BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

Cyber resilience for business continuity in the financial system

by Boris Giannetto e Antonino Fazio

April 2022

Number 18

BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento
(Markets, Infrastructures, Payment Systems)

Questioni istituzionali
(Institutional Issues)

Cyber resilience for business continuity in the financial system

by Boris Giannetto e Antonino Fazio

Number 18 – April 2022

The papers published in the 'Markets, Infrastructures, Payment Systems' series provide information and analysis on aspects regarding the institutional duties of the Bank of Italy in relation to the monitoring of financial markets and payment systems and the development and management of the corresponding infrastructures in order to foster a better understanding of these issues and stimulate discussion among institutions, economic actors and citizens.

The views expressed in the papers are those of the authors and do not necessarily reflect those of the Bank of Italy.

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

Printed copies can be requested from the Paolo Baffi Library: richieste.pubblicazioni@bancaditalia.it.

ISSN 2724-6418 (online)
ISSN 2724-640X (print)

Banca d'Italia
Via Nazionale, 91 - 00184 Rome - Italy
+39 06 47921

Designed and printing by the Printing and Publishing Division of the Bank of Italy

Cyber resilience for business continuity in the financial system

Boris Giannetto e Antonino Fazio*

JEL: F50, G38, K24, L50, O33.
Peywords: cyber resilience, systemic scenario analysis, business continuity, financial system, cybersecurity.

CONTENTS

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

1. Abstract[1]

This paper presents initiatives and measures to foster cyber resilience for business continuity in the financial system.

Threats are increasingly varied and hybrid:[2] cyber and natural events,[3] fires, epidemics and pandemics, geopolitical tensions, terrorist attacks and other phenomena.

Since several interconnections characterize the financial sector, it is important to intervene quickly to prevent and contain cyber threats: an event in a single infrastructure, if not promptly addressed, can rapidly spread to the entire system, with chain reaction effects. Furthermore, the diffusion of digital technologies has been widening the attack surface of systems exposed to cyber events.

In this context, cyber resilience is a central tool for preventing and managing events that can affect business continuity in the financial system.

After describing developments in the external context (chapters 1, 2 and 3), this paper outlines key institutional initiatives launched at the national (chapter 4) and international (chapter 5) level to strengthen cyber resilience in the financial system, including ad hoc measures adopted over time by the Bank of Italy (BDI). Evolutionary issues are then addressed (chapters 6 and 7), before moving on to the conclusions.

---

1 This text is the English version of a paper published in Italian on the institutional website of the Bank of Italy on 9 March 2022. The views expressed here are those of the authors alone and do not necessarily reflect those of the Bank of Italy. After the publication of the present paper in Italian, the EU Commission launched on 16 March 2022 an EU public consultation on a forthcoming "European Cyber Resilience Act".

2 For a definition of hybrid threat, see EU Commission, Industry and Defence Space: 'Hybrid threat – state or non-state actors seek to exploit the vulnerabilities of the EU to their own advantage by using in a coordinated way a mixture of measures (i.e. diplomatic, military, economic, technological) while remaining below the threshold of formal warfare'.

3 A cyber event is 'Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring'. Source, the Financial Stability Board's Cyber Lexicon.

1. Context evolution

The digitization of the economy and society represents an undoubted spur for progress; however, it can also engender cyber risks and threats.[4]

Geopolitical confrontation between states makes the financial system – by virtue of its openness to online services and the transnational nature of cyberspace – particularly exposed to cyber-attacks.

New risks, in addition to undisputable opportunities, also derive from the increasingly widespread use of advanced information technologies and telecommunications systems (development of artificial intelligence algorithms is just one example) in new financial products and services.

Relationships between the financial system, new technologies and security are becoming increasingly important; FinTech – a term used to refer to financial products and services that involve advanced information and communication technologies (ICT) – is no exception (on FinTech and security, see WEF, 2020 and Bank of Italy, 2022).

Over the last few years, the disintermediation of traditional financial entities – resulting from technologies based on decentralized systems – has been increasing (e.g. *DeFi* - decentralized finance).[5]

A continuous evolution of in the ICT market requires both the development of new security models (Ciocca, 2020) and innovative regulatory approaches (Perrazzelli, 2021). Measures ought to be planned according to a cross-authority and cross-border approach, not only at the national level.

WHAT IS FINTECH?

The English term FinTech refers to financial technology, namely highly technological tools that generate innovation in the financial services market. Such tools may relate to financing, payment, investment and advisory services. In this context, public authorities carefully scrutinize trends in progress, in order to promptly define initiatives and interventions that safeguard the public interest by guaranteeing an adequate balance between opportunities and risks in the innovation process.

Financial institutions and operators are facing growing challenges in ensuring adequate controls and security levels in the supply chain of digital financial

4 Cyber risk could be defined as 'The combination of the probability of cyber incidents occurring and their impact.' and cyber threat as 'A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security' – Source, Cyber Lexicon FSB.

5 Financial authorities, including European ones, have repeatedly warned against risks (volatility, complexity of underlying technologies, regulatory and legal uncertainty) associated with investing in cryptocurrencies. At the same time, they have undertaken actions for governing change and launching innovative initiatives at the institutional level.

services. Defence measures must be continually fine-tuned to cope with rapid and relentless technological transformation.

In this context, security is no longer an ancillary feature; it becomes a central asset for infrastructures and services. Safeguarding digital operational resilience is strategic (BCBS, 2020a, 2020b).

Collaboration between financial institutions, the private sector, academia, intelligence and law enforcement bodies is also important for enhancing cyber resilience at a systemic level. To do this, states should aim for an adequate national workforce as well as a solid and strategic relationship between institutions and private entities (Baldoni, 2021a, 2021b).

2. Cyber threats in the financial system

To describe trends that characterize cyber threats in the financial system, attention should be paid to: (1) nature of threats; (2) target organizations; (3) threat actors; (4) possible purposes underlying malicious operations; (5) type of campaigns and attacks; (6) state confrontation and main measures to strengthen cyber sovereignty available to public authorities.

Cyber threats and other phenomena – such as natural events, climate change, political, economic and financial instability, social precariousness, migration, geopolitical tensions, terrorist attacks, epidemics and pandemics – are more and more interconnected (WEF, 2021, 2022).[6]

HYBRID THREAT PHENOMENON

'Hybrid threat' indicates a situation in which state or non-state actors attempt to exploit the vulnerabilities of a target to their advantage (e.g. in a financial infrastructure), using a combination of (diplomatic, military, economic, technological) measures, while remaining below the threshold of formal warfare. This phenomenon implies a deliberate desire on the part of the actors to hit one or more targets with different means.

Threats are often intrinsically hybrid (Sørensen and Nyemann, 2018). Beyond threat interconnection, threat actors pursue more and more multiple goals, by hitting different targets, using various means (Treverton *et al.*, 2018). Cyber-attacks are preferred tools, since they are often difficult to detect and perpetrators are rarely prosecuted cross-border, for lack of certain and conclusive evidence or because of jurisdictional issues.

[6] This interconnection was particularly evident during the Sars-Cov-2 pandemic emergency. Ordinary threat modelling activity already had been highlighting indeed links between pandemics, cyber threats and financial organizations even before the COVID-19 pandemic phenomenon broke out (Bodeau, McCollum & Fox, 2018). As for a predictive analysis about pandemics, see (Coats, 2019).

Although cyber threats are inherently cross-cutting (they actually affect almost all sectors), the financial system is undoubtedly one of the most targeted.

Targets of malicious actions in the financial sector include central banks, commercial banks, payment system providers, money transfers, cryptocurrency exchange companies, other financial organizations and users.

Threat actors are mainly hackers, cyber-criminals, hacktivists (hackers acting for ideological, political, civil disobedience, etc.), cyber-terrorists and state entities (Maurer and Nelson, 2021). Attackers can sometimes have huge resources and high technical capabilities, as is the case of Advanced Persistent Threats (APTs).[7]

Malicious actions are ever more attributed (sometimes by government bodies) to specific cyber units of intelligence agencies. This phenomenon is worthy of attention, due to the advanced cyber equipment and broad rules of engagement of these units.

However, one ought to be very careful in attributing attacks, since disinformation, anonymization and source obfuscation are widespread phenomena that constitute often one of the components of the attack itself.[8] Difficulties in attribution may, for example, be encountered in presence of 'false flags' operations, conducted with the intent of blaming another actor for an attack (e.g. through infrastructure hijacking).[9] Conversely, the 'name & shame' phenomenon – in which one accuses a threat actor (for example a state) of a cyber-attack – can also be used for purposes of diversion and deterrence.

As for the purposes, cyber malicious actions in the financial sector can cover assets, tasks and reputation: theft, fraud, exfiltration or manipulation of data and information,[10] protest actions, espionage, actions against reputation and disruption of infrastructures.

---

7 According to the FSB's Cyber Lexicon, an APT is 'A threat actor that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple threat vectors.' APT: '[…] pursues its objectives repeatedly over an extended period of time'.

8 As far as *anonymization* is concerned, *virtual private networks* (VPNs) prevent often to track true IP chains. *Obfuscation* techniques make difficult *reverse engineering* on artefacts; cryptographers strive to develop *fully undetectable malwares* (FUD). Steganography (a technique that aims to hide communication – or rather the very existence of communication – between sender and receiver; from the Greek στεγανός, covered and γραφία, writing) and advanced exfiltration techniques – that are often prerogative of state *tiger teams* – make hard to defend IT perimeters. Super computers, quantum computing and post-quantum cryptography can change current scenarios.

9 In this type of operation, an attacker acquires control – through a malicious cyber action – of the tools used by another threat actor (for example its command and control – C2 – infrastructure and software used for cyber-attacks), to conceal its action. However, a *false flag* can also be a simple mimicking of the tactics, techniques and procedures (TTPs) used by another actor.

10 The use of the term exfiltration is common in this context; it derives from the English phrase "data exfiltration"; in Italian it is sometimes also "data extrusion"; to simplify, it can be associated with data theft and data breach. As for manipulation of data and information, *adversarial machine learning* attacks – techniques aimed at compromising the correct functioning of a computer system that uses machine learning algorithms – can have even more serious effects than exfiltration (impacts can be very significant for a financial organization).

At the country level, attacks can aim at conducting disinformation and cyber espionage[11] actions or even at altering financial and geopolitical equilibrium; nation-state and state-sponsored cyber-attacks can sometimes be part of wider campaigns of psychological operations (PSYOP) and information operations (IO)[12].

Cyber-attacks in the financial sector aim ever more to exploit specific vulnerabilities and characteristics of organizations (ENISA, 2020a, 2020b) (in such cases there is a preventive action of profiling and social engineering).[13] The fastest growing phenomena are the following: ransom requests sometimes connected with attacks that make services unavailable or disrupt infrastructures, fraud and theft (for example at ATMs, hacks against crypto-currency exchanges, wallets exploits),[14] operations against supply chain, actions against reputation and name. In particular, there is a continuous increase in ransomware campaigns, data leaks, *cryptojacking*, *DDoS* and *RDDoS*, supply chain attacks, disinformation, as well as phishing in its various forms (EUROPOL, 2020, 2021; ENISA, 2021a, 2021b).[15]

High speed of (true, partially true or false) news propagation increasingly accompanies cyber events (attacks, malfunctions, etc.), also through uncontrollable viral news and echo chambers[16] on the Internet (Giannetto and Paganini, 2020): this feature is able to influence financial markets in a particularly rapid way. A balanced and proportionate management of news and external exposure can be crucial for business continuity, as well as a resilient management of events.

Physical and logical attacks often go together; hence, information systems should be upgraded to interact continuously with the physical context in which they operate (cyber-physical systems). Simple attacks are still massive and widespread, even though sophisticated and technologically advanced attacks are on the rise too.

---

11 This indicates an activity of collecting secret or sensitive information by means of IT tools for personal, economic, technological or political purposes; targets can be individuals, companies, institutions and states.

12 Even economic motives and theft of money – contrary to what one might think – can also be a trigger for operations launched by some state agencies. Intelligence units – to maximize results, while minimizing costs – can sometimes resort to simple and economic means available *in the wild*, also to mislead the origin of attacks. These units are obviously also capable of fielding advanced reconnaissance, intrusion and exfiltration techniques, that are secret and scarcely detectable by common systems, including those in use in financial institutions and organizations.

13 Social engineering is 'A general term for trying to deceive people into revealing information or performing certain actions' (FSB, Cyber Lexicon).

14 In *crypto* environments, wallet thefts, exchange hacks and ransomware attacks (with related illicit proceeds) are often associated with money laundering phenomena (from virtual to physical). It is also worth pointing out the occurrence of money laundering in the opposite direction (from physical to virtual), especially for funds deriving from organized crime activities. In this regard, national and international AML/CFT measures are important.

15 According to the ENISA Threat Landscape 2021: 1) 'Ransomware is a type of malicious attack where attackers encrypt an organisation's data and demand payment to restore access' 2) 'Cryptojacking or hidden cryptomining is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency' 3) 'DDoS is one of the most critical threats to IT systems, targeting their availability by exhausting resources, causing decreases in performance, loss of data, and service outages'.

16 This locution indicates a situation in which communication and repetition inside a closed system amplifies and reinforces beliefs, with censorship of opposing views. Episodes of disinformation are often linked to such phenomenon.

Both ordinary and new types of attacks affect new technological environments.[17]

As far as geopolitical confrontation between states is concerned – with consequent repercussions also for the financial sector – cyber operations are often 'below-the-threshold', i.e. done with the intention of not provoking a response or counter-offensive by the attacked. In this case, in addition to the primary purpose of not triggering a reaction, threat actors often manage to dodge the discovery of such operations (in this regard, there is also a detection problem).[18] In a hybrid war context, they are preferred to openly hostile operations, due to lower costs and risks (Bilal, 2021). In some cases, *nation state* or *state-sponsored* attacks can be deliberately 'above-the-threshold', in consideration of the difficulty to prosecute and sanction at the international level, as well as because of the possibility of non-response by the victim and international community, which may not respond to avoid chain reaction effects. Internationally, however, debates about technical, political and legal nature on the very concept of threshold and its precise definition in cyberspace are ongoing (Schmitt, 2021).

In this scenario, to cope with cyber threats, states take actions for fostering their strategic autonomy, technological independence (and supremacy), as well as "cyber sovereignty". Measures adopted by states vary from country to country and include geopolitical, legal, economic, financial and technological matters, such as: a) public policy actions in multilateral *fora* on Internet governance and cyber operations b) national provisions on homeland security (including specific obligations for private companies to share information with intelligence units) c) "golden power" d) limitations on the use of file sharing platforms and social networks e) development of national *DNS* (domain name system) and servers, national Internet and clouds f) control of submarine and transoceanic cables g) autonomous production of components and technological infrastructures h) verification of supply chains and infrastructures through national assessment and certification centres i) technical standards on cyber issues j) defensive and offensive cyber operations; k) Internet censorship, website blocking, VPN blocking, *geoblocking* (geographic blocking, i.e. limiting access to the Internet content on the basis of users' geographical location) (Giannetto, 2019, 2021).

Due to the increasingly changing and complex threat landscape, governmental bodies – that are in charge of cybersecurity prevention and management – enhance adaptive and evolutionary models in accordance with a *zero trust*

---

17 For instance, consensus attacks are specific to DLT and blockchain environments (consensus being a set of validation rules that provide independent participants with the ability to verify the validity and integrity of transaction records on a ledger). Some examples are '51% attack' with control of most validators on *permission-Less* public networks or 'regulator exploitation attack' on *permissioned* private networks. Consensus mechanisms can lead to unauthorized transfers of digital assets, unauthorized censorship of operations, double spending or operational disruption of transaction validation. Attacks against algorithms that govern the consensus can act on various entry points such as networks, nodes, users and code.

18 Detection capabilities (i.e. ability to detect malicious activities) is a front to strengthen, from reconnaissance to exfiltration, according to the well-known matrix MITRE ATT&CK - (*https://attack.mitre.org*); see also *https://d3fend.mitre.org/*; *https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2665993/nsa-funds-development-release-of-d3fend/*).

approach, starting from the assumption that a threat actor can have already penetrated an organization's perimeter (NSA, 2021a, 2021b).[19]

It is therefore crucial to monitor such perimeter on a continuous basis and adopt strong *multi-factor authentication* (MFA) schemes (ENISA, 2022). Nonetheless, even if one puts in place cutting-edge technologies and far-reaching strategies, it is clear that systemic risk can never be eliminated (Baldoni, 2021b).

Since organizations and institutions strive to equip themselves with adequate cyber defence tools, which in any case cannot be at the level of a foreign state, they should work in close cooperation with national intelligence/law enforcement bodies. Such approach can prove to be extremely effective, since states are strengthening special joint forces dedicated to diversified activities in cyberspace.

3. Cyber resilience and the financial system

The term 'resilience', borrowed from materials science and psychology, is now widely used in various fields. In short, it indicates ability to react, adapt and evolve when known or unknown events of various kinds occur. In addition to this core concept, resilience represents also a capability to prevent such adverse events and, more generally, emergencies.

According to an ECB's definition, cyber resilience[20] has a direct correlation with cyber-attacks: 'Cyber resilience refers to the ability to protect electronic data and systems from cyberattacks, as well as to resume business operations quickly in case of a successful attack'.[21]

A similar definition is given by the Financial Stability Board (FSB)'s Cyber Lexicon: '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'.[22]

CYBER RESILIENCE

Cyber resilience is the ability of an organization to continue to carry out its business when adverse events (whether it is a cyber-attack or threats of another nature) occur, by adapting its behaviour (adaptive approach) and ensuring a rapid return to normal operating levels.

---

19 Data, people, devices, networks, infrastructures should never be considered safe; a check is always recommended. Threat is no longer just external (beyond internal threats, moles, malfunctions and human errors).

20 In Italy, the adjective 'cybernetic' has been in vogue for years; recently, the locution 'cyber-sicurezza' was introduced in the institutional context (this is an Anglo-Italian mix, to avoid the use of 'cybernetics', which actually indicates a different discipline). Likewise, in the Italian national context, one could use the neologism 'cyber-resilienza'.

21 ECB, 2018b.

22 See FSB, 2018. On this topic, see also WEF, 2018.

Complexity and nonlinear interconnections characterize the financial system. Consequently, small events and minimal cyber perturbations, even if only of a local nature, can cause large-scale repercussions at a systemic level, sometimes with chaotic dynamics (Visco, 2013).

The financial system is essentially made up of institutions, markets and (financial and technological) infrastructures; in a nutshell, it is composed of: a) lenders and borrowers of funds (e.g. households and businesses) b) financial intermediaries (e.g. banks, insurance companies, asset management businesses, securities firms, etc.) c) markets (monetary, financial, foreign exchange, etc.) d) infrastructures, platforms and payment systems e) products and services traded on markets f) supervisory and regulatory authorities (as for the Italian financial sector, e.g. the Bank of Italy, IVASS, CONSOB, COVIP, AGCM – see Bank of Italy, 2019).

Several physical and logical interconnections between various components in the financial system go far beyond national borders, extending to a global dimension and giving rise to a dense network of both operational and economic-financial interdependencies. Increasing digitalization amplifies these relationships. A large-scale cyber-attack against nodes in the financial system can therefore trigger a global systemic crisis (Zhang, 2020).[23] Information sharing is key[24] to promote a prompt and complete information exchange between different operators.

In order to set up effective defence, it is essential that financial entities – and in particular systemically relevant actors and main infrastructure operators – develop adequate knowledge about the attackers' ability to circumvent security and defence measures, also adopting proactive measures (Fazio and Zuffranieri, 2018).

The financial system has a time critical nature: transactions must end as quickly as possible, and in any case within a predetermined maximum time. On the one hand, this ensures that a financial transaction is completed (e.g. a payment order) and ultimately certainty and trust from operators; on the other hand, an intrinsic weakness derives from the speed with which an anomalous or fraudulent event can affect the entire system.

Figure 1 shows – for the European context – the close interconnection between different players in the financial system (the nodes' size indicates their weight as a function of different parameters; the nodes' distribution and colour indicate grouping by type of actor; the graph is updated on a continuous basis and is also used for dynamic monitoring purposes).

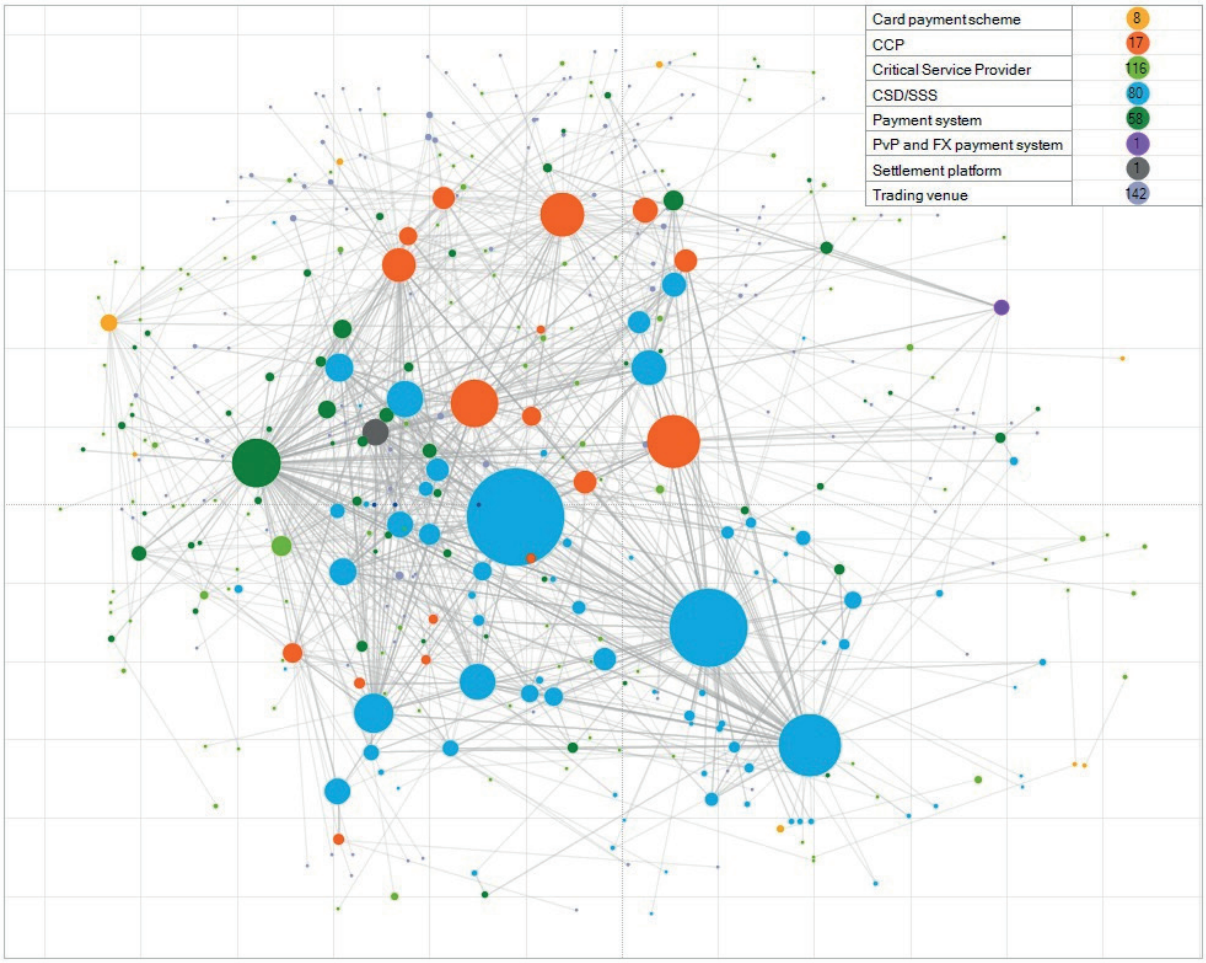
---

23 A further boost to the widespread digitization process was given by European and national plans aimed at promoting economic recovery and resilience following the Sars-Cov-2 pandemic emergency (European Council, 2020 and Signorini, 2021).

24 Information sharing, according to the FSB's Cyber Lexicon, is 'An exchange of data, information and/or knowledge that can be used to manage risks or respond to events'. In this work, therefore, reference is made to sharing of information at a general and institutional level, with particular regard to impacts; it is not here only intended as info sharing of technical and peer-to-peer information between CERTs, based on exchange of forensic evidence, indicators of compromise (IoCs), artefacts and vulnerabilities. As for information sharing at the institutional level, there are relevant cooperative and sector initiatives, such as CIISI-EU in the EU context and CERTFin in the Italian system (see below, in this work).

Figure 1 - MAIN INTERCONNECTIONS IN THE EUROPEAN FINANCIAL SYSTEM, 2021

GRAPH BASED ON REAL DATA (anonymized nodes and links)



Source: *Market Infrastructure and PAyments Committee* (MIPC) – *European Central Bank*.

Because of the strong and growing physical and logical interconnections between different systems and platforms, the financial sector has a very large potential attack surface. This is made up of a number of critical points of access, such as international credit institutions, market infrastructures for trading and settlement of financial instruments (e.g. central counterparties, clearing houses), systemically important payment systems (SIPS), global providers of technology and network services (e.g. SWIFT network).

A specific function to ensure business continuity[25] in the financial sector is the supervisory power on payment system. Such power goes together with

[25] Business continuity indicates the ability of institutions, organizations and providers of critical technological services in the financial system as a whole to deliver regularly products or services, even when adverse events occur. This concept includes also preliminary setting of instructions and procedures, which describe how organization's processes will be supported during and after a significant disruption. On the latter point, see: *https://csrc.nist.gov/glossary/term/business_continuity_plan*. About business continuity and operational resilience in the financial system, see also Bank of England, 2021.

the power of oversight over financial infrastructures and the power of banking and financial supervision. The Bank of Italy's power to supervise the payment system is based on Article 146 of the Testo Unico Bancario (TUB), whose paragraph 1 reads (translated): 'The Bank of Italy supervises the payment system, taking into account its regular functioning, its reliability and efficiency as well as the protection of payment service users'.

This legal provision must be read in conjunction with the rule contained in art. 127 paragraph 2 of the Treaty on the Functioning of the European Union (TFEU), where it is established that one of the fundamental tasks to be performed through the European System of Central Banks (ESCB) is 'to promote the smooth operation of payment systems'.

The Bank of Italy (BDI) performs these tasks over subjects who: issue, manage or lend payment instruments; manage exchange, clearing and settlement systems; manage technological infrastructures. BDI – together with CONSOB - also supervises securities settlement systems and infrastructures that facilitate trading in financial assets, such as the central depository Monte Titoli S.p.A. and the central counterparty Cassa di Compensazione e Garanzia S.p.A. (CCG or Euronext Clearing). The Bank of Italy supervises also over efficiency and orderly functioning of the wholesale market for government bonds (MTS). The Bank of Italy shares with CONSOB the powers of supervision and oversight over markets and infrastructures supporting negotiations.[26]

THE FINANCIAL SYSTEM

The financial system is made up of institutions, markets and infrastructures; in a nutshell, it is composed of: a) lenders and borrowers of funds (e.g. households and businesses); b) financial intermediaries (e.g. banks, insurance companies, asset management businesses, securities firms, etc.); c) markets (monetary, financial, foreign exchange, etc.); d) infrastructures, platforms and payment systems; e) products and services traded on markets; f) supervisory and regulatory authorities (e.g. for the Italian financial sector, the Bank of Italy, IVASS, CONSOB, COVIP, AGCM).

Supervisory and oversight activities within the payment system include those on national and European retail exchange and settlement systems (such as BI-Comp and STEP2-T), on wholesale systems (such as TARGET2 or the European private system Euro1) and, at the international level, on the settlement system for interbank multi-currency payments, the Continuous Linked Settlement (CLS). The oversight activity has also been extended to the more recent European instant payment settlement platforms (RT1 and Target Instant Payment Settlement, TIPS).

The Bank of Italy monitors also the proper functioning of the payment circuits used by end customers, such as those on which debit and credit cards and various forms of digital payment operate. Providers of instrumental

[26] According to a supervisory criterion by purpose, CONSOB is responsible for the transparency and protection of investors, the Bank of Italy for the stability and systemic risk containment.

technological or network services relevant to the payment system – which carry out activities on the national market or at the transnational level – are also subject to controls. Among the latter, for example, the SWIFT infrastructure – as well as the CLS system – is under a cooperative oversight regime by the G10 countries, including Italy.

The measures described hereafter in this work aim at fostering business continuity of infrastructures, financial institutions and providers of the critical technological services described above. Their operational resilience is essential for safeguarding stability in the financial system.

4. Institutional initiatives at the Italian level

The Bank of Italy has been launching over the years several activities to promote innovation and resilience in the Italian financial sector.[27] The actions taken, in the wake of the strategic lines agreed in the Eurosystem, have entailed continuous interaction with other national authorities in the financial sector (in particular, with CONSOB, IVASS and MEF) and with other government entities.

To achieve cyber resilience, the Bank of Italy has been promoting interventions aimed at favouring: – increase in resilience of each individual financial entity – effective transnational cooperation in the European financial area – prompt sharing of information in public and private sectors – enhancement of the ability to analyse and react to cyber events and other phenomena – definition of adequate public-private partnerships and intra-sectoral cooperation – suitable exchange of inter-sectorial know-how – development of an efficient regulatory context and awareness about cyber risks. Some of these measures are have already been adopted; some are under development and others are still evolutionary initiatives, given the necessary and continuous adaptation to an evolving and increasingly complex threat scenario.

Since the issue of the Prime Minister Decree of 17 February 2017 (the so-called Gentiloni Decree) and the National Plan for cyber protection and cybersecurity in March 2017,[28] the Bank of Italy – as supervisory Authority on payment systems and market – has gradually consolidated its activities in the field of cybersecurity and cyber resilience.

---

27 Ad hoc measures were envisaged in the BDI 2017-2019 Strategic Plan; in particular, the following action plans were made: 1.3 Promote innovation and resilience in the Italian financial sector – also by increasing the security and business continuity of the Italian financial sector through the implementation of a cyber resilience strategy for the infrastructures of the Italian market; 4.4 Strengthening the Bank's cybersecurity in relation to new risk scenarios – also through the establishment and development of the Computer Emergency Response Team, CERTBI.

28 The mentioned decree established, among other things, the Nucleo di Sicurezza Cibernetica (NSC); the Plan designed the national cyber architecture.

In recent years, BDI has overseen, with different levels of involvement, various initiatives and measures about cyber matters.

Back in 2017, the financial infrastructures sector had been included in the perimeter of Italy's (strategic) essential interests, for exercising special powers under the so-called *golden power*;[29] decree-law n. 23 of 8 April 2020 updated and integrated these measures.

As for protection of strategic assets and in connection with the *golden power* issue, the measures envisaged in the regulatory package on the National Cyber Security Perimeter (Law 133 of 2019, which converted Legislative Decree no. 105 of 2019) and subsequent related provisions (implementing decrees) are currently being implemented and tested.

The Legislative Decree 18 May 2018 n. 65 implemented the NIS 2016/1148 Directive (Network and Information Security Directive), which provides for a series of measures aimed at creating a common level of security of networks and information systems within the European Union. At the European level, work is still underway to balance national implementations of the NIS Directive – albeit with relatively wide margins of tolerance – in line with some principles outlined in the NIS 2 proposals.[30]

The creation of the European Competence Centre for industrial, technological and research development in the field of cybersecurity also had repercussions at the national level, due to the links with the network of National Coordination Centres (DIS, 2021a, 2021b).

At the national level, the Agenzia per la Cybersicurezza Nazionale (ACN)[31], dependent on the Italian Presidency of the Council of Ministers, plays a central role in the field of cyber resilience. ACN is in charge of cybersecurity and cyber resilience policies direction. The CSIRT Italy (Computer Security Incident Response Team) that was previously within DIS, also merged into the Agency.

As for Italian national cyber positioning documents, it is worthwhile to mention the 'Italian Position Paper on International Law and Cyberspace' and the 'Strategia Cloud Italia' both released in 2021.[32]

---

29 In particular, pursuant to the article 14 of the decree-law of 16 October 2017 n. 148 (converted by law no.172 of 4 December 2017, containing urgent provisions on financial matters and for non-deferrable needs) which inserted paragraph 1-ter in art. 2 of the decree-law of 15 March 2012 n. 21, containing discipline on golden power, converted, with modifications, by the law 11 May 2012 n. 56.

30 Other initiatives launched by the European Commission and with repercussions at the national level (including the proposal for a Directive on the resilience of critical entities of 16 December 2020 – see European Commission, 2020d and 2020e – and the regulatory package of September 2020 – see Commission European Union, 2020b and 2020c) will be addressed in the next chapter. After the publication of the present paper in Italian, the EU Commission launched on 16 March 2022 an EU public consultation on a forthcoming "European Cyber Resilience Act".

31 National Cybersecurity Agency, established with DECREE-LAW 14 June 2021 n. 82 and Law 109/2021.

32 These documents are available at the following links: *https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf; https://cloud.italia.it/strategia-cloud-pa/*.

A specific legal provision about business continuity and critical infrastructures was also adopted at the national level (Article 211 *bis* of Legislative Decree 05/19/2020, n. 34) as for the updating of security plans, with detailed measures to ensure a sound management of crises resulting from health emergencies.

With reference to specific initiatives in which the Bank of Italy is involved at the national level, it is worthwhile to mention the Committee for business continuity of the Italian financial sector (Codise), established in 2003 and chaired by the Bank of Italy. CONSOB, systemically significant financial sector operators (main banks, payment system operators and market infrastructures) and other Authorities participate in this initiative. Information sharing is one of the key points for crisis prevention and management.

Specifically, Codise deals with timely exchange of information and coordination of necessary measures in case of events that may jeopardize business continuity of critical financial operators and the regular functioning of essential financial services. The Committee, through a representative of the Bank of Italy, also participates in the Civil Protection Operational Committee and interacts with the Civil Defence Interministerial Technical Commission, coordinated by the Ministry of the Interior.

Codise also links up with CERTFin (Computer Emergency Response Team Financial Italian), a public-private cooperative initiative established in 2017 in collaboration with ABI (Italian Banking Association), in which operators from the national banking and financial sector participate on a voluntary basis.[33] This connection allows the activation of shared procedures on cyber and crisis events, reported by individual operators, the Bank of Italy or CERTFin. Codise carries out periodic exercises to verify the adequacy of procedures in the event of an emergency, through testing of internal systems for the management of business continuity.

In addition to the national dimension, the Committee is a point of contact with the ESCB in the event of a crisis at the European level. As for cyber matters, the Committee is active in organizing and carrying out exercises at the international level (e.g. G7), through 'table-top' discussion of possible emergency events (*discussion-based*) or with simulation of operations in likely scenarios (*operation-based*).[34] In this regard, the Cyber Incident Response Protocol (CIRP) is an agreement signed within the G7 forum: this agreement involves the G7 financial authorities as for management of cyber cross-border incidents in the financial sector. The Protocol provides for a series of procedures and interventions to be implemented in case of need; in this case, Codise constitutes the national entity for the coordination of operational crises at the G7 level.

---

[33] Payment service providers, banking and financial intermediaries, insurance companies, market infrastructure operators. Other Authorities and trade associations in the financial sector may also participate in the work of CERTFin, according to ad hoc agreements.

[34] cf. G-7 Fundamentals of cyber exercise programs – October 2020.

Finally, Codise carries out analysis and research (through events and publications) on business continuity and cyber resilience in the financial system.

The aforementioned CERTFin, whose Presidency is shared between the Bank of Italy and ABI,[35] aims to increase response capacity of financial operators to cyber threat and foster cyber resilience of the national financial system as a whole.

CERTFin carries out both operational and strategic activities: from prevention of cyber crises to response to cyber-attacks and security incidents.

In particular, CERTFin fulfils the following tasks: it serves as a single point of contact for reporting and management of cyber events in the financial sector; it promotes public-private and inter-sectoral cooperation; it favours exchange of information on cyber events; it launches awareness campaigns.

As far as inter-institutional collaboration on cybersecurity and cyber resilience is concerned, the Bank of Italy cooperates with MEF and CONSOB on several major projects. In recent years, the Bank of Italy has defined with CONSOB both a joint strategy for the supervision of national financial infrastructures (payment systems, markets and post-trading), and a strategy for cyber resilience in the financial system.[36]

The Bank of Italy has also adopted internally a 'Governance Framework for Cyber Resilience', with regard to resilience of systems that fall within its perimeter.

5. International and European initiatives: EU, G7, G20, FSB, BIS

One of the first steps in the development of international cyber resilience policies was the publication in 2016 of the 'Guidance on cyber resilience for financial market infrastructures'. This guidance was released by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO), in the context of the Bank for International Settlements (BIS).

Subsequently, following the adoption of a Eurosystem cyber resilience strategy within the Market Infrastructure and Payments Committee (MIPC), the European Central Bank (ECB) established in June 2017 the Euro Cyber Resilience Board

---

35 CERTFin's core unit is the Strategic Committee, which defines management and development guidelines. The Strategic Committee includes – in addition to the Bank of Italy and ABI – IVASS and ANIA for the insurance sector and CONSOB for the financial sector. Other units are the Operations Department and a Virtual Team that is mostly engaged in technical-tactical activities.

36 Focused in particular on some European regulatory initiatives (e.g. DORA, Digital Operational Resilience Act and NIS, Network and Information Security Directive) and on a joint action plan which regards, among other things, the adoption of supervision/testing tools and methodologies, such as CROE and TIBER-EU (on this point, see later in this work).

for pan-European Financial Infrastructures, a public-private cooperative forum in charge of defining and promoting a cyber resilience policy.

In 2018, the Financial Stability Board (FSB), set up by the G20 within the BIS, published the so-called Cyber Lexicon. In the same year, the NIST (US National Institute of Standards and Technology – see NIST, 2018) Framework version 1.1 and the Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU) of the ECB (see ECB, 2018a) were also released. The latter, borrowed from the original TIBER-NL, provides for testing schemes and procedures. Afterwards, a TIBER-EU Knowledge Centre (TKC) was established. To date, the TIBER-EU has been adopted by several countries in the European Union (about TIBER-EU and TIBER-IT see below).

In 2018, the ECB released another document about cyber resilience, the Cyber Resilience Oversight Expectations (CROE), which provides a methodology for assessing the degree of cyber resilience of financial entities; it is mainly aimed at payment system operators and market infrastructures. This tool was developed within the Eurosystem so that competent Authorities can carry out thematic assessments on the supervised subjects with regard to cyber risk management. Such methodology can also be used independently by financial entities, for self-assessment and interactions with counterparties of their ecosystem.

In February 2020, the Euro Cyber Resilience Board launched the Cyber Information and Intelligence Sharing Initiative (CIISI-EU), a cooperative initiative between public and private actors: financial infrastructures at the European level, central banks (including the Bank of Italy), critical service providers, ENISA and EUROPOL. It aims to build a trusted network for information exchange.

In September 2020, as part of the Digital Finance Strategy, the European Commission proposed, among other things, a Regulation dedicated to the issue of operational resilience (DORA – Digital Operational Resilience Act – see European Commission, 2020a). In December of the same year, the Commission published a document about a new Cybersecurity Strategy for the Digital Decade.

The EU Commission launched on 16 March 2022 an EU public consultation on a forthcoming "European Cyber Resilience Act" which seeks to establish common cybersecurity rules for digital products and associated services sold across the EU. The European Cyber Resilience Act will complement the existing relevant EU legislative framework (NIS, Cybersecurity Act, and the proposed NIS 2).

These initiatives aim to strengthen collective resilience in the European cyberspace and ensure a full and reliable use of digital services and tools by citizens and businesses. This objective is also pursued through other means, such as the harmonization of regulatory frameworks, the development of the single market for digital services and the strengthening of essential services operators' resilience.

On the G7 front, one of the most important action regarding the cooperation between financial institutions was the establishment in 2015 of a group of experts (CEG – G7 Cyber Expert Group), in charge of defining non-binding

high-level principles, aimed at fostering cyber resilience in the financial systems of the countries involved. The CEG is also engaged in the development of methodologies and protocols to facilitate coordination and communication between financial authorities and private operators.

In 2016, the G7 issued the 'G7 Fundamental Elements of Cybersecurity for the Financial Sector', a set of principles aimed at providing public and private sectors with a common reference framework for the development of cybersecurity strategies (G7, 2016).

In 2019, the G7 organized a Cybersecurity Exercise: 24 financial authorities of the G7 countries were involved in a simulated cross-border cyber-attack against the financial sector.

At the G20 level, following the declaration of the Heads of Government in July 2017, cybersecurity has become a priority in the agendas of various presidencies. Within the G-20 Finance Track, the Financial Stability Board (FSB) has been increasingly engaged on this issue; in 2020, it launched a package of guidelines for the effective response to cyber events (Cyber Incident Response and Recovery Toolkit, 2020). This cross-border harmonization effort continues with a line of work focused on reducing fragmentation in reporting cyber incidents. A recently published report offers an overview of existing regulatory reporting schemes at the G20 level and identifies some possible lines of intervention to encourage greater convergence at the international level.[37]

G20 and FSB groups and committees focus their work also on the enhancement of cyber capabilities and financial inclusion. The first topic is addressed primarily with a series of activities aimed at promoting safety of services; strengthening cyber capabilities of countries with less advanced endowments can prevent that single events affect the entire financial system. As to the latter, in this context, representatives and competent functions of the Bank of Italy promote financial awareness and education among people.[38] This activity is essential for building a resilient cyber context; awareness and knowledge about financial matters, together with consumer protection and digital infrastructure, are features that can help to build a resilient and inclusive financial ecosystem (Visco, 2021).

In the context of the Bank for International Settlements (BIS), two benchmarks are the Cyber Guidance for Financial market Infrastructures (2016) and the Wholesale Payment Security Strategy (2018), which have given impetus to a series of initiatives and documents at the international, European and national level. These measures, supported by other international committees, are intended to strengthen cyber resilience in the financial system; the Committee on Payments and Market Infrastructures (CPMI) defined them. In particular, the CPMI is committed to implement a strategy aimed for cyber resilience of market financial infrastructures and related ecosystems, with specific reference to wholesale payment systems. The most relevant initiatives in this area, in

37 FSB, 2021.

38 About financial education, see https://economiapertutti.bancaditalia.it.

addition to the aforementioned Cyber Guidance, in fact concern actions aimed at reducing risk of fraud in wholesale payment systems and raising cybersecurity in the financial system's end-points. Furthermore, BIS – also in collaboration with universities and other institutions – is engaged in the development of a database for conducting analysis and research on the quantification of cyber risks, both for losses attributable to cyber incidents, and for potential systemic impacts and financial stability.

6. *Threat Intelligence*, TIBER-EU and TIBER-IT

The FSB's Cyber Lexicon, in line with a definition from NIST, refers to threat intelligence as 'Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes'. Threat intelligence, here understood as both information gathering and threat analysis in general, can be considered as a subset of intelligence *tout court*.[39]

As for threat intelligence – and in particular for cyber threat prevention and detection capabilities – the TIBER-EU testing activities and its national versions (in the Italian context, the TIBER-IT, currently under development) are relevant initiatives.[40]

TIBER-EU, published by the ECB in 2018, is a European framework for ethical red teaming based on threat intelligence. It is essentially a set of guidelines, at the European level, on actors, processes and responsibilities involved in testing activities for cyber resilience of organizations in case of a cyber-attacks.[41]

TIBER-EU tests mimic tactics, techniques and procedures (TTPs) of threat actors in real life (states, individual hackers, cybercrime, hacktivists, cyber-terrorists etc.). Tests should be tailored-made for a specific organization and simulate an attack on critical functions, systems, people, and processes. They aim to reveal strengths and weaknesses of the tested entity – in terms of prevention, detection and response – allowing it to reach a higher level of cyber resilience at the end of the process.

---

39 In this regard, see Digregorio and Giannetto, 2019, page 14. The locution threat intelligence is sometimes considered equivalent to cyber threat intelligence; here, this stance is also taken into account.

40 ECB – TIBER-EU FRAMEWORK – How to implement the European framework for Threat Intelligence-based Ethical Red Teaming – May 2018. TIBER-EU was developed by the ECB and the EU national central banks; it was approved by the Governing Council of the ECB and published in May 2018.

41 TIBER-EU takes into account initiatives already launched in some countries such as United Kingdom (CBEST) and the Netherlands (TIBER-NL). TIBER-EU was initially included in a cyber resilience supervisory toolkit developed by the Eurosystem, implementing a supervisory strategy for the cyber resilience of payment systems and market infrastructures. The toolkit also included a cyber resilience survey (a sort of 'first diagnosis' tool, it was a multiple-choice questionnaire) and Cyber Resilience Supervision Expectations (CROE). This joint tool was made available to competent Authorities for carrying out thematic assessments on cyber risk management by the supervised entities. In Europe, the regulation on trading venues (MiFID2/MiFIR) and the Central Securities Depository Regulation (CSDR) also contain provisions on cyber operational risk. A regulatory strategy (approved by the Governing Council of the ECB) on Systemically Important Payment Systems (SIPS) was then defined within the Eurosystem.

Actors involved in a TIBER-EU test operate in different teams, according to their role and responsibilities:

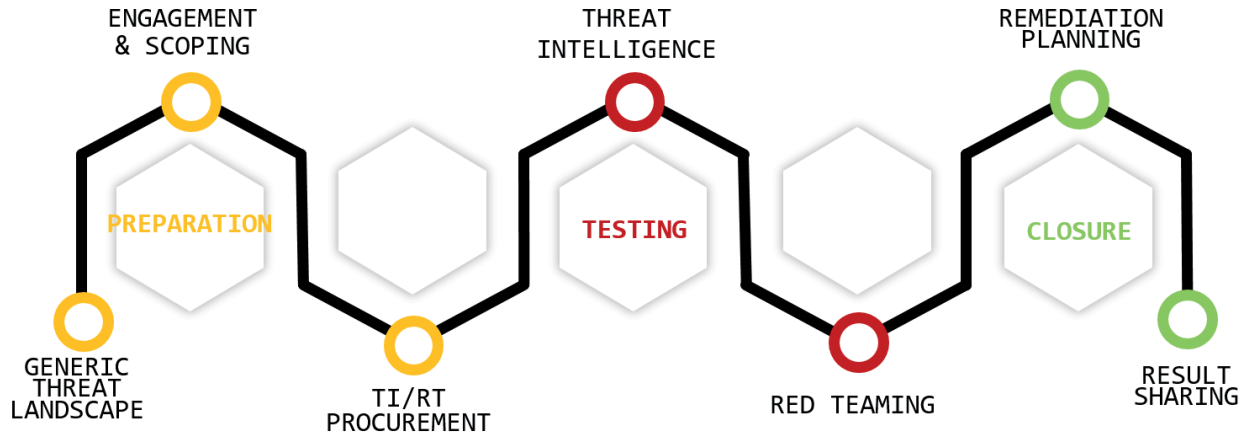
- blue team (BT): people of the tested organization in charge of defending against cyber-attacks; they are not aware of the test;
- threat intelligence provider (TI): company that examines the range of possible threats and supports the organization in the information gathering and analysis phase;
- red team (RT): company that carries out the simulated attack trying to disrupt critical functions of the entity, imitating tactics, techniques and procedures of a real threat actor;
- white team (WT): team within the target organization that is responsible for the entire testing process; it is aware of the test; it guides and manages the test in collaboration with the TIBER cyber team;
- TIBER cyber team (TCT): team within the Authority that facilitates interaction between the different actors involved in the test; it supervises the fulfilment of the test and ensures compliance with the requirements of the TIBER framework.

In addition to these teams, TIBER-EU envisages the so-called purple team (PT) – formed by members of the BT and RT – for maximizing the test's benefits, through a deeper and more structured cooperation between attackers and defenders.[42]

The TIBER-EU framework aims to harmonize and standardize the approach to ethical red teaming based on threat intelligence across the EU. To achieve this, the various national TIBER frameworks should follow the guidelines provided for in the TIBER-EU.

A TIBER-EU end-to-end test include three main phases: preparation, testing and closure. A synopsis of the TIBER-EU (and TIBER-IT) testing process is shown in Figure 2.

Figure 2 - STAGES OF THE TIBER-EU AND TIBER-IT PROCESS



[42] Normally a purple team intervenes at the end of the offensive phase to strengthen results and lessons learned. It can also be activated during the attack phase if the BT identifies the actions of the RT as a security test. At the European level, the development of evolutionary methodologies and best practices – in the field of threat intelligence testing and purple teaming advanced practices – is still ongoing.

Upstream of the test, there may be a threat scenario-profiling phase (with a Generic Threat Landscape – GTL). Within the process, one can distinguish different stages: scoping (definition of objectives and scope), procurement (engagement/procurement of IT and RT teams), threat intelligence (information gathering and analysis), red teaming (simulated attack activity), remediation (technical remedies) and result sharing (distribution and discussion on results). Tests conclude with a summary report and a certification.

The TIBER-EU framework is designed for national Authorities and entities that are IMFs (financial market infrastructures), including those whose cross-border activities fall within the regulatory power of different Authorities. It is applicable to both financial sector entities and organizations in other critical sectors.

In addition to a number of mandatory requirements, the framework also includes options that can be adapted to specificities of different jurisdictions. This facilitates mutual recognition and reduces burden on both the Authorities and entities being tested.

The TIBER-EU procurement guidelines provide details on how to select red-teaming providers and acquire threat intelligence services.[43] The TIBER-EU White Team Guidance explains how to set up the team managing the TIBER test within the target entity.

In January 2020, the Bank of Italy and CONSOB adopted a joint action plan for cyber resilience of the Italian financial sector, which envisages, among other things, the development of the TIBER-IT testing framework, in line with the cyber resilience strategy of the Eurosystem and in collaboration with other authorities and national stakeholders in the financial sector (e.g. CERTFin).

TIBER-IT is under development: it could take into account national peculiarities, both from a financial and legal point of view, as well as institutional synergies with other Authorities, in order to offer a harmonized and coordinated tool for operators in the national financial system.

As already positively experienced in other countries, TIBER-IT could be applied to all financial entities, being able to act also as a reference methodology for subsequent developments (also in terms of regulation and supervision).

In line with best practices adopted in other jurisdictions, the development of TIBER-IT could be oriented towards the following principles: participation of financial operators on a voluntary basis, application to critical operators in the Italian financial system and progressive implementation.

[43] To ensure that threat intelligence and red-teaming services implement appropriate standards in conducting a TIBER-EU test, organizations being tested must perform due diligence, ensuring that the selected supplier meets all requirements in the procurement guidelines of the TIBER-UE. In the future, organizations should only use services of suppliers who have obtained a formal TIBER-EU certification and accreditation. There is currently no dedicated certification and accreditation agency in Europe for this purpose.

7. CYBER RESILIENCE IN THE FINANCIAL SYSTEM: EVOLUTIONARY ASPECTS

In recent years, some trends have emerged internationally about evolutionary aspects in cyber resilience strategies, for example: capacity building for organizations and states, specialization of people employed in cybersecurity, well-balanced regulatory environment for cyberspace, advancement in analysis skills and inter-institutional cooperation.

The development of multidisciplinary skills in cyber matters is a key feature for resilience in the financial system (Maurer and Nelson, 2020). Technical-IT knowledge alone cannot help in framing results of technical investigations in a context of multiple concomitant phenomena and identifying plausible motivations and threat actors; complementary skills are needed. Developing units made up of people with varied skills is one of the measures that can help in defining and implementing sound cyber resilience policies.

ANALYSIS AND SYSTEMIC RESILIENCE

Analysis on threats and other phenomena (geopolitics, finance, economy, technology, intelligence) plays a central role in fostering cyber resilience for business continuity in the financial system. Analysis activities must be preceded and accompanied by continuous information gathering and monitoring, from a system and scenario perspective.

Regulatory oversight is another key point for the development and implementation of cyber resilience policies, at the national, European and international level. The main goal is promoting a balanced (between public and private) regulatory environment for cyberspace. In addition, it is important to favour a regulatory level playing field, as well as proportionality of interventions.

Developing brand-new and cutting-edge analysis activities is another evolutionary issue. Cyber resilience for business continuity in the financial system requires a relentless work of information gathering, monitoring and analysis on cyber events, threats and manifold phenomena (geopolitics, finance, economics, technology, intelligence). Therefore, threat intelligence alone, which essentially deals with threats, is not enough. Conversely, one ought to implement systemic scenario analysis (SSA) (Giannetto, 2020, 2021), to synoptically and simultaneously scrutinize a gamut of multiple and interconnected phenomena.

Finally yet importantly, interaction between financial institutions and intelligence/law enforcement bodies is crucial for developing cyber resilience policies. Strengthening this cooperation may prove to be particularly fruitful in the future, especially for joint and cooperative discussion on strategic cybersecurity issues.

Conclusions

This work explores institutional initiatives launched at national and international level to strengthen cyber resilience and promote business continuity in the financial system. It presents measures adopted by the Bank of Italy – some already implemented, others under development according to the strategic lines drawn up by the Institute and the Eurosystem – as well as a wide range of initiatives taken by various international organizations. This research shows the need to constantly adapt and develop actions designed to foster cyber resilience at national and international level, in order to face an evolving and increasingly complex context.

References

Baldoni, R. (2021a), Direttore ACN, Keynote speech, Conference *"Dalla sicurezza aziendale alla sicurezza collettiva"*, Roma, 15 October 2021.

Baldoni, R. (2021b), Direttore ACN, Keynote speech, *"36° Convegno Giovani Imprenditori di Confindustria"*, Napoli, 23 October 2021.

Banca d'Italia (2019), *La Banca d'Italia. Funzioni e obiettivi,* December 2019.

Banca d'Italia (2022), *Canale Fintech*, website.

Bank of England (2021), *CBEST Threat Intelligence-Led Assessments*, January 2021.

Basel Committee on Banking Supervision (2020a), *Principles for Operational Resilience*, BIS, March 2021.

Basel Committee on Banking Supervision (2020b), *Consultative Document Principles for operational resilience*, BIS, August 2020.

Bilal, A. (2021), *Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote*, NATO Review, 20 November 2021.

Bodeau, J.D., C.D. Mccollum, D.B. Fox (2018), *Cyber Threat Modeling: Survey, Assessment and Representative Framework*, MITRE, November 2018.

Ciocca, P. (2020), Commissario CONSOB, Keynote speech, "*Dati e finanza: nuove opportunità e nuove vulnerabilità. La necessità di cambiare paradigma"*, Roma, 18 November 2020.

Coats, D.R. (2019), *Worldwide Threat Assessment of the US Intelligence Community*, 29 January 2019.

Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions (2016), *Guidance on cyber resilience for financial market infrastructures*, BIS, June 2016.

Digregorio, P. e Giannetto B. (2019), *Development of a cyber threat intelligence apparatus in a central bank,* Banca d'Italia, QEF 517, 11 October 2019.

Dipartimento delle informazioni per la sicurezza (2021a, 2021b), *Relazione sulla politica dell'informazione per la sicurezza 2020 e 2021*, 1 March 2021; 28 February 2022.

Dipartimento per la trasformazione digitale, Agenzia per la cybersicurezza nazionale (2021), *Strategia Cloud Italia*, September 2021.

European Central Bank (2018a), *How to implement the European framework for Threat Intelligence-based Ethical Red Teaming*, TIBER-EU Framework, May 2018.

European Central Bank (2018b), *Cyber resilience oversight expectations for financial market infrastructures*; December 2018.

EU Commission – EU public consultation on a forthcoming "European Cyber Resilience Act" – 16 March 2022.

European Commission (2020a), *Consultation Document – Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure*, 24 September 2020.

European Commission (2020b), *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341*, Brussels, 24 September 2020.

European Commission (2020c), *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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) No 909/2014*, Brussels, 24 September 2020.

European Commission (2020d), *Joint Communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade*, Brussels, 16 December 2020.

European Commission (2020e), *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities, Brussels*, 16 December 2020.

European Council (2020), *Next Generation EU*, Brussels, 21 July 2020.

European Union Agency for Cybersecurity (2020a), *ENISA Threat Landscape – Emerging Trends*, 20 October 2020.

European Union Agency for Cybersecurity (2020b), *Artificial Intelligence Cybersecurity Challenges*, 15 December 2020.

European Union Agency for Cybersecurity (2021a), *EU Cybersecurity Initiatives in the Finance Sector*, 5 March 2021.

European Union Agency for Cybersecurity (2021b), *ENISA Threat Landscape 2021*, 27 October 2021.

European Union Agency for Cybersecurity, CERT-EU (2022), *Joint Publication – Boosting your Organisation's Cyber Resilience,* 14 February 2022.

Europol (2020), *Internet Organized Crime Threat Assessment (IOCTA) 2020*, 5 October 2020.

Europol (2021), *Internet Organised Crime Threat Assessment (IOCTA) 2021*, 11 November 2021.

Fazio, A. e F. Zuffranieri (2018), *Interbank payment system architecture from a cyber security perspective,* Banca d'Italia, QEF 418, 29 January 2018.

Financial Stability Board (2018), *Cyber Lexicon*, 12 November 2018.

Financial Stability Board (2021), *Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence*, October 2021.

Gazzetta Ufficiale (2021), *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale,* DECRETO-LEGGE 14 giugno 2021, n. 82, convertito in Legge 109/2021.

Giannetto, B. (2019), *Cyber Governance & Cyber Threat Intelligence*, Security Summit, 5 June 2019.

Giannetto, B. (2020), *All-Source Intelligence: Reshaping an Old Tool for Future Challenges*, Security Affairs, 18 December 2020.

Giannetto, B. e Paganini P. (2020), *Mastering Communication in Cyber Intelligence Activities: A Concise User Guide*, Cyber Defense Magazine, 21 April 2020.

Giannetto, B. (2021), *Innovazione Tecnologica e Cybersecurity nel Sistema Finanziario*, Cyber Security Virtual Conference, 26 May 2021.

G7 (2016), *G7 fundamental elements of cybersecurity for the financial sector*, 11 October 2016.

Maurer, T. e A. Nelson (2020), *International Strategy to Better Protect the Financial System against Cyber Threats*, CARNEGIE, 18 November 2020.

Maurer, T. e A. Nelson (2021), *The Global Cyber Threat*, IMF, March 2021.

Ministero degli Affari Esteri, Presidenza del Consiglio dei Ministri, Ministero della Difesa, *Italian Position Paper on International Law and Cyberspace*, 4 November 2021.

MITRE, *ATT&CK Matrix for Enterprise, D3FEND*.

National Institute of Standards and Technology (2018), *Cybersecurity Framework*, Version 1.1, 16 April 2018.

National Security Agency (2021a), *Embracing a Zero Trust Security Model*, February 2021.

National Security Agency (2021b), *NSA Funds Development, Release of D3FEND*, 22 June 2021.

Perrazzelli, A. (2021), Vice Direttrice Generale della Banca d'Italia, *"Le iniziative regolamentari per il Fintech: a che punto siamo?"*, Università degli Studi dell'Insubria, Laboratorio di Finanza Digitale, 4 May 2021.

Schmitt, M.N. (2021), *Terminological Precision and International Cyber Law*, Articles of War, 29 July 2021.

Signorini, L.F. (2021), Direttore Generale della Banca d'Italia, *Economic Outlook, Public Finances and the Next Generation EU*, Banca d'Italia, 10 March 2021.

Sørensen, H. e D.B. Nyemann (2018), *Going beyond resilience – A revitalized approach to countering hybrid threats*, Hybrid CoE Strategic Analysis 13, November 2018.

Treverton, G.F., A. Thvedt, A.R. Chen, K.Lee e M. McCue (2018), *Addressing hybrid threats*, SDU, CATS, Hybrid CoE, 2018.

Visco, I. (2013), Governatore della Banca d'Italia, *Economia e finanza dopo la crisi,* Accademia Nazionale dei Lincei, Conferenza a Classi Riunite, 8 March 2013.

Visco, I. (2021), Governatore della Banca d'Italia, *Considerazioni finali del Governatore, Relazione annuale*, Banca d'Italia, Roma, 31 May 2021.

World Economic Forum (2018), *Cyber Resilience Playbook for Public-Private Collaboration*, January 2018.

World Economic Forum (2020), *Systems of Cyber Resilience: Secure and Trusted FinTech*, July 2020.

World Economic Forum (2021), *The Global Risks Report*, January 2021.

World Economic Forum (2022), *The Global Risks Report*, January 2022.

Zhang, T. (2020), *Building Cyber Resilience*, (Virtual) IMF Cybersecurity Workshop, 9 December 2020.

Papers published in the 'Markets, Infrastructures, Payment Systems' series

n. 1 TIPS - TARGET Instant Payment Settlement – The Pan-European Infrastructure for the Settlement of Instant Paymentsi, *by Massimiliano Renzetti, Serena Bernardini, Giuseppe Marino, Luca Mibelli, Laura Ricciardi and Giovanni M. Sabelli* (Institutional Issues)

n. 2 Real-Time Gross Settlement systems: breaking the wall of scalability and high availability, *by Mauro Arcese, Domenico Di Giulio and Vitangelo Lasorella* (Research Papers)

n. 3 Green Bonds: the Sovereign Issuers' Perspective, *by Raffaele Doronzo, Vittorio Siracusa and Stefano Antonelli* (Research Papers)

n. 4 T2S - TARGET2-Securities – The pan-European platform for the settlement of securities in central bank money, *by Cristina Mastropasqua, Alessandro Intonti, Michael Jennings, Clara Mandolini, Massimo Maniero, Stefano Vespucci and Diego Toma* (Institutional Issues)

n. 5 The carbon footprint of the Target Instant Payment Settlement (TIPS) system: a comparative analysis with Bitcoin and other infrastructures, *by Pietro Tiberi* (Research Papers)

n. 6 Proposal for a common categorisation of IT incidents, *by Autorité de Contrôle Prudentiel et de Résolution, Banca d'Italia, Commissione Nazionale per le Società e la Borsa, Deutsche Bundesbank, European Central Bank, Federal Reserve Board, Financial Conduct Authority, Ministero dell'Economia e delle Finanze, Prudential Regulation Authority, U.S. Treasury* (Institutional Issues)

n. 7 Inside the black box: tools for understanding cash circulation, *by Luca Baldo, Elisa Bonifacio, Marco Brandi, Michelina Lo Russo, Gianluca Maddaloni, Andrea Nobili, Giorgia Rocco, Gabriele Sene and Massimo Valentini* (Research Papers)

n. 8 The impact of the pandemic on the use of payment instruments in Italy, *by Guerino Ardizzi, Alessandro Gambini, Andrea Nobili, Emanuele Pimpini and Giorgia Rocco* (Research Papers) (in Italian)

n. 9 TARGET2 – The European system for large-value payments settlement, *by Paolo Bramini, Matteo Coletti, Francesco Di Stasio, Pierfrancesco Molina, Vittorio Schina and Massimo Valentini* (Institutional Issues) (in Italian)

n. 10 A digital euro: a contribution to the discussion on technical design choices, *by Emanuele Urbinati, Alessia Belsito, Daniele Cani, Angela Caporrini, Marco Capotosto, Simone Folino, Giuseppe Galano, Giancarlo Goretti, Gabriele Marcelli, Pietro Tiberi and Alessia Vita* (Institutional Issues)

n. 11 From SMP to PEPP: a further look at the risk endogeneity of the Central Bank, *by Marco Fruzzetti, Giulio Gariano, Gerardo Palazzo and Antonio Scalia* (Research Papers)

n. 12 TLTROs and collateral availability in Italy, *by Annino Agnes, Paola Antilici and Gianluca Mosconi* (Research Papers) (in Italian)

n. 13 Overview of central banks' in-house credit assessment systems in the euro area, *by Laura Auria, Markus Bingmer, Carlos Mateo Caicedo Graciano, Clémence Charavel, Sergio Gavilá, Alessandra Iannamorelli, Aviram Levy, Alfredo Maldonado, Florian Resch, Anna Maria Rossi and Stephan Sauer* (Institutional Issues)

n. 14 The strategic allocation and sustainability of central banks' investment, *by Davide Di Zio, Marco Fanari, Simone Letta, Tommaso Perez and Giovanni Secondin* (Research Papers) (in Italian)

n. 15 Climate and environmental risks: measuring the exposure of investments, *by Ivan Faiella, Enrico Bernardini, Johnny Di Giampaolo, Marco Fruzzetti, Simone Letta, Raffaele Loffredo and Davide Nasti* (Research Papers)

n. 16 Cross-Currency Settlement of Instant Payments in a Multi-Currency Clearing and Settlement Mechanism, *by Massimiliano Renzetti, Fabrizio Dinacci and Ann Börestam* (Research Papers)

n. 17 What's ahead for euro money market benchmarks?, *by Daniela Della Gatta* (Institutional Issues) (in Italian)