# Can Cyber Risk Affect Financial Stability?

Claudiu Ioan Negrea
*Romanian Academy,*
*"Costin C. Kirițescu" National Institute of Economic Research, Bucharest, Romania*
claudiu.negrea@bnro.ro

**Abstract**

*This paper addresses cyber risk as a risk that may affect financial stability. Based on the conceptual framework of cyber risk, I've highlighted a number of research papers and reports issued by regulators and supervisors that assess cyber risk in terms of its potential to affect financial stability.*

*In the paper, I described a cyber risk scenario that could, in certain circumstances, become a systemic risk.*

**Key words:** Cyber risk, systemic risk, financial stability, financial market infrastructures, payment systems
**J.E.L. classification:** E50, E58, E59, E71, G28, G41

## 1. Introduction

Digital innovation has significantly reshaped the population's behaviour in its daily life and the way it interacts with financial institutions. It is almost impossible to live in today's world without being connected to the internet, both in our daily office activities and in our private lives, in order to make our lives easier. E-commerce tends to gain more and more value in the life of the modern consumer and, in order to ensure the basis of this way of trade, we must keep in mind the availability of stable, efficient and secure technical infrastructures starting from the merchant's websites, to electronic payment methods, the payment provider's solution, online banking or phone banking applications, payment systems, settlement systems and ending with technical infrastructure within courier companies. Any element in this chain, if vulnerable, would lead to a decline in consumer confidence in e-commerce.

As the use of information technology has become an important part of everyday life, and even more so during the Coronavirus pandemic (COVID-19), the potential disadvantages of a growing dependence on technology have become even more apparent. Thus, it is essential that the technical infrastructure on which critical services are offered to the population, such as the public health system, access to the financial system, utilities are protected from cyber attackers and are available at all times, to ensure the proper functioning of the modern society.

The Covid crisis has forced traditional financial institutions to completely reorganize their operations, having to deal with situations of operational blockages, temporary branch closures, increased demand for online banking services, including the physical unavailability of staff, who have had to work remotely.

Given the current geopolitical context and the recent escalation of cyber attacks, it can be stated that cyber risk is taking on new horizons from the perspective of traders, service providers and regulators, who are stepping up their efforts to ensure consumer safety and maintaining confidence of the population in the financial system.

Recently, national supervisors have considered cyber risk to be particularly important and have consistently assessed it. At EU level, various working groups were set up to assess the potential of cyber risk to affect financial stability.

## 2. Literature review

According to the European Central Bank, the European financial sector did not suffer major disruptions in the provision of banking services during the health crisis, even if there was a considerable increase in cyber attacks. Cyber risk was considered of major importance in the analysis of all the risks for the financial system that were identified and it was included in the category of major risks. The European Central Bank and central banks members of The European System of Central Banks included analyses regarding cyber risks in their financial stability reports.

Healey et al. (2018b) pointed out that so far no incident has affected financial stability, while stressing the difficulty of measuring the impact of the materialization of a cyber incident that would affect several entities which are directly interconnected with the affected entity. The contagion effect of the entire financial system related to the attacked infrastructure cannot be quantified, taking into consideration that the reaction of the market and the consumers of financial services are not similar from one operational event to another. This risk for the banking financial system is insufficiently examined by the academic literature, by the supervisory authorities, and even by the actors providing financial services. The lack of complex analyzes is, in my view, the result of two key issues, namely the lack of clear information on cyber incidents and the lack of information regarding the technical infrastructure used by financial institutions. The dissemination of this information may pose a major risk for the financial institution, as this information could contribute to facilitating access of the attackers who intend to gain access to the institution's technical infrastructure.

The latest analyzes performed by authorities and academia show that cyber risk has the potential to trigger financial instability. This view is also reflected by recent European regulatory initiatives that address the cyber resilience issues in an increasingly complex way, with an emphasis on the importance of this type of risk.

## 3. Research methodology

After analyzing secondary data and the relevant literature, I conducted a qualitative research focused on a scenario in which a cyber incident can generate systemic risk.

## 4. Findings

### 4.1. Systemic cyber risk

Because cyber risks that affect individual entities have the potential to affect other entities that use similar infrastructures, this risk can become a systemic risk and affect financial stability. For this scenario (in which financial stability is affected) to manifest, some type of amplifier would need to be present, so that the shocks produced at the level of the financial system can no longer be absorbed, causing blockages in accessing liquidity, which would result in diminishing public confidence in the financial system. Such a crisis, generated by an operational incident of a cyber nature, can generate effects similar to those observed in times of a financial crisis, with the potential to generate major negative consequences in the real economy and may even create situations of economic recession.

Taking potential financial losses into account, the uncertainty created by the materialization of a major cyber attack, combined with the loss of public confidence in the financial system, are in my opinion the critical catalysts (amplifiers) in triggering a crisis that would affect financial stability.

Historical data on financial crises has shown that the insolvency of a systemic financial institution or a serious incident at the level of such an institution leading to its total unavailability and the loss of financial data of customers generate a major crisis in the financial system. In these situations, the reaction of other market participants is particularly important in mitigating the effects of temporary economic downturns and in maintaining public confidence in the financial system.

Given the interdependencies in the financial system, in the process of analyzing a major cyber incident that may have an effect on financial stability, all direct and indirect channels through which the shock will have a direct or indirect effect on other institutions from the financial sector must be assessed.

Effective communication and transparency about the real situation have been shown to lead to more effective crisis management.

Lack of transparency or incorrect information's can create panic among other financial market participants, which results in a loss of confidence in other financial market participants, which affects liquidity, especially for smaller market participants.

Thus, for a better management of cyber risk with systemic effects, it is important to understand the nature of the initial incident, the potential areas affected and to estimate the potential financial losses.

A definition of systemic cyber risk is found in a paper published by the World Economic Forum in 2016, which referred to cyber attacks or events that can affect a critical component of an infrastructure and can lead to the unavailability of services, causing losses, which would also affect other entities in the ecosystem where the affected entity operates, having an impact on the safety and health of the population, on financial stability or affecting national security.

In a paper published by Kopp et al. (2017), cyber risk is presented as a potential risk that can generate systemic risk due to the common technical infrastructures operated by the financial sector entities, the interdependencies between them and the contagion effect at the level of the financial sector.

The potential of a cyber risk to have systemic implications is also highlighted by the Office of Financial Research (2017), which highlights the existence of three channels through which a cyber incident can affect financial stability: the lack of substitutability of financial market actors, especially of financial market infrastructures, the loss of confidence of both partner entities and consumers of financial services and the loss of data integrity or unavailability for a longer period of time.

Healey et al. (2018a) argue that at least one channel should be added to the three channels identified by the Financial Research Bureau, namely the lack of substitutability of technical infrastructure. The authors point out that a large (and increasing) share of computing and storage power is provided by a limited number of vendors and given that technical infrastructures in the financial field tend to be extremely similar and use the same security protocols, this makes these infrastructures vulnerable to cyber attackers.

Thus, the risk of a major incident at local level can lead to disruption or destruction at the regional level or even at the level of the entire industry. Also Healey et al. (2018a) identify three main amplifiers for an incident of a cyber nature to generate systemic risk: the moment of occurrence of the incidents, the complexity of the degree of security of the technical infrastructure and the intention of the attacker.

A number of papers address scenarios of unavailability or compromise of data integrity in the financial system, and the scenario of unavailability of a financial market infrastructure as a result of a cyber incident. These scenarios are a real concern for regulators and supervisors and also for the financial sector participants, because all these scenarios can lead to a loss of public confidence in the financial system.

Danielsson et al. (2016) consider that a cyber risk has a low potential to become a systemic risk, but highlight that the situation of simultaneous materialization of a cyber incident with a financial crisis situation can act as a trigger of a systemic crisis.

A particularity of this risk is the possibility of hackers to attack a target over a long period of time, often penetrating systems and gaining access to information managed by these systems, giving attackers the opportunity to assess and identify all features and mechanisms, existing system-level defense before completing the attack and extracting data and information or blocking these systems to subsequently demand money from infrastructure owners.

In many cases, attackers may have financial resources to help them use highly advanced methods of attack, and they may often be motivated to destroy rather than make a profit.

Thus, cyber attacks can be considered a matter of national defense in certain circumstances, involving the financial supervisors together with the national security authorities in carrying out activities that the financial supervisors normally do not consider in their regular activities related to providing the current financial market monitoring.

As a distinct feature of cyber risk, three elements differentiate it from an operational risk, namely the speed of spreading, the extent of the risk and the intention or motivation of the cyber attackers. The interconnection of different information systems facilitates the rapid and widespread reach of cyber incidents, affecting a large number of financial market players.

It can be said that cyber incidents have no borders and can easily spread widely, affecting several sectors beyond geographical borders, including entities that were not targeted by attackers. Cyber incidents are becoming more and more destructive, persistent and rapidly increasing, illustrating the high level of sophistication and coordination that cyber attackers can achieve.

A cyber incident can turn into a systemic crisis when confidence in the financial system is eroded. A critical point in assessing the possibility of escalation of a cyber incident to a systemic financial crisis is whether or not the incident escalates from an operational level to an incident that affects consumer confidence. For a cyber incident to raise systemic financial and trust concerns, it must severely affect the availability of critical functions that support the real economy, with the financial impact being so great that the financial system is no longer able to absorb the shock.

I emphasize two important issues when it comes to cyber risk - firstly, given the speed and magnitude with which a cyber incident can spread, the rapid coordination between the affected entities and authorities is essential in order to minimize the impact of the incident and maintain public confidence in the economy and financial stability. Secondly, the restoration of key economic functions requires detailed planning, involving market authorities, market players, technical infrastructure providers and the availability of financial resources to cover the costs of restoring these functions.

The response of the central bank is essential in addressing such incidents affecting financial institutions, so that such an incident does not trigger a crisis that could affect financial stability.

### 4.2. Possible scenario for cyber risk to become systemic risk

Starting from the previously analyzed studies, I developed a scenario that could target a cyber incident at the level of an RTGS-type payment system - System Y, which could significantly affect capital flows in a national economy.

System Y is a high-value payment system that ensures national interbank payments and the final settlement of debt positions within interconnected ancillary systems (low-value payment system, instant payment system, card payment systems and settlement securities systems). The system is used for central bank operations, treasury operations and liquidity facilities provided by the central bank for credit institutions operating nationwide.

In the current geopolitical context, an Advanced Persistent Threat (APT)-type group has attacked and made the core application of the payment system unavailable. The system can no longer be used by participants. The core application is managed by an external provider. A cyber incident occurs in the first part of the day: there is a security breach through which the attackers managed to obtain the source code of the core application of the payment system and other information. Thus, the attackers are able to exploit a security breach that the application administrators were unable to identify.

Once this incident manifests, the local defense team tries to restart the application but finds that the problem persists. The secondary site has the same errors, as it is technically replicating the primary site.

The incident message is sent to the participants and the oversight and intervention authorities are alerted that a cyber incident occurred.

The system administrator issues a press release, announcing that an operational incident has occurred at the level of the Y payment system and the period for remedying this incident cannot be estimated.

The software solution provider is notified to intervene remotely to fix the incident, but it is found that local intervention is needed to rewrite a new version of the application, so that the system's vulnerability is remedied and the attackers that compromised the application lose the access and control they have over it. A new technical infrastructure must be implemented to prevent the recurrence of a similar incident.

As the outage lasts, the effects on the companies that have to make payment transactions begin to materialize and all these transactions are put in queues, as there are no bank correspondent accounts that can not be used either. In order to avoid blockages, credit institutions have to notify all customers that all domestic interbank payment transactions cannot be made due to a Y-system payment incident that ensures the settlement of interbank payment transactions.

Information about this incident is also publicized by the national media. This creates a state of panic among credit institution customers, who massively go to their respective credit institutions' branches where they have opened their accounts, in order to withdraw their money, fearing that not converting scriptural money into cash will cause them to lose money.

At the same time, a series of messages, which were meant to create panic among the population, appear on social networks, conveying the idea that the money of bank customers was stolen by a cybercrime organization from a neighbouring country.

Context: The incident has its roots in the core software of the Y payment system, which ensures the processing and settlement of payment transactions. The software is developed and maintained by a third-party vendor in a foreign country.

The regional geopolitical context, the war at the border of the country and the firm position of the country towards the attacker create the premises for an APT-type attack of a national critical infrastructure in the financial field.

During the morning, after the first hour of operation, the system becomes totally unavailable.

Restarting the system does not bring any improvement to the system after its re-operationalization at the secondary site. Subsequent investigations make it clear that the system is was under a successful cyber attack that blocked the core application.

The incident lasts all day and fails to settle the daily operations of the system, affecting all interbank payments and does not operate the settlement of net positions related to ancillary systems. The operator has a major impact on credibility, the operational risk materializing also from the perspective of the sanctions it will receive from the oversight authority and the potential penalties that participants will request as a result of complaints from the bank customers that were affected.

The application provider is working on the new version of the application but does not know if it will be able to finalize and test this version until the beginning of the next day.

The database is unaffected by this incident and the vendor's response team arrives at the payment systems' headquarters in the second half of the day, after the end of the banking day.

• Shock: the system does not work throughout the banking day, affecting a volume of approximately 20.000 payment transactions and affecting 6 ancillary systems (low value payment system, instant payment system, net positions from card payment systems Visa and Mastercard and securities settlement systems for the processing treasury bills and for the processing of financial instruments traded on the stock exchange). The estimated value of all transactions to be processed during the day is approximately 100 billion.

As there is no bank correspondent relationship between credit institutions at national level and no other system allows for the processing and settlement of these transactions, the interbank payment transactions are not settled at maturity. The State Treasury is affected, considering that at the time of the incident, the payment obligations for companies related to VAT and payroll taxes were due.

• Impact on the operator: the Y system operator is facing a severe reputational impact due to the materialization of this serious operational incident that has temporarily blocked all critical activities and functions of the system. The short-term financial impact is limited to the sanction applied by the oversight authority, the long-term financial (and legal) impact beyond the costs of strengthening cyber resilience is expected to be severe (for example, penalties charged by customers of credit institutions participating in the system and penalties for delay applied by the state treasury for all delays in the payment of taxes and duties due on the date of the incident).

The panic caused by this incident leads to high liquidity pressure, given that many customers want to withdraw their liquidity from the banking financial system. All ATMs are left without cash and there are very long queues at the bank counters. It creates a general state of nervousness given the need for liquidities – cash is not sufficient at the credit institutions' braches to cover all the liquidity needs of customers who want to liquidate their positions.

• Amplification: all interbank payments are blocked nationwide, panic and distrust starts among bank customers, there are penalties for late payment of fees and taxes, lack of liquidity at bank counters and ATMs and distrust of the population in the banking financial system.

• Reputational impact: the panic created in the national financial ecosystem is difficult to quantify and the Y payment system operator shareholders react cautiously and give up all ongoing projects for the development of the company and focus all resources on strengthening resilience. The participants have major grievances because they are waiting for new developments in the payment system so that they can adopt the new messaging standards for complying with the new requirements for anti-money laundering, countering terrorist financing and to implement instant payments.

The value of the shares on the stock exchange decreases by 20% and the monitoring authority calls for the urgent creation of a liquidity fund to ensure immediate investments in ensuring cyber resilience, including an external penetration test and an external audit of the technical infrastructure. Shareholders are unwilling to provide additional liquidity reserves, considering the potential financial losses caused by this incident.

• Operational incident with financial impact: all interbank payments are blocked, there are major difficulties for credit institutions in finding short-term sources of liquidity as the securities settlement system of treasury bills transactions is no longer able to ensure the final settlement of transactions and the central bank conditions the provision of short-term liquidity of REPO-type operations with treasury bills. There are bottlenecks in the economy, especially among small and medium-sized companies that cannot provide the necessary resources for production because they cannot pay for them.

• The incident affects confidence in the financial-banking sector: the panic created by the financial sector is difficult to manage even if the representatives of the central bank make a series of interventions during the day to assure the population that the national financial system is resilient and does not present liquidity problems, but some groups distribute a series of false information on social networks in order to destabilize the financial sector. All these messages are quickly assimilated by consumers of financial services, due to the low level of financial education. All these elements, combined with the inability of System Y and the authorities to remedy the incident in a short time, will lead to a loss of public confidence in the financial sector.

• Systemic event: in this hypothetical scenario, all domestic interbank payments are blocked. Despite continued efforts to remedy the incident and resume business, the system fails to settle due payments by the end of the day.

Shortly after the initial incident, the software vendor discovers that the core application has a security breach that has been exploited by attackers and that a new version of the application needs to be installed from scratch on a new technical configuration in order to remove the attacker from the infrastructure.

Prolonged disruption of the national payment system, combined with uncertainty and the spread of false news on social networks would trigger a crisis in the financial system, affecting financial stability.

A key point to consider in this scenario is the loss of confidence of the financially uneducated population in the ability of financial institutions to ensure the resilience of the financial sector and the security and safety of clients' funds.

The scenario described above illustrates how a cyber incident at the level of a financial market infrastructure (RTGS payment system) would generate a shock for the financial sector. Lastly, I would like to emphasize that such an incident could materialize through a complex attack by APT-type attackers, given the current geopolitical context.

All the elements described above, together with the uncertainty regarding the nature of the incident and the subsequent speculations on social networks, combine to give this operational event the characteristics of cyber stress, in turn contributing to the transformation of an operational risk of a cyber nature into a systemic risk, with impact on the national financial system and the economy as a whole.

## 5. Conclusions

As highlighted in the paper so far, there have been no cyber incidents with systemic impact on the financial system yet, but the scenario described is plausible given the current geopolitical context. However, it is important to note that cyber risk has the potential to have serious, even systemic, financial repercussions, as detailed in the scenario described above.

The modern financial system has a number of vulnerabilities, in the context of the digitalization of financial services, and the exploitation of these vulnerabilities could trigger a crisis situation as a result of the materialization of a successful cyber attack. In the scenario presented above, the biggest impact on the financial system occurred when several amplifiers were activated, which turned an operational incident into a crisis situation that affected the public's confidence in financial institutions, in the ability of the authorities to solve such a crisis and in the national financial system.

A major financial market infrastructure incident should not lead to a crisis situation, but additional elements amplifying the crisis situation have shown that a cyber incident could trigger a crisis situation with an impact on financial stability. The scenario highlights the loss of public confidence in the financial system, the effects of which are difficult to quantify. The restoration of critical activities and functions after the materialization of a systemic cyber crisis are similar to those observed in financial crises and result in large financial losses and a significant weakening of public confidence in the financial system.

The analysis reveals that the exploitation of vulnerabilities, together with the materialization of systemic amplifiers, can conclude in making a cyber crisis potentially become a systemic crisis.

Further efforts are needed in order to reduce the potential impact of such a crisis and the likelihood of it occurring, by ensuring close collaboration between authorities and financial market actors and the adoption of best practices to ensure cyber resilience.

In order to strengthen the cyber resilience of the financial system, both public authorities and private entities are taking a significant number of initiatives to reduce the risks associated with cyber attacks. Although the characteristics of cyber risk make it completely difficult and costly to eliminate completely, there are a number of policy areas that need to be further explored to identify and mitigate systemic cyber vulnerabilities, thus significantly reducing systemic cyber risk, such as shared information and a detailed mapping of the financial system to identify all the interdependencies in the financial sector.

In the current regional context, a deliberate incident which aims to destabilize the financial system would generate a systemic crisis, given the technical and financial capacity of APT-type cyber attackers.

Authorities have repeatedly stressed the need to address cyber vulnerabilities in risk assessment reports and recent regulations, as they create the context for a cyber incident to turn into a serious crisis with the potential to threaten financial stability. A number of common vulnerabilities were identified, such as inadequate supervision of technical solution providers for the financial sector, which are concentrated in a limited number of providers (large technology companies) or "inadequate cyber hygiene" in all financial market players, which are potential gateways for cyber attackers into the financial system.

The general level of awareness of financial institutions about the need to improve cyber resilience, as well as the preparation of business continuity plans from the perspective of cyber incident management, has increased in recent years. However, continued investment is needed, together with complex tests to strengthen cyber resilience, considering technological progress and given the continued diversification of cyber threats.

## 6. References

- 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*, IMF Staff Discussion Notes, No 20/07, International Monetary Fund, December.
- Adelmann, F.; Gaidosch, T.; Morozova, A.; Wilson, C., 2019, *Cybersecurity Risk Supervision*, Departmental Paper Series, No 19/15, International Monetary Fund, Monetary and Capital Markets Department, September.

- Aldasoro, I.; Gambacorta, L.; Giudici, P.; Leach, T., 2020, Operational and cyber risks in the financial sector, *BIS Working Papers*, No 840, Bank for International Settlements, February.
- Bank for International Settlements and International Organization of Securities Commissions, 2016, *Guidance on cyber resilience for financial market infrastructures*, June.
- Bank of England, 2021, Financial Policy Summary and Record of the Financial Policy Committee, Meeting on 11 March 2021.
- Bank of England, Prudential Regulation Authority and Financial Conduct Authority, 2021, *Operational resilience: Impact tolerances for important business services*, Responses to Bank CPs relating to FMIs, March.
- Bank of England, Prudential Regulation Authority and Financial Conduct Authority, 2018, *Building the UK financial sector's operational resilience*, Discussion Paper Series No 01/18, Bank of England, July.
- Bank of England, 2018, *Could a cyber attack cause a systemic impact in the financial sector?*, Quarterly Bulletin, 2018 Q4
- Basel Committee on Banking Supervision, 2021, *Principles for Operational Resilience*, Bank for International Settlements, March.
- Basel Committee on Banking Supervision, 2013, *Global systemically important banks: updated assessment methodology and the higher loss absorbency requirement*, Bank for International Settlements, July.
- Bouveret, A., 2018, Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, *IMF Working Papers*, No 18/143, International Monetary Fund, June.
- Central Bank of Ireland, 2021, *Consultation on Cross Industry Guidance on Operational Resilience*, Consultation Paper Series, No 140, Central Bank of Ireland, April.
- Danielsson, J.; Fouché, M.; Macrae, R., 2016, *Cyber risk as systemic risk*, [online] Available at: https://voxeu.org/article/cyber-risk-systemic-risk [Accessed 3 February 2022].
- Duffie, D.; Younger, J., 2019, Cyber Runs, *Hutchins Center Working Paper Series*, No 51, Hutchins Center on Fiscal & Monetary Policy at Brookings, June.
- Eisenbach, T.M.; Kovner, A.; Lee, M.J., 2021, *Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis*, Federal Reserve Bank of New York Staff Reports, No 909, Federal Reserve Bank of New York, May.
- European Banking Authority, 2019, *EBA Guidelines on ICT and security risk management*, November.
- European Central Bank, 2022b, *Financial Stability Review*, May.
- European Central Bank, 2021, *IT and cyber risk: a constant challenge*, Supervision Newsletter, 18 August.
- European Central Bank, 2020b, *Annual report on the outcome of the SREP IT Risk Questionnaire*, June.
- European Central Bank, 2020a, *Major European financial infrastructures join forces against cyber threats*, ECB press release, 27 February.
- European Central Bank, 2019, *ECB Banking Supervision: Risk Assessment for 2019*.
- European Central Bank, 2018b, *Cyber resilience oversight expectations for financial market infrastructures*, December.
- European Central Bank, 2017, *Cyber resilience and financial market infrastructures*.
- European Commission, 2021a, *EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents*, European Commission press release, 23 June.
- European Insurance and Occupational Pensions Authority - EIOPA (2020), *EIOPA sets out strategies on cyber underwriting and SupTech*, EIOPA press release, 11 February.
- European Systemic Risk Board, 2021, *Adverse scenario for the European Securities and Markets Authority's 2021 EU-wide central counterparty stress test*, June.
- European Systemic Risk Board, 2020, *Systemic cyber risk*, February.
- European Systemic Risk Board, 2018, *The ESRB handbook on operationalising macroprudential policy in the banking sector*.
- European Union Agency for Cybersecurity, 2021a, *EU Cybersecurity Initiatives in the Finance Sector*, March.
- European Union Agency for Cybersecurity, 2021b, *Glossary*.
- Europol (2020), *Internet Organised Crime Threat Assessment* (IOCTA).
- Financial Stability Board, 2018, *Cyber Lexico*n.
- Financial Stability Board, 2021, *FSB Financial Stability Surveillance Framework*, September.
- Goh, J.; Kang, H.; Koh, Z.X.; Lim, J.W.; Ng, C.W.; Sher, G.; Yao, C., 2020, Cyber Risk Surveillance: A Case Study of Singapore, *IMF Working Papers*, No 20/28, International Monetary Fund, February.

- Healey, J.; Mosser, P.; Rosen, K.; Tache, A., 2018a, *The future of financial stability and cyber risk*, Brookings Institution.
- Healey, J.; Mosser, P.; Rosen, K.; Wortman, A, 2018b, The Ties That Bind: A Framework to Assess the Linkage Between Cyber Risks and Financial Stability, *CRFS Working Paper*.
- Heijmans, R.; Wendt, F., 2020, Measuring the Impact of a Failing Participant in Payment Systems, *IMF Working Papers*, No 20/81, International Monetary Fund, June.
- Kopp, E., Kaffenberger, L.; Wilson, C. (2017), Cyber Risk, Market Failures, and Financial Stability, *IMF Working Paper* No 17/185.
- Moody's, 2021, *Sunburst attack on public and private entities raises credit risks as extent of breach unfolds*.
- Office of Financial Research, 2017, *Cybersecurity and Financial Stability: Risks and Resilience*, [online] Available at: https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf [Accessed 15 January 2022]
- Ros, G., 2020, The making of a cyber crash: a conceptual model for systemic risk in the financial sector, *ESRB Occasional Paper* Series, 16/2020.
- World Economic Forum, 2016, *Understanding Systemic Cyber Risk*, White Paper, [online] Available at: https://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_ VERSION_2.pdf [Accessed 10 January 2022]