ECONOMY AND FINANCE • VOL. 12. ISS. 3 • SEPT 2025 • DOI: 10.33908/EF.2025.3.1

CYBER SECURITY AND FINANCIAL STABILITY: RELATIONSHIPS, RISKS AND REGULATORY APPROACH

Gabriella Biró[1]

ABSTRACT

As digital technologies press ahead, the operation of financial systems increasingly relies on ICT systems and networks, so managing cyber security issues to maintain financial stability has become key not only for individual institutions but also at systemic level. The objective of this paper is to identify the relevant concepts, to describe the processes how systemic cyber security risks escalate and to assess international and local regulatory and institutional efforts targeting risk reduction. In the first part, the concepts of cybersecurity, cyber resilience and cyber risks are clarified with particular attention to the definitions used in the financial sector. The study focuses on the analysis of three models (framework systems offered by the IMF, the ESRB and the National Bank of Hungary (MNB) describing the escalation of how cyber security incidents affect the financial system as well as the nature of transmission channels. The author compares the logical structures, differences and applicability of the models, and makes an assessment of how the individual models can help identify and reduce systemic risks. The issues of financial stability relevant to Hungary are also presented. In the last part of the paper, the risk reduction measures to be applied in the course of managing systemic cyber risks are reviewed. Applying a three-tier approach of preventive, detective and corrective control measures, the risk reduction options available for regulators, information sharing and testing are analysed. To sum up, we emphasise the cyber resilience of the financial system can only be achieved by a multi-disciplinary approach assuming the coordinated efforts of cybersecurity and financial stability experts.

Jel codes: G18, G28, O33

Key words: financial stability, cybersecurity, cyber resilience, systemic risk, risk management

1 *Gabriella Biró* cybersecurity expert, PhD student, National University of Public Service. E-mail: biro.gabriella@uni-nke.hu.

1 INTRODUCTION

As regards cyber security incidents threatening financial stability, experts often say the question is not if but when they are likely to happen. As a major part of our everyday life including finances or business activities take place on digital platforms, the need is growing to understand and professionally manage cyber risks potentially threatening financial stability. Key players of the financial world have recognised the tendency of risk increase. Christine Lagarde, President of the European Central Bank (ECB) said in a statement in 2020 that the next financial crisis might be triggered by a cyber-attack, so preparations must be made to manage such risks (Thornton, 2020). Cybersecurity has become a returning factor in the annual global risk reports issued by the World Economic Forum (WEF) while the risk of „cyber espionage and warfare"[2] has been classified among the five most serious short term risks (two years) and among the first ten for mid-term (ten years) (WEF 2025). The International Monetary Fund (IMF) also pays particular attention to the risks presented by cybersecurity; it devoted a separate chapter in its 2024 report on global financial stability to reiterate that cyber risks give rise to increasing worry in terms of macro-financial stability (IMF, 2024).

Significant cybersecurity incidents have already arisen in the finance sector. ENISA, the cybersecurity agency of the European Union has been publishing their map of cyber threats in the EU every year. Further, they published an analysis specifically devoted to the financial sector in 2025 which has proven the number of incidents is growing from one year to the next (ENISA, 2024b). According to the report by ENISA, the financial sector is third in the line of most frequently attacked industries following the public sector and transport. Approximately 9% of cyber-attacks are directed at financial organisations (ENISA, 2024a). One of the most famous incidents affecting banks was an attack on the national bank of Bangladesh (Bangladesh Bank) in February 2016 when hackers compromised the bank network and tried to steal almost one billion US dollars via the Bank's SWIFT system. The actual material damage came to almost 81 million US dollars in the end. The incident made the owners of SWIFT reassess the security requirements of the system and set up a mandatory security programme (Customer Security Programme) for SWIFT customers (Bangladesh Bank robbery 2025). In another example, the close-down of Russian owned Amsterdam Trade Bank registered in Amsterdam in 2022 was partially the consequence of Microsoft having enforced sanctions against it by stopping its access to banking data stored in cloud services, although the bank was still solvent in financial terms (Chamber

2 In a change of methodology, cybercrime and weaknesses of cyber security were transferred to the category of "cyber espionage and warfare" in the 2025 report.

International, 2022). So, there was a precedent of how a technology service provider can render the operation of a bank impossible from one day to the next.

In this paper our goal is to find an answer to the question of how to interpret cybersecurity risks with respect to financial stability. In other words, what cyber risk actually is, and when and how it can reach a level where it can pose a threat to financial stability, and what means are available to us to manage those risks. The question is fairly complex since cybersecurity and financial stability are rather distant areas with relatively few thoroughfares and connections found so far. In general, experts and researchers of cybersecurity are not really at home in the world of macro-prudential policies[3] while experts dealing with financial stability find the world of high-tech cyber- and information security alien. However, general definitions and models have been developed on both sides as well as in the cross-border areas which allow a substantive analysis of the impact of cyber risks on financial stability.

2 CYBER SECURITY – BASIC CONCEPTS

In order to understand cyber risks, you must first identify the baseline you want to achieve, i.e., the point where you are under threat by risk. There are several definitions of cybersecurity and cyber resilience accepted in the financial sector and beyond. They share a component, i.e., all of them require the presence of three conditions, namely, *confidentiality, integrity and availability.* The Financial Stability Board (FSB) developed in 2017 and updated in 2023 a Cyber Lexicon with the aim of providing uniform definitions used in the financial sector (FSB 2023). The FSB Cyber Lexicon provides the following definitions that are important for this study:

*"**Cyber Security**: Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved"*[4]

*„**Cyber Resilience:** The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the*

3 Macro-prudential policies cover regulations and supervision of the whole financial system or its significant parts; the objective is to recognise and manage systemic risks. Micro-prudential supervision, on the other hand, focuses on the safe operation of individual financial institutions.

4 Cybersecurity: Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. (FSB 2023).

environment and by withstanding, containing and rapidly recovering from cyber incidents."[5]

„***Cyber Risk:*** *The combination of the probability of cyber incidents occurring and their impact."*[6]

In the European Union DORA (Digital Operational Resilience Act, 2022) is the number one regulation on cybersecurity in the financial sector. Although it mentions digital operational resilience in its title, one of its main objectives is the management of cybersecurity risks. The Act does not identify the concept of cybersecurity or cyber risk; however, the definition of *digital operational resilience* is quite similar to the above, more pragmatic definition of *cyber resilience* by FSB:

„***Digital operational resilience:*** *means the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions."*(DORA, 2022).

The set of concepts in DORA is adjusted to a more general EU Directive, Directive NIS 2 (NIS 2 2022), since it is NIS 2 that identifies high-level cyber security requirements for the sectors in its scope, namely "banking services" and "financial market infrastructures" by the terminology of NIS 2. NIS 2 itself, similar to DORA, fails to identify the concept of cybersecurity but refers back to the EU Cyber Security Regulation (Cyber Security Regulation, 2019), which includes a more general definition of *cybersecurity:*

„Cybersecurity*: means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats."* (Cyber Security Regulation, 2019).

The above may indicate why the Financial Stability Council found it necessary to clarify the definitions applied and recommended for other financial regulators when dealing with the financial stability aspects of cybersecurity.

Contrary to that, the definition of risk is definitely more uniform partly because regulators often do not feel it necessary to re-interpret it and partly because all (cyber and non-cyber) definitions describe the measure of risk as a function of

5 Cyber Resilience: The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents. (FSB 2023).

6 Cyber Risk: The combination of the probability of cyber incidents occurring and their impact. (FSB 2023).)

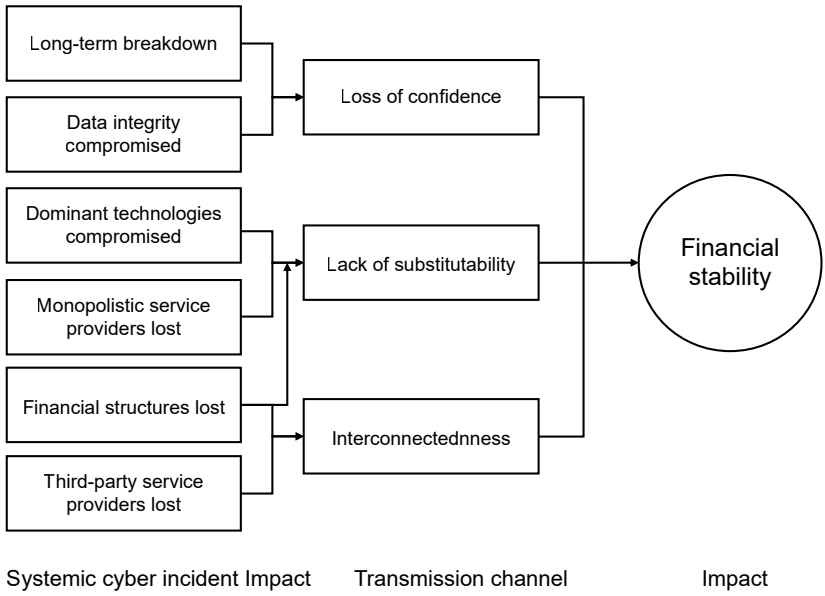
the probability of occurrence and potential impact of risk in some form. Different methodologies also seem to agree that risk management means the elimination, passing on, reduction or acceptance of risk. If cybersecurity risk is of a size that can threaten financial stability, risk reduction can be the only answer. If a financial system is resilient, it can perform its duties uninterrupted as it possesses the abilities identified in the FSB definition, i.e., it prepares, adjusts, resists, restrains, or recovers if needed.

3 IMPACT OF CYBERSECURITY ON FINANCIAL STABILITY

There is a wide range of cybersecurity risks beginning from operational incidents affecting ICT systems (e.g., a power outage caused by a high-voltage pylon downed by a storm) through deliberate hacker attacks to instances of cybercrime targeting customers. As there are innumerable different scenarios, rather than analysing single threats, you need some general methodology to analyse how a cybersecurity incident can pose a threat to financial stability. Several theoretical models have been described over the past few years, and two major ones stand out as a result of the efforts made by professional expert teams.

The European Systemic Risk Board (ESRB) set up a team, the European Systemic Cyber Group (ESCG) in 2017. The Group had developed and published a model by 2020 to describe the general process of how cybersecurity incidents can escalate into incidents affecting financial stability (ESRB 2020; Ros 2020). Shortly afterwards, the IMF published its model also in 2020 (Adelmann et al., 2020). Both models started out of a single incident that can escalate into a systemic problem affecting financial stability provided certain conditions are fulfilled. The IMF model is less complex, so it is presented first.

Figure 1
Relationship between cybersecurity and financial stability as per the IMF model



Source: own design (based on Adelmann et al., 2020)

In the original IMF model (*Figure 1*) a cybersecurity incident is *a priori* a systemic event. It has reached that level because it affects an institution (financial infrastructure[7], or systemically significant bank) exercising impact on financial stability[8]. According to the IMF assessment, the transmission channels of the impact can be divided into three categories: erosion of confidence, indispensability or interconnectedness. Erosion of confidence is a well-known factor in terms of financial stability, it cannot only be triggered by a cybersecurity incident but other traditional scenarios – well known for analysts of financial stability – can also play a part, such as a stock exchange panic or bank run. On the other hand, the model neglects potential input events such as a sudden large-scale increase of

7 For instance, an institution operating a central securities depository, an important contracting party or payment system.

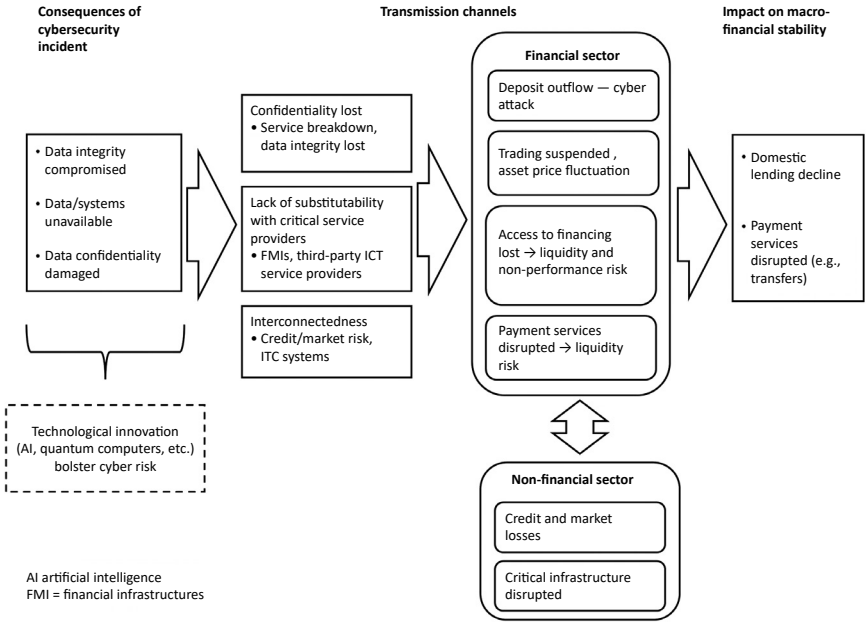
8 The methodology to identify systemically significant institutions and services has already been developed (FSB 2013).

cybercrime events affecting customers, or fake news spreading on social media that may result in the major erosion of customer confidence. It is, naturally, a question, how quickly such erosion of confidence can happen, i.e., if there is time and opportunity to intervene and reduce the risk.

The second channel affects operations, that is, it means the loss of an indispensable technological component or of a service provider in a monopolistic position (for instance, a financial infrastructure).

The third channel is similar. It can cause a systemic problem due to the interconnectedness of the systems if the problem affects a financial infrastructure or an element of the supply chain. In the IMF model, the triggering event affects the confidentiality, integrity, or availability of data or of the ITC system. In other words, the model is built upon the traditional definition of cybersecurity as recommended in FSB Cyber Lexicon. The advantage of the model is that it is visual and easy to grasp; the triggering events are easy to interpret. The IMF upgraded the original model later on (*Figure 2*) in its Global Financial Stability Report in 2024 (IMF 2024). However, even the upgraded model is unable to cover all potential scenarios that can be managed by the ESRB model, which has been developed at a higher level of abstraction.

Figure 2
Relationship of cybersecurity and macro-financial stability as per the more detailed IMF model



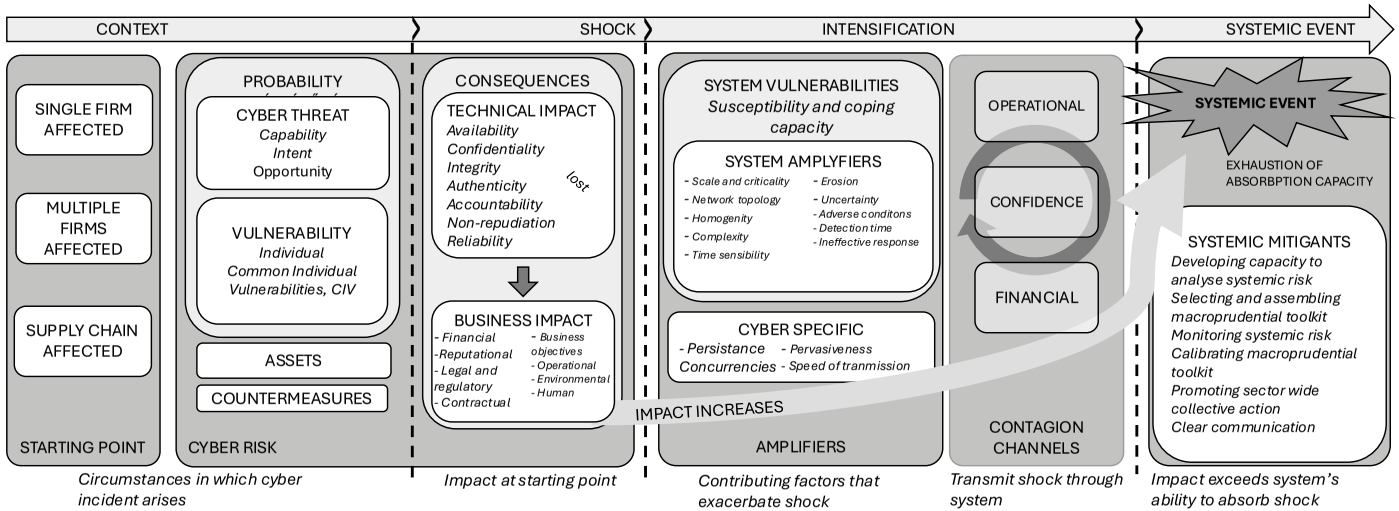
Source: own design (based on IMF 2024)

The approach by ESRB (*Figure 3)*, in fact, ends at the point where IMF starts, i.e., when a systemic cybersecurity incident arises. The starting point of the ESRB model is then a less significant (not necessarily systemic) cybersecurity incident affecting one or several companies or the supply chain. It is the first step in an escalation process. Examining the possible context, analysts have found you need not have a single event affecting a systemically important institution to reach a level of risk threatening financial stability, but events affecting several institutions and/or supply chains at the same time may reach a critical level that triggers a shock, which can multiply leading to a systemic incident.

The second step of the process is the actual occurrence of the incident, i.e., the shock with its technological impact including other effects such as the loss of authenticity, accountability, undeniability and reliability – in addition to the damage caused to ICT systems, the confidentiality, integrity or availability of data. Those features originate from the definition of cybersecurity in the FSB

Cyber Lexicon, which is not surprising if you assume that the first edition of the FDB Cyber Lexicon had already been available when the model was prepared (and some participants in the ESRB team had been working on it). It should be noted that in its preamble DORA makes a reference to the work on systemic cyber risks done by ESRB, i.e., the definitions used there are implicitly accepted (DORA, 2022).

Figure 3
Escalation of a cybersecurity incident threatening systemic financial stability as per the ESRB model



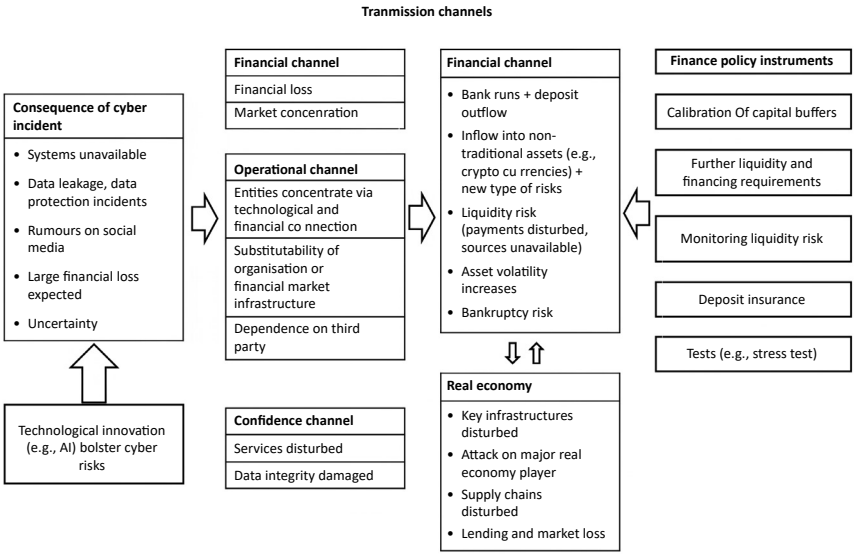
Source: own design (based on Ros 2020)

The classical definition of risk is reflected on the borderline of the first and second phases of the ESRB model, i.e., the probability of the occurrence of a risk event and its potential impact defines the measure of cyber risk. The potential impact is amplified in the third phase. Like the IMF model, the ESRB model also identifies three channels. One of them is the erosion of confidence, while the other two channels identified by IMF (substitutability and interconnectedness) can be included in the ESRB channel relating to operations. ESRB experts have concluded that financial impact might be a third channel playing a part in the spread of the shock, further, the three transmission channels can interact multiplying the impact.

The final stage of the ESRB model is the point where the escalation of a systemic incident reaches a level where the financial system is unable to absorb the shock. The model also considers factors reducing systemic risk that can slow down or curb the transmission of the shock. In total, the ESRB model is more detailed and tries to consider all possibilities, however, it is definitely more complex and difficult to grasp than the IMF model.

In its 2024 macro-prudential analysis, the National Bank of Hungary (MNB) published their interpretation of the transmission channels between cyber risk and financial stability (*Figure 4).* It is a hybrid approach using both the IMF and the ESRB models. It focuses on the transmission channels and makes its starting point at actual potential events, like the IMF model, but it follows the breakdown as per the ESRB channels. Viewing it from the aspect of a cybersecurity expert, the MNB model lacks a theoretical approach built on the trinity of confidentiality, integrity and availability that can be found in both the IMF and the ESRB models. One could say that – in the interpretation of MNB – cyber risk has lost its cyber nature and has become one among macro-prudential tasks in the management of which technology experts have no part. The MNB model is quite similar to the models applied for the transmission mechanism of monetary policy.

Figure 4
Transmission channels between cyber risk and financial stability as per the MNB model



Source: own design (based on MNB 2024)

The MNB model also differs from those by IMF and ESRB since it fails to mention systemic incidents or systemically important institutions. This may be because if you take a look at the Hungarian relevance of the models, you will not find any institutions exerting a major impact on financial stability globally, i.e., that could be termed G-SII (Global Systemically Important Institution).

In terms of the MNB as well as the other two models, the question may arise what kind of institutions the models in question should be applied to, or in other words, what the criteria of a systemically important institution are. The ESRB model's answer is, an institution affected by an incident need not be systemically significant or important, however, an incident affecting any kind of institution might escalate into becoming systemic if suitably unfortunate circumstances prevail. In its description of the model, IMF considers financial markets infrastructure (FMI), particularly payment systems, to be systemically important, which is probably due to the focus of IMF activities.

MNB discusses incidents affecting key infrastructures in the description of its model.

In addition, several so termed other systemically important institutions (O-SII) can be identified in the Hungarian financial sector according to the regulatory terminology of the European Union. They are all credit institutions, mainly large banks. There are seven O-SIIs in Hungary when this paper is published.

There exists another approach to decide which institutions of the Hungarian financial sector might reach a critical level considered to be significant from the aspect of financial stability if they are hit by cybersecurity incidents under certain conditions. Identifying and marking the critical infrastructure components of the financial sector including critical ICT infrastructures that are relevant in terms of cybersecurity is within the scope of the protection of critical infrastructures. Such identification was completed in Hungary in 2016 with collaboration by the MNB as the relevant authority. However, a new CER Directive (CER 2022) on the protection of critical infrastructures was published at the same time as DORA and NIS-2, and as a result, the legislative environment in Hungary has also been updated. There have been little changes in the requirements of identification regarding the financial sector, although the number of institutions involved has become lower. Although the list of institutions identified as critical financial infrastructures is not public, Act No LXXXIV of 2024 on the resilience of critical entities includes the following list:

1. Banking services: credit institutions financial services
2. Financial markets infrastructure: operation of trading sites; operation of payments and clearing and settlement systems; operation of central contracting party; operation of central securities deposit; cash supply; core tasks of the National Bank of Hungary excluding monetary policy, macro-prudential policy and the operation of the ICT system of the central bank.

In view of the Act and the related requirements relating to the financial sector included in the relevant implementing regulation, and knowing the Hungarian financial sector, it is easy to compile a list of entities that can be regarded as potential starting points of a cybersecurity incident potentially threatening financial stability. *(Government Decree 474/2024. (XII. 31.); Act LXXXIV of 2024).*

European legislators have also recognised the interrelations of the protection of critical infrastructure and cybersecurity, and as a result the contents of NIS-2, CER and DORA have been harmonised. Each European legislative action requires the collaboration of the national authorities involved to ensure the management of the relevant risks as effectively as possible.

4 REDUCTION OF SYSTEMIC CYBER RISKS

Following the description of the escalation of cybersecurity incidents threatening financial stability in models, the IMF, the ESRB, and the MNB have all proposed measures to be taken to ensure risks mitigation. The ESCG team of ESRB continued working after their model had been evolved and published in 2020 trying to approach the issues from several directions. Formulating DORA also started at the same time. It also included requirements aimed at reducing systemic cyber risks. The measures proposed and mandatorily required by the different professional bodies and authorities can be categorised by different aspects, therefore in this study a division into three categories is applied, which can be regarded as traditional in terms of ICT security: preventive, detective and corrective control measures. The list is far from complete, however, it includes the major groups of measures and provides insight into their interrelations.

Preventive measures include a list of measures specified in law and regulatory publications by the Supervision (recommendations, circulars) financial institutions must implement to reduce the probability of the occurrence of cyber risks and/or to mitigate their potential impact. Different authorities and agencies have been publishing recommendations since the 1990s with reference to ICT security, cybersecurity and cyber resilience as well as part of regulatory expectations related to the reduction of operational risk. Global preparations for Y2K[9] boosted ICT regulatory activities, i.e., supervision, control and directory measures by designated supervisors of financial authorities having expertise in ICT control. It may have been the only ICT risk not only discussed by ICT experts but also reaching the level of top corporate management to appear on the agenda of corporate BoD meetings.

You can find a detailed review of the establishment of ICT supervision in Hungary and the development of its international regulations in (Kandrács, 2023.7.1.). With regard to regulations, year 2016 was the turning point: it was the year when the EU published the NIS Directive – a predecessor of NIS-2 (NIS, 2016). The G7[10] collaboration also expressed high-level cybersecurity expectations for the financial sector (G7, 2016), CPMI (Committee on Payments and Market Infrastructures), while IOSCO (International Organization of Securities Commissions) published a joint Directive relating to the cybersecurity resilience of financial infrastructures (CPMI-IOSCO, 2016) which has been in use to this day. Several sets

9 Prior to 2000 many ICT systems were coded to store years with only 2 digits, so there were fears that systems would misinterpret "00" as 1900 instead of 2000 causing malfunction in various systems.

10 France, Germany, Italy, Japan, the United Kingdom, the United States, Canada.

of requirements, recommendations and methodologies were published in the following years, since all players found it important to contribute to the mitigation of cybersecurity risks. That multi-coloured regulatory palette had led European legislators to standardise fragmented requirements in DORA in 2022.

DORA and other regulations based on associated authorization include several other expectations on prevention of cyber risks side by side with the establishment of a risk management framework connected to ICT technologies. A novelty among them is the emphasis placed on the management of risks originating from third-party ICT service providers. Major incidents over the past years have directed attention to ICT risks associated with supply chains, which also appear in the IMF and ESCG models. A new feature of DORA is – in addition to providing requirements for financial entities – that it empowers financial supervisors with a kind of guardian role[11].

The financial sector is one of the most regulated ones. Regulations on cybersecurity have probably reached a level by now where a higher number of more details cannot further improve the cybersecurity resilience of its entities. In terms of implementation, it may mean that entities with limited resources must decide whether to spend on legislative compliance or invest into the practical aspects of cybersecurity such as technologies, processes and professionals. In an ideal scenario, naturally, the regulatory and practical aspects of cybersecurity would meet; improved technological protection would also imply legislative compliance. However, such a favourable constellation is fairly unusual in everyday situations.

There are opinions to the effect that the issues of cybersecurity have already been overregulated, and the existing uniform European regulations should rather be simplified. The European Banking Federation (EBF) published a more general analysis (not only focusing on cybersecurity regulations) in which simplifications of the regulations are proposed (EBF 2025). At the same time, opinions have appeared from outside the financial sector, which believe overregulating cybersecurity will cause a competitive disadvantage for businesses operating in the EU. Legislators have not yet made steps in the direction of simplification, but the emphasis is expected to shift to the implementation and enforcement of the rules already in place. To achieve that, a uniform European regulatory practice must be established across sectors and organisations. A review of DORA is expected in January 2028 according to Article 58 (1) of the Regulation.

Proposals by the IMF also include the need to develop the methodology of cybersecurity risk analysis and to integrate it into analyses related to financial sta-

11 The set of means available to a supervision and a guardian is different; a guardian usually operates using more sophisticated indirect means.

bility (Adelmann et al., 2020). The statement seems to be relevant even today in 2025. Although a high number of well-established methodologies are available for analysing cybersecurity risks, technological development is fast bringing with it new risks you did not have to consider earlier. An example might be the fast progress of artificial intelligence, or quantum computing that represent a real threat to currently used cryptography algorithms. Another open question is how the professionals of cybersecurity and financial stability can collaborate so that the analyses by the two areas could become homogeneous and offer a real picture about cyber risks actually threatening financial stability. Identifying and accurately assessing such risks is unavoidable to achieve effective risk management.

The second major group of risk management measures include detective control measures that contribute to the timely detection of risks. Sharing information is emphatic in DORA: both mandatory reports of the incidents that have actually occurred to regulatory bodies and voluntary reports of the threats perceived (typically patterns and methods of attacks). Such knowledge share may help institutions perceive patterns of attacks already described more easily so they can protect themselves particularly if they are provided with information on the nature of protection techniques that are effective in the case of a given attack. The IMF also emphasizes the importance of sharing information, for instance, there are several relevant actual recommendations in its cybersecurity assessment of the Euro zone from the aspect of financial stability (IMF, 2025). Although there are European platforms for sharing information related to cybersecurity incidents, they fail to cover the whole financial sector. For instance, the Euro Cyber Resilience Board (ECRB) set up by the European Central Bank in 2018 deals with the cyber resilience of cross-border financial infrastructures in Europe and operates its own information sharing site (Cyber Information and Intelligence Sharing Initiative, CIISI-EU, IMF 2025).

After presenting its escalation model, the ESRB ESCG team mentioned above concluded that cyber risks do not stop at country borders, as the cyber risks of large technology service providers and systemically significant financial corporate groups require management at European level. According to the team, the next step should be to set up a pan-European cyber risk framework system for risk management. At the end of 2021 and in early 2022 they published, in several forms, their proposal to establish the European Systemic Cyber Incident Coordination Framework (EU-SCICF) 2021 (ESRB 2021, 2022). Setting up the detailed operational rules of EU–SCICF was later integrated into the implementation of the tasks ordered by DORA, as it matches the incident management and cooperation logic of DORA.

A well-practiced response process is a key part of the effective management of cybersecurity incidents when an entity mitigates the adverse consequences of an

incident that has already occurred. It is the third group of control measures, i.e., corrective risk mitigating measures, to mitigate the potential impact of an incident. DORA actually requires major entities to execute threat-led penetration tests (TLPT) regularly. Also in the financial sector, financial institutions have been required to carry out penetration tests on their ICT systems (for instance, on internet bank applications), i.e., they should hire ethical hackers to check if an attacker could penetrate their systems. TLPT operates on the basis of more complex scenarios by imitating real attacks: as the first step, scenarios are made based on real information of threat (real attack patterns), while the "attackers" try to penetrate the target systems. Compared to simple penetration tests, the difference is that during a TLPT the protection team of the entity, i.e., the internal ICT and operating team are unaware that a test is being conducted. They have to respond in the way they would in the event of an actual attack. This approach will greatly enhance the skills of the team, since – after the live test is finished – the lessons will be processed, and the attacking team will also give detailed feedback. The TLPT requirements of DORA follow the pattern of the framework system Threat Intelligence-Based Ethical Red teaming (TIBER-EU, ECB, 2023) set out by the ECB. As in the case of EU–SCICF, in the case of TIBER–EU you can see that work started earlier has been integrated into the framework of requirements of uniform European digital operational resilience.

Cyber stress tests are another form of cybersecurity tests that are relevant in terms of financial stability. Like other stress tests in the financial sector, their objective is to place the system under a "pressure test" to check its bearing strength. In a stress test, certain pre-defined parameters are changed and monitored to find out what their impact on the total system is and where the point is when there is a threat of collapse. In the case of cyber stress tests, the trigger is some kind of cybersecurity incident. However, unlike in TLTP, the impact of the cyber incident on the whole entity or financial system is analysed rather than the entity's ability to respond to the incident. The test process is also different. A cyber stress test is not a real-time simulation.

A major challenge of such tests is that the parameters related to cybersecurity and digital operational resilience are more difficult to quantify, measure or calculate than traditional economic or financial indicators. Current cyber stress test methodologies apply two kinds of approach (or their combination). One is top-down, from the economic impact towards the level of technology, the other is bottom-up from the scenario of a cyber incident towards possible impacts (Vermeulen et al. 2025) (Khiaonarong–Korpinen–Islam 2025). At present, there is relatively little experience related to cyber stress tests, but some lessons have already been drawn (ECB 2024). The authorities are quite tight-lipped regarding the shortcomings revealed, which is understandable as they do not wish to provide potential attack-

ers with ideas. On the other hand, cyber stress tests are in a border area where the components of both cybersecurity and financial stability must be clearly understood while experts must also devise the test methodology as they go. Thus, consistent results to be compared and published from one year to the next are difficult to achieve.

Looking at the preventive, detective and corrective protection measures divided into categories according to the logic of cyber risk reduction, you can see that, in most cases, the activities described in the definition of cyber resilience are applied, i.e., *you prepare* for an incident, *you adapt* to the situation and try to maintain operations, *you resist* attacks, you *curb* the spread of the incident with your response and mitigate its consequences, and then you *recover* normal operations. So reviewing risk mitigation measures you are back at the definition applied in the FSB Cyber Lexicon (FSB 2023).

5 SUMMARY

It was already clear at the beginning of this study that the key players of the financial sector believe a systemic cybersecurity incident might occur presenting an actual threat to financial stability. There have already been serious cybersecurity incidents in the financial sector, and the number of instances is increasing. It can only be partly explained with the stricter rules on incident reporting, as a result of which authorities are informed about a growing number of incidents. It may happen, of course, that financial organisations are more and more able to perceive such incidents, their latency is decreasing, so the number of detected and reported incidents is increasing. On the other hand, the number of incidents seems to increase faster than the internal processes and technical capabilities of the entities improve, therefore, it is likely there is a higher number of incidents in absolute terms too. Thus, it is probably just a question of time when a systemically significant cybersecurity incident arises in the financial sector.

To be able to recognise and manage a systemically significant cybersecurity incident posing a threat to financial stability, you must identify its characteristic features. In this paper the author wanted to find an answer to the question of how to interpret cybersecurity risks in terms of financial stability.

The key definitions of cybersecurity and cyber risk were analysed including the trio of confidentiality, integrity and availability as well as their analogues of cyber resilience and digital operational resilience in different relevant framework systems (FSB, DORA). It has been found cyber risk fits well into the methodologies identifying operational risk or other risk types, since risk is considered to be a

function of the probability of its occurrence and its potential impact. So, cybersecurity risk can be inserted into the list of risks that can threaten financial stability.

Several theoretical models exist trying to answer the question of how cyber risk can reach a level where it can threaten financial stability. In the paper, the ESCG, the IMF and the MNB models (the latter being inspired by the former two) have been analysed. The ESCG model has been found to be the most complex and most universal, and it can be applied for almost all scenarios. The ESCG team that developed the model in the first part of its operations from 2017 to 2020, continued to work and has submitted several other valuable proposals including the most significant one: the EU-SCICF pan-European incident response system. At the same time, several different expert teams have been working on the management of systemic cyber risks using different means. In terms of cybersecurity regulations, the most important step for risk prevention was the issue of DORA. The regulation identifies several requirements to be implemented by financial entities to mitigate cybersecurity risks. They include, side by side with setting up the ICT risk management framework system, the so termed TLTP tests imitating real cyber-attacks. They are the most important from the aspect of developing cyber resilience and information sharing.

Cyber stress tests are similar in terms of their objectives, but their development is independent from DORA, and the methodology of their implementation is far from the sophistication of TLTPs. The regulatory and supervisory means available for cyber risk management are expected to converge in the coming years. As EU–SCICF and TLP have been incorporated into the scope of DORA, more and more regulatory initiatives and methodologies are expected to be integrated in a uniform European cybersecurity supervisory framework. This effect can be boosted by EU initiatives coming from outside the financial sector, such as NIS-2 or the implementation of the CER Directive.

To sum up, it is obvious you need a multidisciplinary approach to corroborate the cyber resilience of the financial system. Experts of cybersecurity and financial stability need to work together to identify, measure and effectively manage potential risks. Regulatory frameworks, information sharing and regular testing of cybersecurity and financial stability must all provide contribution so that the financial sector can prepare, adapt to, resist and curb the escalation of cybersecurity incidents and recover operations following a potential cyber incident to ensure financial stability in a continuously changing digital environment.

The challenges of future technological development such as the progress of artificial intelligence and quantum computing carry new risks that call for uninterrupted vigilance on the part of regulators and innovative solutions to maintain cyber resilience. In addition to the risks already mentioned, finding and employ-

ing properly qualified professionals is also a growing challenge both for financial organisations and their supervisory authorities and regulators.

REFERENCES

474/2024. (XII. 31.) Kormányrendelet, [Government Decree 474/2024 (XII. 31.)] https://njt.hu/jogszabaly/2024-474-20-22.

2024. évi LXXXIV. törvény (2025). [Act LXXXIV of 2024], https://njt.hu/jogszabaly/2024-84-00-00.

Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (EGT-vonatkozású szöveg) (2019). [Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)] https://eur-lex.europa.eu/eli/reg/2019/881/oj/hun

Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (EGT-vonatkozású szöveg). [Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU 2016/1011 (Text with EEA relevance)] 333 OJ L (2022). http://data.europa.eu/eli/reg/2022/2554/oj/hun.

Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (EGT-vonatkozású szöveg) (2022). [Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)] https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről (EGT-vonatkozású szöveg) (2022). [Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 Decenmber 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)] https://eur-lex.europa.eu/eli/dir/2022/2557/oj/hun.

Bangladesh Bank robbery (19.05.2025): in: *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Bangladesh_Bank_robbery&oldid=1291091781.

Chamber International (06.07.2022): Solvent but bankrupt: how sanctions felled Amsterdam Trade Bank. *Chamber International*. https://www.chamber-international.com/news/latest-news/solvent-but-bankrupt-how-sanctions-felled-amsterdam-trade-bank/ (Downloaded: 2025.07.29).

CPMI – IOSCO (ed., 2016): Guidance on cyber resilience for financial market infrastructures. June 2016. Basel: *Bank for International Settlements*. https://www.bis.org/cpmi/publ/d146.pdf.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *OJ L* (2016). http://data.europa.eu/eli/dir/2016/1148/oj/eng

EBF (10.02.2025): Less Is More – Proposals To Simplify And Improve European Rule-Making In The Financial Services Sector. EBF. https://v3.globalcube.net/clients/eacb/content/medias/publications/eacb_studies/report_lessismore_fin.pdf.

ECB (23.03.2023): What is TIBER-EU? https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html (Downloaded: 29.07.2025.).

ECB (26.07.2024): ECB concludes cyber resilience stress test. https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240726~06d5776a02.en.html (Downloaded: 29.07.2025).

ENISA (2024a): ENISA threat landscape 2024. *LU: ENISA Publications Office*. https://data.europa.eu/doi/10.2824/0710888.

ENISA (2024b): ENISA threat landscape: finance sector: January 2023 to June 2024. *LU: ENISA*. https://data.europa.eu/doi/10.2824/5410466.

ESRB (2020): Systemic cyber risk. *European Systemic Risk Board*. https://data.europa.eu/doi/10.2849/566567.

ESRB (25.03.2022): Recommendation of the European Systemic Risk Board of 2 December 2021 on a pan-European systemic cyber incident coordination framework for relevant authorities (ESRB/2021/17). *ESRB*. https://www.esrb.europa.eu/pub/pdf/recommendations/esrb.recommendation220127_on_cyber_incident_coordination~0ebcbf5f69.en.pdf?f2ec57c2199306 7e9ac1d73ce93a0772.

ESRB (2022): Mitigating systemic cyber risk: January 2022. *LU: ESRB*. https://data.europa.eu/doi/10.2849/99500.

Adelmann, F. – Elliott, J. – Ergen, I. –Gaidosch, T. – Jenkinson, N. – Khiaonarong, T. – Morozova, A. – Schwarz, N. – Wilson, C. (2020): Cyber Risk and Financial Stability: It's a Small World After All. In: *Staff Discussion Notes*. *International Monetary Fund*,7. https://doi.org/10.5089/9781513512297.006.

FSB (16.07.2013): Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on Identification of Critical Functions and Critical Shared Services. *Financial Stability Board*.: https://www.fsb.org/uploads/r_130716a.pdf.

FSB (04.13.2023): Cyber Lexicon: Updated in 2023. *Financial Stability Board*. https://www.fsb.org/uploads/P130423-3.pdf.

G7 (2016): G7 Fundamental Elements of Cybersecurity for the Financial Sector. *G7*. https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf.

IMF (2024): Global Financial Stability Report, April 2024: The Last Mile: Financial Vulnerabilities and Risks. Washington, D.C.: *International Monetary Fund*. https://doi.org/10.5089/9798400257704.082.

IMF (2025): Euro Area: Publication of Financial Sector Assessment Program Documentation-Technical Note on Cyber Risk and Financial Stability-Selected Issues in Regulation and Supervision. *IMF Staff Country Reports* 2025(213): 1. https://doi.org/10.5089/9798229019873.002.

Kandrács, C. (ed., 2023): Stabilitás és bizalom: A magyar pénzügyi felügyelés története. Budapest: *Magyar Nemzeti Bank*. [stability and confidence: the history of financial supervision in Hungary, Budapest, *National Bank of Hungary*.

Khiaonarong, T. – Korpinen, K. – Islam, E. (2025): Using Simulations for Cyber Stress Testing Exercises. *International Monetary Fund (IMF)*. https://doi.org/10.5089/9798229008952.001.a001.

MNB (2024): Makroprudenciális jelentés 2024. *Magyar Nemzeti Bank*. [macro-prudential report 2024. national bank of Hungary https://www.mnb.hu/letoltes/mnb-makroprudencialis-jelentes-2024.pdf.

Ros, G. (2020): The making of a cyber crash: a conceptual model for systemic risk in the financial sector. *LU: European Systemic Risk Board*. https://data.europa.eu/doi/10.2849/915512.

Thornton, P. (02.06.2020): Cyber-attacks could cause next financial crisis, says ECB boss. *The Independent*. https://www.independent.co.uk/news/business/news/cyber-attack-financial-crisis-christine-lagarde-ecb-a9322556.html (Downloaded: 26.07.2025).

Vermeulen, R. – Sydow, M. – Brousse, C. – Cascão, F. – Fique, J. – Marques, C. – Nyholm, J. – Virel, F. (2025): Cyber resilience stress testing from a macroprudential perspective. *Macroprudential Bulletin* (27): https://www.ecb.europa.eu/press/financial-stability-publications/macroprudential-bulletin/html/ecb.mpbu202502_01~f4914a46c1.en.html (Downloaded: 28.03.2025).

WEF (2025): The Global Risk Report 2025. Vol 20. Cologny/Geneva, Switzerland: *World Economic Forum*..