”Secure Supply Chains for Control Systems”*, FOI-R—4759*. Swedish Defence Research Agency.

SVERIGES RIKSBANK
Tel +46 8 - 787 00 00
registratorn@riksbank.se
www.riksbank.se

PRODUCTION SVERIGES RIKSBANK