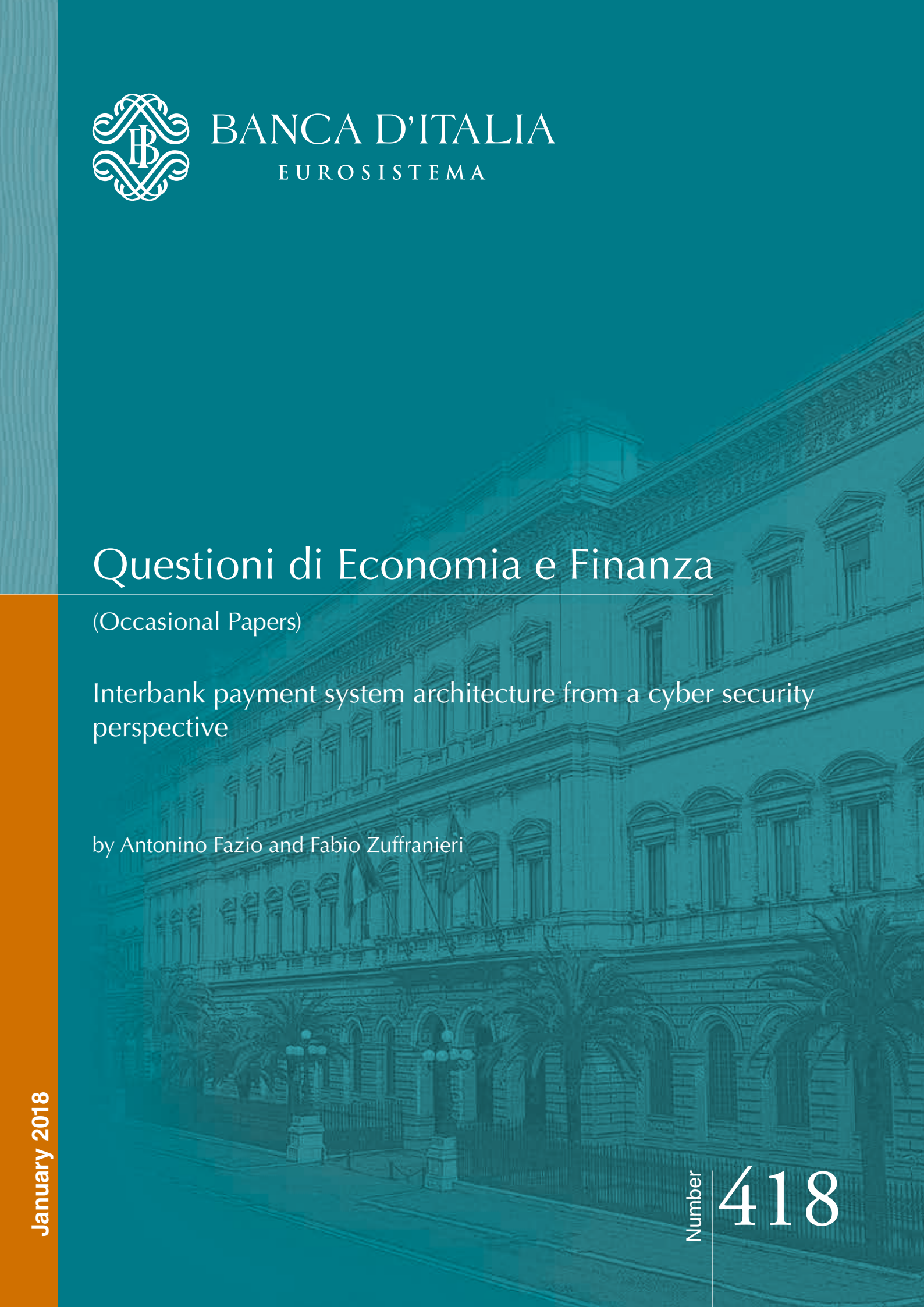
BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

Interbank payment system architecture from a cyber security perspective

by Antonino Fazio and Fabio Zuffranieri



January 2018

Number 418

BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

Interbank payment system architecture from a cyber security perspective

by Antonino Fazio and Fabio Zuffranieri

Number 418 – January 2018

The series Occasional Papers *presents studies and documents on issues pertaining to the institutional tasks of the Bank of Italy and the Eurosystem. The* Occasional Papers *appear alongside the* Working Papers *series which are specifically aimed at providing original contributions to economic research.*

The Occasional Papers *include studies conducted within the Bank of Italy, sometimes in cooperation with the Eurosystem or other institutions. The views expressed in the studies are those of the authors and do not involve the responsibility of the institutions to which they belong.*

The series is available online at www.bancaditalia.it .

ISSN 1972-6627 (print)
ISSN 1972-6643 (online)

Printed by the Printing and Publishing Division of the Bank of Italy

INTERBANK PAYMENT SYSTEM ARCHITECTURE FROM A CYBER SECURITY PERSPECTIVE

by Antonino Fazio* and Fabio Zuffranieri*

Abstract

This paper outlines how a paradigm shift is required when approaching cyber risk management for interbank payment systems, which are affected by the growing interconnectedness of systems, the digitalization of financial services and continuously evolving cyber threats. In this scenario, cyber threats may derive from a wider number of actors, who are constantly active on the Internet and able to exploit an increasing number of vulnerabilities and attack vectors to achieve their goals. Financial institutions should therefore assume that specific cyber threats can overcome any defence. Firstly, the paper outlines the theoretical reasons for this necessary paradigm shift; secondly, it aims to highlight the importance of all the stakeholders in strengthening the cyber resilience of payment systems, in particular the central and enabling role of messaging service operators, by providing an analysis of a real case study - the recent Bangladesh Bank cyber fraud; and finally, the paper aims to encourage discussion on the new paradigm and the adequacy of current regulatory frameworks and supervisory approaches.

JEL Classification: E42, F50, K24, L50.
Keywords: payment systems, cyber security, cyber resilience.

Contents

* Bank of Italy, Directorate General for Markets and Payment Systems.

1. Introduction

Banks and payment services providers, particularly in the field of retail payments (card and internet payments), are generally considered the most exposed to cyber threats due to the economic motivation of cyber-criminals and the relative ease with which the end user, typically the weakest link in the security chain, can be attacked. Yet some recent cases, such as the cyber fraud against the Bangladesh Bank or the Shadow Brokers' leaks, are of particular concern because they highlight vulnerabilities also in the interbank environment and financial infrastructures, until now areas considered less exposed to cyber risks. Such cases demonstrate that cyber attacks have the potential to affect even the core elements of the global financial system, and given the broad interconnectedness of systems, may have implications for financial stability.

To address these emerging risks, financial regulators and supervisors have launched several initiatives, both at national and cross-border level (G7, BIS, FSB and so on), to enhance the cyber resilience of the financial systems. At the same time, the financial industry has set up programmes for improving security for financial system participants (e.g. the SWIFT Customer Security Program).

However, some of these actions are based on a traditional paradigm, which assumes that all interbank payment system security relies on trust among its participants and operators, as they are a closed system. The increasing digitalization of financial services coupled with the extreme interconnectedness of the financial sector impose a deeper insights on mutual risks posed by logical and physical interconnections which requires cyber security to be approached in two complementary ways: i) financial institutions should be aware that attackers are able to overcome their counterparts even strong defenses and therefore can't consider them as fully trusted entities; and ii) the operators of central infrastructures (payment systems and messaging services) should adopt proactive measures to help improve the overall security of the systems.

2. Interbank payment system architecture

This paper does not intend to provide a comprehensive overview of interbank payment system architecture but will focus on some specific elements deemed relevant to the topic under discussion.

1.1. Messaging and routing functions in interbank payment systems

Payment systems facilitate commercial and financial transfers between buyers and sellers and for this reason are important components of a country's financial system. They comprise a set of

financial institutions, supporting technological infrastructures and setups which share rules, processes and standards to make payments efficient and secure.

In spite of the adoption of international standards, every country's payment system has its own features, reflecting banking and financial history as well as the technological development of information and communication infrastructures.

Financial institutions communicate with each other **through a messaging and routing system (MRS)**. Transactions, labelled with codes identifying the beneficiary's bank, are routed through automated clearing houses (ACHs)[1] which manage the transmission and reconciliation of payment orders and determine the final balances to be settled. Usually, transactions are settled in different systems according to the type of payments and instruments, namely large value (RTGS), retail (RPS) or securities (SSS), through the debiting/crediting of the accounts of the parties involved in the transaction. Accounts are generally opened at central banks to ensure settlement finality for each transaction and foster trust and confidence in the whole system (Figure 1).

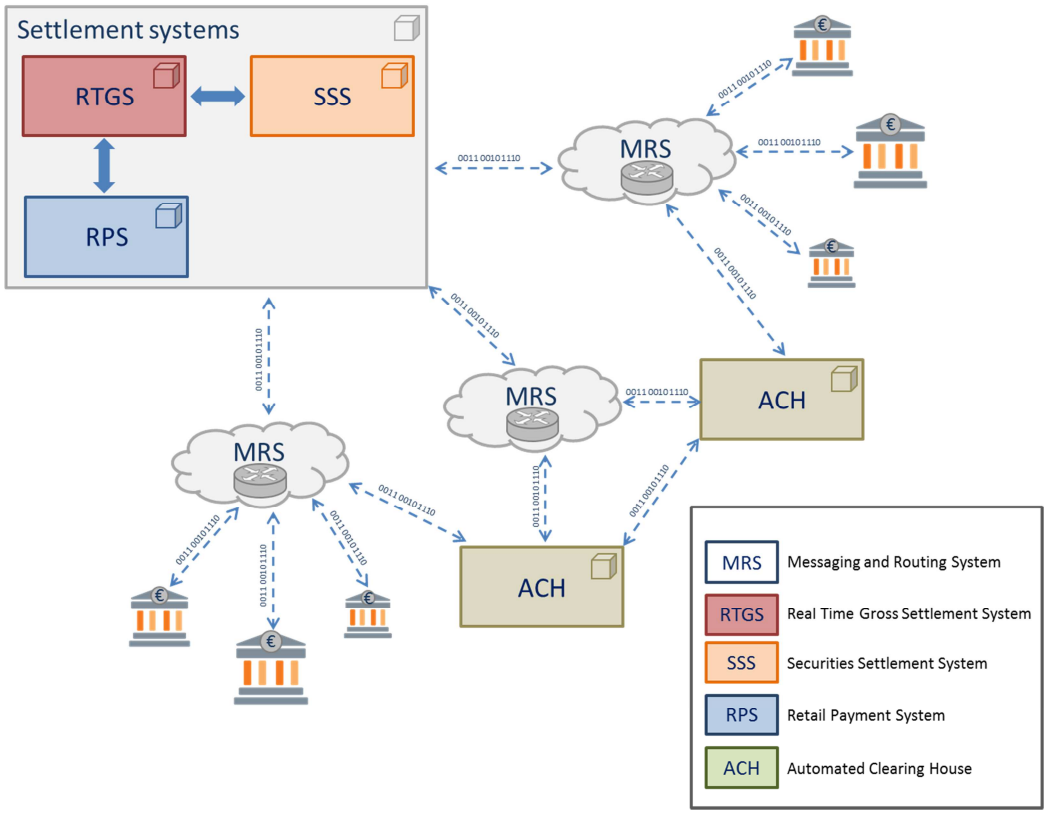


Figure1: MRS role in the Domestic Payment System

[1] Large value payments (LVPs) are generally sent directly to a settlement system.

When the parties of the transaction belong to different countries which do not share common infrastructures and/or procedures, the payment cycle is similar to that described above, but the international MRS functions as a hub where all transactions are channelled, playing an even more central and critical role in the smooth functioning of the system. In this case, settlement can even not occur in the account systems of a central bank, and obligations can be handled by bilateral banking accounts (correspondent banking). Such a method can also be used between banks belonging to the same country, leveraging the services of common network infrastructures (Figure 2).

For historical reasons, only one company is currently playing the role of the international MRS, namely SWIFT.[2]

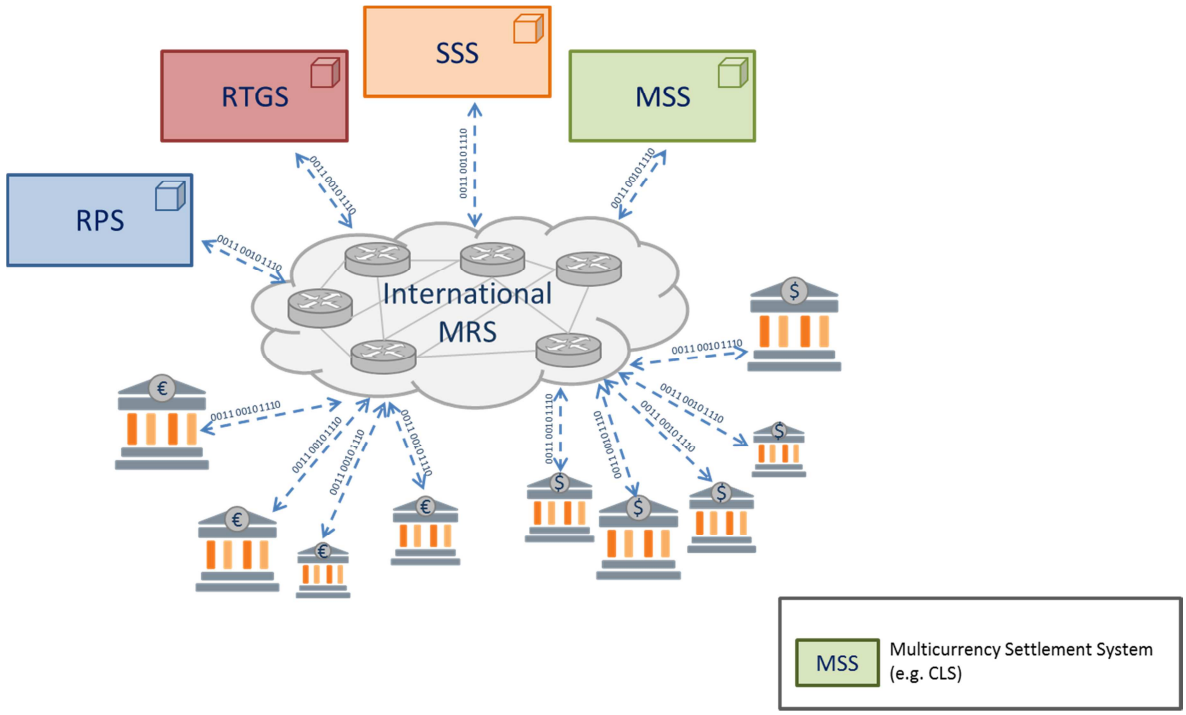


Figure2 MRS role in the Cross-border/International Payment System

[2] SWIFT (Society for Worldwide Interbank Financial Telecommunication) is a Belgium-based cooperative society linking more than 11,000 financial institutions, including 193 central banks, in more than 200 countries. 'In 1973, 239 banks from 15 countries got together to solve a common problem: how to communicate about cross-border payments. The banks formed a cooperative utility, headquartered in Belgium. SWIFT went live with its messaging services in 1977, replacing the Telex technology that was then in widespread use, and rapidly became the reliable, trusted global partner for institutions all around the world. The main components of the original services included a messaging platform, a computer system to validate and route messages, and a set of message standards. The standards were developed to allow for a common understanding of the data across linguistic and systems boundaries and to permit the seamless, automated transmission, receipt and processing of communications exchanged between users'. - www.swift.com

1.2.Payment system security architecture

In the second half of the twentieth century, when electronic payment systems were created, all stakeholders (financial institutions, ACHs, settlement systems and so on) were looking for a fast, automated, secure, easy and low-cost way to operate their financial and commercial transactions. Hence, they set up infrastructures that directly connected financial institutions and operators (banks, ACHs, settlement systems and so on), through some information and communication technical companies (Service Providers), mainly owned by the same banks. The answer - and the result - was a 'closed' system of financial entities (mainly banks or bank-owned entities) where a bank receiving a message from another bank could be sure of the authenticity of the sender and of the integrity of the message. The system's security architecture reflected the structural 'trust' shared by the participants. As a consequence, once 'in', there was no need to closely control messages flowing between participants, as the sender and the receiver trusted each other as well as their messaging and routing systems (*trust paradigm*).

For example, with regard to the cross-border interbank payment system where, as mentioned above, the MRS is provided by SWIFT, a payment message going from Bank A to Bank B is not subject to any other authorization control when entering/exiting the SWIFT network. Controls are eventually implemented only in Bank A's own infrastructure and completely rely on Bank A's ability to make its infrastructure safe (Figure 3).

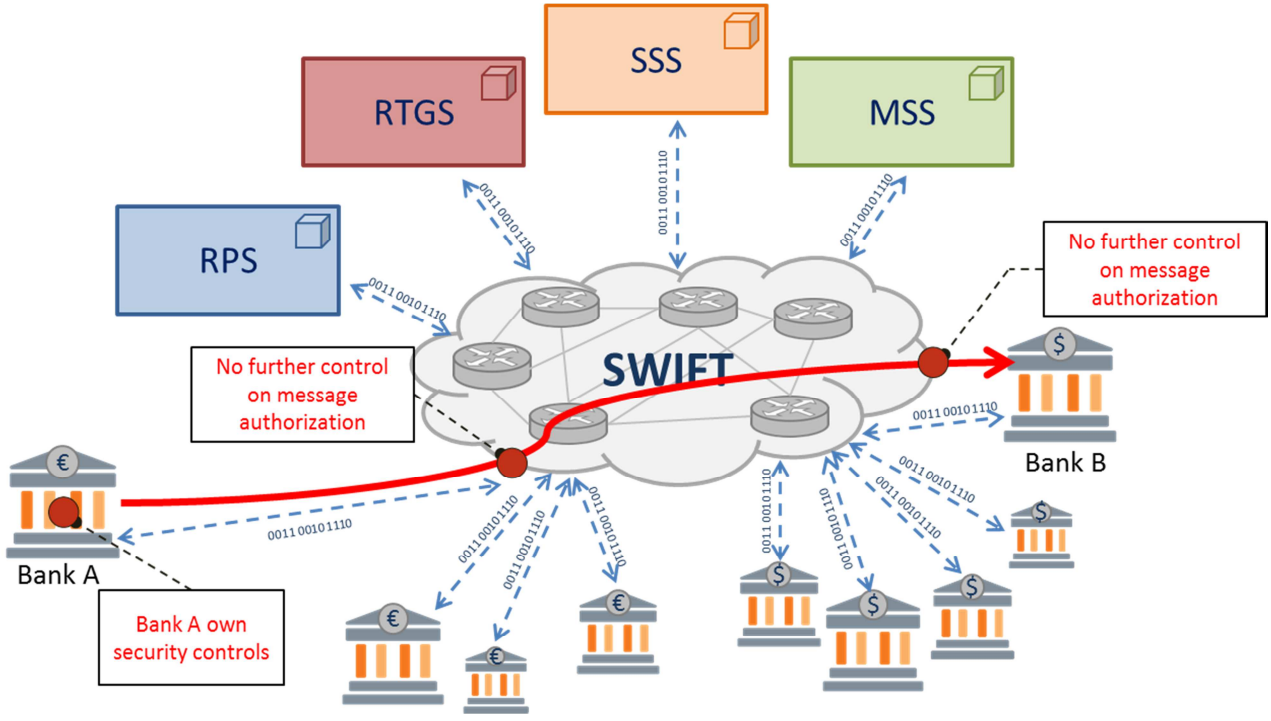


Figure3.Messagge flow through the Cross-border/International Payment System

3. Payment systems and cyber security

In recent years, several cyber disruptions in critical sectors have demonstrated that the scenario has completely changed.

Participants in payment systems, both at national and international level, are connected to the Internet, and are therefore individually and collectively exposed to cyber risk.[3] Although the economic analysis of the cyber risk is still in the early stages (see Box 1), the new scenario and its embedded digital innovations are having a profound effect on the financial environment.

The role of technology in the provision of financial services is becoming paramount. Interconnections among operators in financial markets have greatly increased, due to widespread digitalization. From the attackers' side, the incentives and reasons for violating the financial system are increasing as well. There is a wide range of motivations, e.g.: 'hacktivists', who seek merely to disrupt activity; cyber criminals, motivated by financial gain; terrorists, aiming to cause political and financial instability; and 'nation-state related actors' attempting to interfere with or gain access to sensitive information, or to cause systemic instability (Bank for International Settlements, 2014). Attackers are also using increasingly sophisticated and evolving tactics, techniques and procedures (TTPs) to exploit potential weaknesses in the technology, processes and people of financial institutions (e.g. advanced persistent threats - APT - which are driven by intelligence gathered on the potential victims through social engineering actions and then deliver malware into a company's IT systems). At the same time, the entry points through which a participant in payment systems can be attacked are multiplying and include counterparties, vendor products and employee workstations. Moreover, through the payment systems, the financial sector provides services to other critical sectors; therefore a successful cyber attack against payment systems can have implications for/repercussions on the wider economy.[4]

BOX 1: OPEN CYBERSECURITY ISSUES FROM AN ECONOMIC PERSPECTIVE

Despite the increasing importance of securing cyberspace in the digital age and the growing attention paid by the media to cybersecurity, the economic analysis of cyber risk does not yet appear complete. Further insights seem necessary both from macro and microeconomic perspectives.

Being related to the development of the Internet and digital technologies, cybersecurity has been studied so far with reference to the theories of Internet economics, which emphasize the role of externalities, price structures, costs, coordination failures, lock-in effects and so on. It still lacks a more detailed analysis of cyber risk peculiarities (e.g. borderless and cross-sector) and emerging trends such as: i) the asymmetry and evolving nature of the cyber threats;[5] ii) the scarcity of reliable and comparable data on cyber risks (vulnerabilities, number of attacks, costs of security and so on); and iii) the lack of coordination, cooperation and shared tools to face cyber attacks effectively.

Some general government commitments to foster an open, secure, interoperable and reliable

[3] Cyber risk can be defined as the risk stemming from operating in cyberspace, a global domain within the information environment consisting of the interdependent network of information system infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (NIST, 2013).

[4] An insight into the cross-sector dimension of cyber threats and coordination amongst critical sectors (e.g. Energy, Telecommunications and Transport) is highly relevant from a policy perspective in order to implement overall effective protection of cyberspace; this topic is on the G7 agenda and that of other international cyber working groups.

[5] Compared with other natural threats or threats from people to the classic domains (air, sea, land and space), cyber threats have the following asymmetric specificities which make it difficult to acquire comprehensive knowledge as well as a clear and regularly updated understanding of the cyber risk landscape: a very low entry cost, a global accessibility, speed of time-scale (micro-seconds), machine control, and rapid evolution in terms of diversification and sophistication.

cyberspace[6] are a first step towards a more tailored and specific analysis of cyber risks. Authorities and operators, mainly in the US after 9/11 (Kaplan, 2016), are already facing the widespread perception of **cyber insecurity** and its possible economic impacts which could significantly reduce investment in technology, slow the pace of its adoption and hamper trade integration in knowledge-intensive sectors, thus affecting economic growth (World Economic Forum, 2014). In this context, although the financial authorities have started to tackle the problem with several forward- looking initiatives (see Box 2), the effectiveness of public responses to cyber attacks are still under scrutiny: 'We are extremely inefficient at fighting cybercrime; or to put it another way, cyber crooks (…) and their activities impose disproportionate costs on society: cyber crimes are global and have strong externalities, while traditional crimes such as burglary and car theft are local' (Anderson &C, 2012, page 1). Privacy, proprietary data and national security concerns limit the type of information that can be exchanged, especially at global level. This should be discussed, if for no other reason than because it puts the onus still further on individual participants.

In order to respond to the scarcity of available and reliable data, international authorities are promoting the development of common definitions and methodologies for collecting data on the technical characteristics of vulnerabilities and the economic impact of cyber attacks, even in the well-developed financial sector (G7, 2016b). An important contribution to the economic evaluation of cyber risks comes from the OECD's studies on the possible insurance coverage for cyber risk, which should provide a means for companies and individuals to transfer a portion of their financial exposure to insurance markets (OECD, 2017). Moreover, insurance markets and companies can potentially contribute to the management of cyber risk by promoting awareness, encouraging measurement, and providing incentives for risk reduction.

According to the approach promoted by some international organizations (CPMI-IOSCO 2016), cybersecurity requires an interdisciplinary and holistic approach which, going beyond technology, encompasses governance, company culture and business processes. Furthermore, recognizing the borderless and cross-sector nature of cyber threats makes it clear that cybersecurity is a matter of the ecosystem of each financial institution and of the whole financial sector; hence cybersecurity requires a shared responsibility and a common endeavour on the part of important stakeholders which amplifies the risk of coordination failures. Bearing this in mind, each entity must be deeply aware of the cyber risks that may come from or that it may pose to other connected entities. However the Bangladesh cyber fraud (see below), as well as the more recent global cyber attacks (e.g. the 2017 Wannacry and Petya/NotPetya attacks) based on targeting third-party partners to infiltrate organizations, shows that the effective handling of such unconventional and unprecedented risks requires a paradigm shift (Cœuré, 2017).

From a microeconomic perspective, an enrichment of the theoretical framework might come from a better understanding and knowledge of **governance approaches/practices on cybersecurity.**[7] In the US, the National Association of Corporate Directors (NACD) is promoting schemes for self-assessing the 'cyber literacy' of boards; verifying the impact of cyber risk on enterprise-wide risk, compliance, risk management, staffing and budgets; suggesting cybersecurity considerations during the M&A phases and developing metrics and dashboards for making decisions (NACD, 2017).

[6] The concluding statement of the G7 Leaders' Summit of May 2016 reads: 'We strongly support an accessible, open, interoperable, reliable and secure cyberspace as one essential foundation for economic growth and prosperity' (G7, 2016a). Similarly in G7 (2017) point 15.

[7] 'Consistent with effective management of other forms of risk faced by a Financial and Market Infrastructure (FMI), sound governance is key. Cyber governance refers to the arrangements an FMI has put in place to establish, implement and review its approach to managing cyber risks (…) It is essential that the framework is supported by clearly defined roles and responsibilities of the FMI's board (or equivalent) and its management, and it is incumbent upon its board and management to create a culture which recognises that staff at all levels, as well as interconnected service providers, have important responsibilities in ensuring the FMI's cyber resilience' (CPMI-IOSCO, 2016, pages 1-2). See also, NBB 2017, pages 86-87.

From a policy perspective, the analysis of the proper (optimal) regulatory framework to foster cybersecurity requires a coordinated and balanced approach between different fields of regulation, such as financial stability, conduct, and privacy (Caron, 2016). Moreover, the intense public/private cooperation which seems to be needed to properly detect and manage cyber risk - according to some per sector/per country cases[8] - still deserve a thorough analysis in order to become an international standard.

Box.1: Open issues from an economic perspective

In such an open and more hostile environment, financial entities can no longer presume to be in a safe, club-like,[9] isolated environment, since attackers, given their asymmetrical capabilities,[10] can overcome **any defence, at a system and at individual level.** This means that a paradigm shift, from 'trust' to 'resilience', is required. In essence, there is a greater onus to design and build secure infrastructure architecture and establish a comprehensive risk management framework. For this reason, some international authorities have already suggested that financial entities design their internal controls based on the assumption that defences have been breached and attackers have already infiltrated the systems ('the attacker is already in' assumption, CPMI-IOSCO 2014).

Following the 'resilience paradigm', financial entities should manage cyber risk by taking into account at least three perspectives: i) the timely detection and sound understanding of potential intrusions are essential enablers for enhancing an organization's response capabilities; ii) the security capabilities of any counterpart are an essential element of the framework; and iii) although counterparts could be perceived as reliable due to their application of security best practices, they could potentially be 'penetrated by advanced and persistent adversaries' and therefore, they should not be deemed as a fully trusted entity.

The aforementioned assumptions are already embedded in leading international security standards and best practices as well as in the recent approach and guidance of the international financial regulators and bodies. In particular, the National Institute of Standards and Technology (NIST) states in Principle 6: 'Assume that external systems are insecure'; 'an **external** domain is one that is **not under your control**. In general, **external systems should be considered insecure**. Until an external domain is deemed to be 'trusted', system engineers, architects, and IT specialists should presume that the security measures of an external system are different than those of a trusted internal system and design the system security features accordingly'. (NIST, 2004)

BOX 2: PAYMENT SYSTEMS - CYBER INITIATIVES

Given the critical role that Financial Market Infrastructures (FMIs), including payment systems, play in promoting the stability of the financial system, the Committee on Payments and Market Infrastructures (CPMI) of the Bank of International Settlements (BIS) has sought to understand the current cyber risks faced by FMIs and their level of readiness to deal with worst case scenarios

[8] As for example CERTFin, the Italian Financial Computer Emergency Response Team, a cooperative public-private initiative promoted by the Bank of Italy and the Italian Banking Association, aims to enhance the cyber security of the financial sector by providing services in the following main areas: i) information sharing and threat intelligence; ii) cyber knowledge and security awareness; and iii) incident response and crisis management.

[9] Maybe this could be the last but most obvious step of a process that started many years ago with globalization.

[10] The asymmetry is due to: a) attacking costs less than defending as tools and malwares are available on the dark web and ready to use even for unskilled people (cybercrime as a service); b) crime imputation is very complex; c) cyber crime regulation is uneven in different countries and attackers can operate from less regulated countries.

effectively. Their work was reported in November 2014 in the document *Cyber resilience in financial market infrastructures* (CPMI-IOSCO, 2014).

After that, the CPMI and the International Organization of Securities Commissions (IOSCO) agreed to act on cyber security by setting up the joint Working Group on Cyber Resilience for FMIs (WGCR) with a mandate to i) investigate the potential implications of cyber attacks against FMIs, including the implications for financial stability; and ii) provide guidance both to authorities (regulators, overseers) and to FMIs to enhance the cyber resilience of the financial sector.

As a result of a detailed investigation into potential cyber risks for the financial system, the WGCR finalized its *Guidance on cyber resilience for financial market infrastructures* ('Cyber Guidance' - CPMI-IOSCO, 2016) in November 2015, which aims to instill international consistency into the industry's ongoing efforts to enhance its cyber resilience. In addition, the Cyber Guidance provides authorities with a set of internationally agreed guidelines to support consistent and effective oversight and supervision of FMIs in the area of cyber risk.

In accordance with these initiatives, local authorities are looking to improve the cyber resilience of payment systems. In Europe, for example, the Eurosystem's overseers have recently launched an Oversight Cyber Resilience Strategy for financial market infrastructures.[11] This strategy is built on three pillars: 1) cyber resilience of individual financial market infrastructures; 2) resilience of the financial sector as a whole; and 3) establishment of a forum which brings together market actors, competent authorities and cybersecurity service providers (Benoit Coeuré, 2017)

Furthermore, the initiatives described are integrated with similar work by banking supervision authorities and, more in general, by financial system authorities: among these initiatives, it is worth mentioning that the G7 countries have drawn up a set of fundamental elements of cybersecurity for the financial sector, as well as three further recommendations on the effectiveness of cybersecurity assessments, third-party risks, and coordination with other critical sectors (G7, 2016b). Moreover, The Financial Stability Board (FSB) highlighted i) the need to monitor cyber risk arising from financial technology (FinTech); ii) to identify the supervisory and regulatory issues from a financial stability perspective; and iii) to mitigate the adverse impact of cyber risk on financial stability among the top three priority areas for future international cooperation (FSB, 2016-2017).

There are different opinions on the need to specifically regulate cyber risk: arguments against the need of regulation claim that, given the evolving nature of cyber risk, it is unsuitable for specific regulation and also that cyber topics are already covered by existing regulation relating to technology and operational risk.

On the other hand, it is argued that a regulatory framework is needed to deal with the unique nature of cyber risk, and with the growing threats resulting from an increasingly digitalized financial sector.

Moreover the discussion also concerns the optimal level of prescriptiveness, which could be achieved with a principle-based or a more prescriptive approach. In the first case, competent authorities should develop flexible supervision procedures in order to adapt to the rapidly changing cyber issues.

The 'CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures' recommends that an FMI should identify the cyber risks that may come from and that it poses to entities in its ecosystem and coordinate with relevant stakeholders, as appropriate, as they design and implement

[11] http://www.ecb.europa.eu/paym/pdf/infocus/20170619_infocus_cybercrime.en.pdf

resilience efforts with the objective of improving the overall resilience of the ecosystem.[12] (CPMI-IOSCO, 2016).

Furthermore, the 'G7 fundamental elements on cybersecurity for the financial sector' highlight that financial entities and authorities should take into account the interconnections and interdependencies in the ecosystem to design and assess effective cybersecurity controls both at the single financial institution and at sector level (G7, 2016).[13]

Referring again to Figure 3, in this new scenario, Bank B should not trust the message coming from Bank A, because Bank A belongs to an external domain, which should be considered insecure. No one can exclude the fact that the IT infrastructure of Bank A has been compromised and that the payment message is not authorized.[14] Therefore, the payment message authorization should be checked somewhere in the flow of the SWIFT network or when it arrives at Bank B.

Summing up: payment systems and the main financial infrastructures were created on the basis of a trusted model where participants could exchange information through a sort of 'closed' and secure IT environment. From a cyber security perspective, this is no longer true, even if systems are still designed and implemented on the premise that all counterparties can trust each other.

Against this backdrop, all the participants in a payment system are potentially subject to a specific cyber risk (SCB), until a change in the system architecture is pursued and applied.

4. Bangladesh Bank cyber fraud

A relevant case study about the aforementioned topics is represented by the Bangladesh Bank (BB) cyber fraud, where cyber criminals exploited customers' IT vulnerabilities to gain unauthorized access to the SWIFT messaging system.

The SWIFT messaging system comprises a set of codes to standardize information across languages, an encrypted network across which messages are passed, and software that financial institutions use to send messages through the network. Its architecture was designed, as described in a previous chapter, assuming the 'trust paradigm'. Messages entered in the SWIFT network by an institution are considered trustworthy and passed to the addressed institution without any further security control (Figure 3).

[12] The BIS and Board of the IOSCO issued their cyber guidance in June 2016 to provide supplementary details related to the preparations and measures that FMIs should undertake to enhance their cyber resilience capabilities with the objective of limiting the escalating risks that cyber threats pose to financial stability. Although the Guidance is directly addressed to FMIs, it broadly discusses the financial system or ecosystem, specifically noting that given 'the extensive interconnections in the financial system, the cyber resilience of an FMI is in part dependent on that of interconnected FMIs, of service providers and of the participants'.

[13] Element 3, Risk and Control Assessment, states that 'in addition to evaluating an entity's own cyber risks from its functions, activities, products, and services, risk and control assessments should consider as appropriate any cyber risks the entity presents to others and the financial sector as a whole. Public authorities should map critical economic functions in their financial systems as part of their risk and control assessments to identify single points of failure and concentration risk. The sector's critical economic functions range from deposit taking, lending, and payments to trading, clearing, settlement, and custody'.

[14] It means that the message could be sent by a cybercriminal on behalf of Bank A. A similar artifact message could be a fraudulent payment disposal or even potentially contain portions of malicious code that could affect Bank B.

In February 2016, the BB was the target of a significant cyber fraud,[15] which, among other things, caused its Governor to resign.

After gaining unauthorized access to the BB's computers, criminals submitted several fraudulent payment orders through the SWIFT network from the BB's accounts BB at the Federal Reserve Bank of New York (Fed), for a total amount of $951 million. Though the majority of fake orders were blocked or recovered, the attackers succeeded in laundering $81 million from casinos in the Philippines.

The joint analysis of the BB and SWIFT, together with external consultants, showed that it was a large scale APT (Advanced Persistent Threat) cyber attack, large enough to compromise the whole BB IT environment and lasted at least two months. The malware used would also have compromised the device for connecting to the SWIFT network (Alliance Gateway), thus making possible the transfer of funds from accounts at the Fed to accounts opened in the Philippines. Most relevant traces of these activities were deleted by the malware itself.

SWIFT immediately declared that the company had no liability for the incident, as the BB's IT environment was not adequately secure and was heavily compromised, allowing the attackers to take control of the SWIFT infrastructure at the BB. Nevertheless, SWIFT, in the interests of the financial community, delivered an 'update' of its software to prevent the traces of transactions on the SWIFT network from being deleted on local computers, thereby assisting their customers in detecting this type of illegal activity.

In the months that followed, news about other similar cases appeared in the press. The frauds affected private financial institutions in Ecuador, Vietnam and other countries in underdeveloped areas. At the moment, there is no certainty that these kinds of attacks are no longer affecting financial institutions.[16]

Given the occurrence of further similar cases, SWIFT launched a program to strengthen the security of the entire ecosystem connected to the SWIFT network. The SWIFT Customer Security Program (CSP) is based on three mutually reinforcing ideas: (1) financial institutions, considered the weakest link of the chain, will first need to protect and secure their local IT environment; (2) users will then need to enhance their capacity to prevent and detect fraud through their commercial relationships (i.e. with their counterparts); and (3) users will need to continuously share information and prepare against future cyber threats (the intelligence on the cases of cyber fraud is collected by SWIFT on behalf of the whole community).

The first part of the program requires the community of SWIFT users to implement a set of core security standards (16 compulsory and 11 optional security controls). They mainly relate to the user's security environment, access to its systems (including the adoption of multi-factor

[15] The information about the Bangladesh Bank cyber fraud reported in this paper has been collected from a number of public sources, mainly press articles and the SWIFT website.

[16] See for example http://www.csoonline.com/article/3075758/data-breach/up-to-a-dozen-banks-are-reportedly-investigating-potential-swift-breaches.html

http://www.businesstimes.com.sg/banking-finance/swift-discloses-more-cyber-thefts-pressures-banks-on-security/

authentication) and the monitoring of unusual transactions on the basis of the behaviour patterns of the participant.

The CSP also includes a set of enforcement measures, through which SWIFT intend tocan? monitor the effective implementation of requirements from clients: it is mainly based on self-assessment and enhancing transparency measures, with supervisors being informed about the non-compliance of individual users. Drastic measures such as the suspension of services to non-compliant banks, which could eventually lead to extreme consequences such as the interruption of operations, are not included in the program.

According to the cyber security principles outlined in Chapter 2, SWIFT itself recognizes that it is also essential to prepare for the possibility that a direct counterparty has been breached, and that financial institutions may receive suspicious traffic over the SWIFT network that originates elsewhere.

For this reason, in the second part of the CSP, SWIFT suggests that financial institutions check that they are only doing business with trusted counterparties, using the SWIFT's Relationship Management Application (RMA), which supports customers by enabling them to control their counterparty relationships over SWIFT and by providing a pre-transaction check that prevents unauthorized receipt of transactions.

Finally, the third part of the CSP regards information sharing and intelligence as being paramount. The reason is that the financial industry is global, and so are the cyber challenges it faces. What happens to one company in one location can be replicated by attackers elsewhere. It is therefore vital to share all relevant information and to inform SWIFT if there is a problem – which is an obligation for all SWIFT customers. SWIFT's dedicated Customer Security Intelligence team has been introduced to help limit community impact by sharing anonymous information in a confidential manner about indicators of compromise (IOCs) and by detailing the modus operandi used in known attacks.

Moreover, SWIFT regularly informs its customers about important cyber intelligence, new market practices and recommendations.

5. The new paradigm

In general, although a counterpart can be considered trustworthy because it is applying security best practices, it could potentially be 'breached by advanced and persistent adversaries' and therefore, it should not be considered as a potentially 'risk free' counterparty (resilience paradigm).

As for any kind of risks, cyber risk needs to be managed with an appropriate risk management framework.[17] Given the evidence of an increasing likelihood of compromise, coupled with the potentially high impact of its occurrence (quite high likelihood-high impact), any form of risk acceptance should be excluded. At the same time, considering the evolving nature and peculiarities

[17] International standards propose four possible ways to manage risks: accept, mitigate, transfer and avoid (see for example ISO3100)

of cyber risks, avoiding it appears unrealistic. Therefore, only the following strategic approaches remain valid: transfer or mitigation or a combination of both.

The first could simply consist of exploring the possibility for financial institutions to sign insurance contracts to cover the cyber risk stemming from other actors of the interbank payment system.

Regarding mitigation, the easiest action could be that the counterparties (the endpoints of the interbank payment system) should enhance their security defences, through a set of security requirements, as is happening with the SWIFT CSP program. Once again, this approach is not enough in light of the new 'resilience paradigm', where it is assumed that the 'attacker is already in', no matter what the defence level is. Assuming that the attacker could overcome any kind of defence, the only measure for bolstering the endpoint security capability is equivalent to a residual risk acceptance, which, as we said, is not adequate in the case of a quite high likelihood-high impact risk.

Therefore, further mitigation actions should be introduced, with the interbank payment system considered as an ecosystem and above all, not only limited to its endpoints (i.e. banks), for example:

1) given its central role in the system and when considered as an active player, the MRS could be asked to implement a set of centralized controls on the authorization of messages flowing through the infrastructure;
2) an alternative, if the MRS is considered as a mere message carrier with a passive role, is that the message sender and receiver can be thought of as being directly and physically connected. In this case, it should be up to the receiver to implement controls on received messages, for example exchanging acknowledgement messages with the sender, likewise in the case of securities transactions;
3) each participant could be required to enhance their response capabilities in order to counter the potential frauds stemming from its payment system counterparts.

6. Conclusions

Interbank payment systems were designed on the basis of the 'trust paradigm', due to the closed network environment where intermediaries were connected through secure and reliable IT services providers. In this context, all interconnected entities essentially trust each other and the cyber threats would mainly come from insiders (e.g. disloyal employees).

Due to the increasing digitalization and openness of financial services within the Internet, the paradigm has changed and cyber threats can arise from a broader number of financial and non-financial motivated threat-actors active on the Internet 24/7 and capable of exploiting an increasing number of vulnerabilities and attack-vectors to achieve their goals (i.e. activists, cyber criminals, proxy-state and nation–state actors). Financial entities can no longer assume that they are in a safe, club-like, isolated environment, since attackers are able to overcome any defence.

So far, despite the evolving scenario (characterized by the increasing IT consumerization, the intensive digitalization of the economy and the evolving cyber risk landscape), the security

architecture of payment systems seems to have remained essentially the same, based on the 'trust paradigm', which financial institutions rely on, but at the cost of being exposed to **specific cyber risks (SCR)** for the entire financial community.

A paradigm shift, moving from 'trust' to 'resilience', should guide the building of the new security architecture and risk management framework. For this reason, some international authorities have already suggested that financial entities design their internal controls based on the assumption that defences have been breached and attackers have already infiltrated their systems.

The most prominent example of the urgency regarding that shift is the BB cyber fraud (and other similar cases not solved yet), which involved financial institutions and the international MRS, SWIFT. On several public occasions, SWIFT has claimed that its system wasn't actually directly compromised in any of the attacks, but this argument may be misleading. The system is no less vulnerable whether the attacks target its core infrastructure or the connections to it. Therefore, even when using a well-known, secure and trusted network, like SWIFT, the financial institution receiving a message (which remains the only entity responsible for controlling message flows and protecting itself), should have a security framework in place to protect itself, as if it were exposed to a potentially hostile environment.

Against this backdrop, the implementation of the cyber security controls included in SWIFT's Customer Security Program as mitigation measures for the SCR may not be enough, firstly because the enforcement may not be easy to achieve in the short term[18] and secondly because it is not completely clear who will guarantee the financial entities' compliance and how, but above all, because the system will continue to rely only on the previous 'trust paradigm'.

Regulators and supervisors should seek effective approaches to cope with the new scenario. In particular, further investigations are needed to explore potential actions and to find feasible solutions for the proper management of the SCR, both in terms of transferring or mitigating it. In this context, a detailed analysis of the role of MRSs should be carried out, as they could be considered an active part of the whole interbank payment system or a technological infrastructure, at the very least. Finally, the current regulatory frameworks and supervisory approaches, although successful in fostering an awareness of cyber-related issues, should be evaluated and eventually revised to verify whether they fit with the SCR or whether they need additional requirements.

[18] Users will self-attest against the SWIFT security controls during 2017, and only in 2018 will SWIFT mandate a sample of its users to demonstrate this self-attestation with confirmation from an internal or external audit. This sample will be used to ensure the quality of the self-attestation process, and will look for structural/framework issues such as common difficulties in interpreting a specific control.

References

Anderson & C (2012), *Measuring the Cost of Cybercrime*, in http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf

Bank for International Settlements and Board of the International Organization of Securities Commissions (2016), *Guidance on cyber resilience for financial market infrastructures*, June 2016

Benoît Cœuré (2017) *Remarks by Benoît Cœuré, Member of the Executive Board of the ECB, at the High-Level Meeting on Cyber Resilience*, http://www.ecb.europa.eu/press/key/date/2017/html/ecb.sp170619_1.en.html

Biancotti C. (2017), *Cyber Attacks: Preliminary Evidence from the Bank of Italy's Business Surveys*, Occasional Papers 373, Bank of Italy.

Biancotti &C. (2017), *Cyber attacks: an economic policy challenge* in VOX CEPR's Policy Portal

Caron, F. (2016), *Cyber risk response strategies for financial market infrastructures*, in NBB Financial Stability Report, 171-185.

CPMI-IOSCO (2014), *Cyber resilience in financial market infrastructures*, November 2014

CPMI-IOSCO (2016), *Guidance on Cyber Resilience for FMI*, June 2016

FSB (2016), *Financial Stability Board agrees 2017 workplan*, press release, 17 November.

FSB (2017), *Financial stability implications from FinTech: supervisory and regulatory issues that merit authorities' attention*, 27 June

Financial Stability Institute (2017), FSI Insights on policy implementation No 2, *Regulatory approaches to enhance banks'cybersecurity framework*, August 2017, https://www.bis.org/fsi/publ/insights2.htm

Jon Danielsson, Morgane Fouché, Robert Macrae (2016), *Cyber risk as systemic risk*, in http://voxeu.org/article/cyber-risk-systemic-risk

G7 (2016a), *Leaders' Declaration*, Ise-Shima, May 2016

G7 (2016b), *G7 fundamental elements of cybersecurity for the financial sector*, October 2016.

G7 (2017), *Leaders' Communique*, Taormina, May 2017

Kaplan F. (2016), *Dark Territory. The Secret History of Cyber War*, Simon & Schuster, New York.

NACD (2017), National Association of Corporate Directors, *Cyber Risk Oversight*, Directors Handbook Series, Washington, January 2017

NBB (2017), National Bank of Belgium, *Enabling Technologies in FMIs and payment systems* in The Financial Market Infrastructures and Payment Services Report, Brussels

NIST (2004), *SP 800-27 Rev A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A*, Recommendations of the National Institute of Standards and Technology, June 2004

NIST (2013), *NISTIR 7298 Rev 2, Glossary of Key Information Security Terms*, May 2013

OECD (2014), *Measuring the Digital Economy. A New Perspective*, Paris

OECD (2017), *Supporting an effective Cyber Insurance Market*, OECD Report for the G7 Presidency, Paris

Westby J. (2012), *Governance of Enterprise Security*, CyLab 2012 Report, Carnegie Mellon University, 16 May

World Economic Forum (2014), *Risk and Responsibility in a Hyperconnected World*, Washington