1. The Bank's role in oversight and prudential supervision of financial market infrastructures, custodians, payment service providers and critical service providers

To give more insight into the systems and institutions providing payment, clearing, settlement, custody and other services, either from a wholesale or a retail market perspective, section 1.1 presents an overview of their structure and mutual interdependencies. Relevant processes and flows are explained in more detail in the subsequent parts of this report (i.e. chapters 2, 3 and 4). Section 1.2 explains the Bank's mandate and its role in the oversight and prudential supervision of this sector, from either a national or an international perspective.

1.1 Critical links in the functioning of financial markets and payment services

The systems and institutions covered in this report can be divided into three categories according to the type of service provided: (i) securities clearing, settlement and custody, (ii) payments, and (iii) other financial infrastructure service providers. Through their activities or services for the financial industry, these systems and institutions are the critical links in the functioning of financial markets and payment services, and in the real economy. If designed safely and managed properly, they are instrumental in reducing systemic risks and contagion in the event of financial crises. At the same time, they are interlinked with other financial market infrastructures (FMIs), financial intermediaries and other actors such as merchants or retail customers. These interdependencies are briefly presented and illustrated in chart 1.

Securities clearing, settlement and custody

A trade in a financial instrument is concluded between a buyer and a seller by agreeing the price and the contract terms. Trading in such instruments can take place on-exchange (i.e. on a centralised platform designed to optimise the price discovery process and to concentrate market liquidity) or bilaterally on an over-the-counter (OTC) basis (i.e. where the counterparties make the bid and accept the offer to conclude contracts directly among themselves). The final investor uses a custodian bank, which may rely on other intermediaries (e.g. brokers) to conduct trades. Trade exchanges such as Euronext Brussels are supervised by securities regulators and are not covered in this report.

FMIs and financial institutions that provide securities clearing, settlement and custody services are part of the post-trade securities landscape. The clearing of a trade via a central counterparty (CCP) generally means that the CCP becomes the buyer counterparty for the seller and the seller counterparty for the buyer. Both original counterparties to the trade then have a claim on the CCP. The CCP's direct participants – usually banks or

investment firms – are called clearing members. A clearing member may clear not only its own trades via the CCP, but also those of its clients. There are no CCPs established in Belgium, but CCPs in other countries are important for Belgium due to their clearing activities for the Belgian securities market.

After clearing, the settlement of a trade results in the transfer of cash and/or a financial instrument between the parties in the books of a central securities depository (CSD). When a CCP has intervened to clear a trade, settlement takes place on the books of the CSDs between the buyer and the CCP, and between the seller and the CCP. There are three CSDs established in Belgium: Euroclear Bank (an international CSD or ICSD), Euroclear Belgium and NBB-SSS (both CSDs). The settlement of the cash leg of securities transactions takes place either in payment systems operated by central banks (i.e. central bank money, for example T2[1]) or on the books of an (I)CSD with banking status providing (multicurrency) cash accounts (i.e. commercial bank money, for example Euroclear Bank).

Financial institutions that facilitate their clients' access to securities investment markets are referred to as custodians. In that intermediary capacity, custodians can offer their clients safekeeping and settlement services. A local custodian primarily focuses on serving a single securities market. If a custodian has access to markets worldwide, it is considered a global custodian.

Payments

The payments landscape covers both wholesale payments (i.e. transactions between banks for institutional investors) and retail payments (i.e. transactions between retail customers), and includes payment systems, payment service providers (PSPs) such as payment institutions (PIs) and electronic money institutions (ELMIs), processors for retail payment instruments and card payment schemes.

Payment systems encompass large-value payment systems (LVPS) and retail payment systems (RPS). While LVPSs generally exchange payments of very large amounts, mainly between banks and other participants in the financial markets, RPSs typically handle a large volume of payments of relatively low value by means of credit transfers and direct debits. In Belgium, most interbank payments are processed by T2, the LVPS connecting Belgian banks with other European banks, and by the Centre for Exchange and Clearing (CEC), which is the domestic retail payment system processing intra-Belgian domestic payments.

The role of PIs and ELMIs in the retail payments area is multi-faceted and growing. PIs and ELMIs have long been active in the card payment business, issuing payment cards to users and/or acquiring the funds for payments on behalf of merchants. The revised Payment Services Directive (PSD2) has further strengthened the role of non-banks in the market since they are now allowed (under certain conditions) to make use of the banking industry's accounting ledger for accessing and consulting payment service users' accounts online.

Card payments remain the most widely used payment instrument in Belgium and typically involve a "four-party scheme", i.e. cardholder, card issuer, merchant and acquirer. In a transaction with a merchant, the card of the purchaser (cardholder) is issued by an institution (card issuer) which was traditionally always a bank but can also be a PI or ELMI. The acquirer is in charge of acquiring the transaction on behalf of the merchant (i.e. performing for the merchant all the steps necessary for the buyer's money to be paid into the merchant's account). The relevant rules and features according to which card payments – either debit or credit – can take place are defined by card payment schemes. The Belgian domestic (debit) card payment scheme is Bancontact. Mastercard Europe (MCE) is the European subsidiary of the Mastercard group, which owns the international (credit) card payment scheme and is established in Belgium.

1 As of 20 March 2023, the new payments system T2 went live and replaced TARGET2. For more detailed information, see https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230321~f5c7bddf6d.en.html.

As from May 2020, the Eurosystem designated MCE as a systemically important payment system (SIPS) according to the ECB SIPS Regulation criteria. The Mastercard Clearing Management System operated by MCE has become the fifth SIPS in the euro area, alongside T2, EURO1, STEP2 and CORE-FR. For the first time, an entity active in the card business has been designated as a SIPS; its business activities stem exclusively from card-based transactions under the debit and credit card schemes managed by MCE.

For Bancontact, a scheme switch is in place, but one processor provides the underlying network and services for the majority of card payments, namely equensWorldline SE. For Maestro, the processing network is provided directly by Mastercard. After the processing of card payments, transactions are sent to the CEC for clearing and settlement. PIs also play a major role in providing money transfer/remittance services (fund transfers), allowing retail customers to transfer funds from Belgium to a third party in different locations around the world, and vice versa.

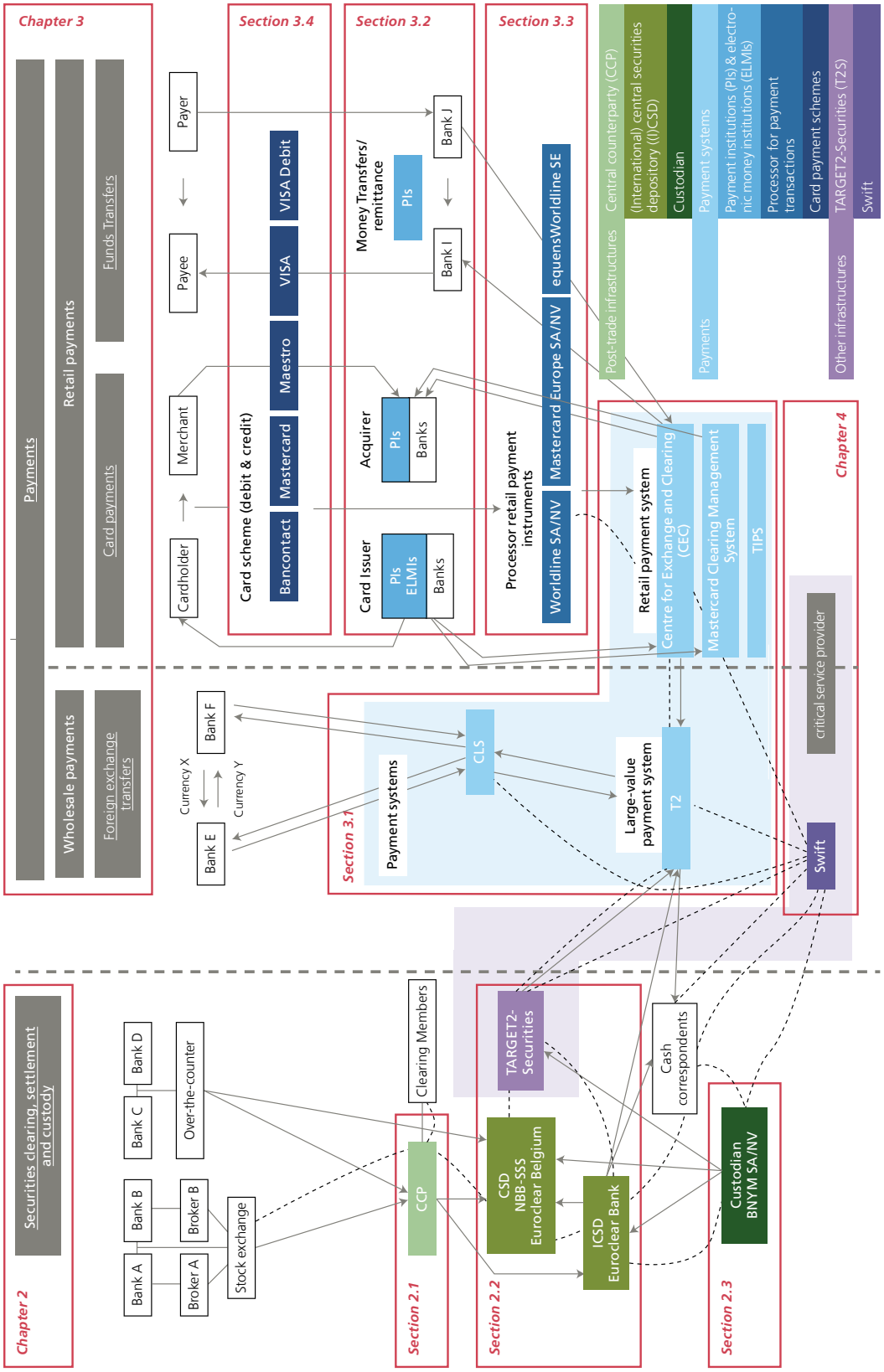
CLS, a settlement system for foreign exchange (FX) transactions is linked to the LVPS systems operated by central banks of 18 currencies (including T2 for EUR), making it possible to settle both legs of the FX transaction at the same time. CLS eliminates FX settlement risk when – due to time zone differences – one party transfers the currency it sold but does not receive the currency it bought from its counterparty.

Other infrastructures and service providers

TARGET2-Securities (T2S) is the common settlement platform for European CSDs. Although messaging service provider Swift is neither a payment system nor a settlement system, a large number of systemically important systems depend on it for their daily financial messaging. It is therefore considered as a critical service provider.

Chart 1

Interlinkages through and between financial market infrastructures, custodians, payment service providers and critical service providers relevant for Belgium



1.2 FMIs, custodians, payment service providers and critical service providers subject to oversight and prudential supervision by the Bank

The Bank has responsibilities in both oversight and prudential supervision of FMIs, custodians, PSPs, such as PIs and ELMIs and critical service providers.

Oversight and prudential supervision of FMIs differ in a number of areas, ranging from the object of the function, the authority responsible, the topics covered, and the regulatory framework and tools used. However, both oversight and prudential supervision activities, and the framework they rely on, evolve over time.

Central banks have always had a close interest in the safety and efficiency of payment, clearing and settlement systems. One of the principal functions of central banks is to be the guardian of public confidence in money, and this confidence depends crucially on the ability of economic agents to transmit money and financial instruments smoothly and securely through payment, clearing and settlement systems. These systems must therefore be strong and reliable, available even when the markets around them are in crisis, and must never themselves be the source of such crisis. The central bank's oversight of FMIs pursues these objectives by monitoring systems, assessing them and, where necessary, inducing change. It is generally recognised as a core responsibility of central banks.

The Bank's oversight of payment, clearing and settlement infrastructures is based on Article 8 of its Organic Law[1] and focuses on systems established in or relevant for Belgium. Although Swift is not a payment, clearing or settlement infrastructure, many such systems use it, effectively making it a critical service provider of systemic importance. Swift is therefore subject to a (cooperative) central bank oversight arrangement, in which the Bank has the role of lead overseer.

The Bank is also the prudential supervisory authority for individual financial institutions, as well as custodians and Payments Service Providers. While significant credit institutions, such as The Bank of New York Mellon SA/NV (BNYM SA/NV), are directly supervised by the single supervisory mechanism (SSM), less significant institutions remain under the prudential supervision of the Bank as the national competent authority.

Some FMIs are subject to both oversight and prudential bank supervision, typically if the FMI operator has bank status (as is the case for Euroclear Bank). Worldline SA/NV is also subject to both prudential supervision (as a payment institution) and oversight (as a retail payment instruments processor). In such situations, the oversight activity and prudential supervision complement one another: while the oversight activity focuses on the sound functioning of the settlement system (by assessing compliance with oversight standards such as the CPMI-IOSCO Principles for FMIs (PFMIs)), the prudential supervision focuses on the financial soundness of the operator (by assessing compliance with prudential regulations). As a result, oversight and prudential supervision typically cover different topics or different perspectives. Typical areas on which oversight focuses concern the functioning of the system and how its organisation and operation minimises or avoids risks not only for itself but – just as importantly – for its participants. Examples include settlement finality rules reducing risks associated with a participant's insolvency (which prevent automatic unwinding of other participants' previous transactions with a bankrupt participant), delivery-versus-payment (DVP) or payment- versus-payment (PVP) mechanisms eliminating principal risks in transactions between participants, fair and open access for participants, and stringent requirements on business continuity plans ensuring continuity of services for participants. Oversight also takes into account risks related to system interdependencies (either via connected systems or participants) that could trigger contagion risks in financial markets. Prudential supervision seeks to ensure that institutions are financially robust at micro-prudential level, thus helping to maintain the trust of the institution's counterparties and thereby

1 Article 8, Law of 22 February 1998 establishing the Organic Statute of the National Bank of Belgium, Belgian Official Gazette 28 March 1998, 9.377.

promoting financial stability. Some types of risks are monitored by both FMI overseers and bank supervisors. However, their perspective is different, as an FMI's business model is based on transferring liquidity (which has an element of time criticality) between – or on behalf of – its participants, whereas a bank's business model tends to be based on maturity transformation (short-term deposits, long-term assets). The regulatory approach for credit, liquidity and operational risk for FMIs therefore differs from that for banks.

As a consequence of such divergences in scope, oversight and prudential supervision rely on different frameworks. For oversight, the PFMIs cover payment systems, securities settlement systems, CSDs, CCPs and trade repositories, as well as critical service providers (Annex F of the PFMI report). For the implementation of these principles, further clarity is provided by relevant guidelines, such as the CPMI-IOSCO guidance on cyber resilience for FMIs or the guidance on resilience and recovery of CCPs. In addition, the CPMI has also published an analytical framework for distributed ledger technology in payment, clearing and settlement.

The tools to conduct oversight and prudential supervision may differ too. Oversight is generally based on principles and guidelines designed in international fora (Eurosystem, CPMI, CPMI-IOSCO). The traditional approach for enforcing them was to urge FMIs and other (critical) service providers to adhere to them via central bank moral suasion (so-called "soft law" approach). Prudential supervision, on the other hand, has laid down its requirements in a formal legal framework enacted through EU Directives, Regulations and local laws ("hard law" approach). However, central bank oversight has become more formal, owing to the expanding role of the private sector in providing payment and settlement systems, as well as the growing criticality of these systems' proper functioning. In a growing number of cases, oversight is evolving into a hard law approach as illustrated, for example, by the fact that the European Central Bank (ECB) has laid down its expectations in the ECB Regulation on oversight requirements for systemically important payment systems (SIPSR), or by the 2017 Belgian Law on systemically relevant processors for retail payment instruments. Also, the EU transposed the oversight framework for CCPs and CSDs (i.e. PFMIs) through Regulations in 2012 and 2014 (EMIR[1], CSDR[2]). The Bank has been assigned as the competent supervisory authority for Belgian (I)CSDs, and, as overseer, is also considered as the relevant authority under CSDR[3].

In order to pool expertise, reinforce synergies and align approaches between the oversight function and that of prudential supervision of FMIs, custodians, PSPs and other (critical) service providers, these two functions have been integrated into the same Department within the Bank.

Table 1 below provides an overview of the systems and institutions supervised and/or overseen by the Bank. In addition to the type of services provided, they have been further grouped according to: (i) the type of regulatory role of the Bank (i.e. prudential supervisor, overseer or both) and (ii) the system/institution's international dimension (the Bank as solo authority, international cooperative arrangement with the Bank as lead, or another role). For the systems and institutions established in Belgium which are systemically relevant in other jurisdictions' financial markets or for the financial industry as a whole, the Bank has established cooperative arrangements with other authorities[4]. These may involve multilateral cooperative arrangements, in which the Bank acts as lead overseer (Euroclear, Swift). The Bank also takes part in a number of international cooperative arrangements (CCPs, BNYM, T2, T2S and CLS) in which another national authority acts as lead overseer/supervisor. Domestically, the Bank cooperates with the FSMA which has responsibilities in the supervision of financial markets with regard to conduct of business rules. Annex 2 illustrates the organisation structure of FMIs with an international dimension established in Belgium.

1 European Market Infrastructure Regulation (EMIR): Regulation (EU) No. 648/2012 of 4 July 2012 on OTC derivatives, CCPs and TRs.

2 CSD Regulation (CSDR): Regulation (EU) No. 909/2014 of 23 July 2014 on improving securities settlement in the EU and on CSDs and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No. 236/2012.

3 The FSMA is assigned, together with the Bank, as the national competent authority for CCPs under EMIR.

4 In line with CPMI-IOSCO Responsibility E (cooperation between authorities). Through this report, the Bank intends to inform other authorities with which it does not have any formal cooperation but which may be interested in understanding the applicable framework, the regulatory approach and the main supervisory priorities.

Table 1

The Bank's oversight and prudential supervision of financial market infrastructures, custodians, payment service providers and other market infrastructures and critical service providers

(January 2023)

	International cooperation		The Bank acts as the sole authority
	The Bank acts as lead authority	The Bank participates in the supervision, under the direction of another authority	
Prudential supervision		Custodian bank The Bank of New York Mellon SA/NV (BNYM SA/NV)	Payment service providers (PSP) Payment institutions (PI) Electronic money institutions (ELMI)
Prudential supervision and oversight	Central securities depositories (CSD) Euroclear Belgium International central securities depository (ICSD) Euroclear Bank SA/NV Supporting institution Euroclear SA/NV	Central counterparties (CCP) LCH Ltd (UK), ICE Clear Europe (UK) LCH SA (FR), Eurex Clearing AG (DE), EuroCCP (NL), Keler CCP (HU), CC&G (IT)	Payment processors Worldline SA/NV
Oversight	Critical service providers Swift	Other infrastructure TARGET2-Securities (T2S) [1]	CSD NBB-SSS
	Payment systems Mastercard Clearing Management System [2]	Payment systems T2 [1] CLS	
	Card payment schemes Mastercard Europe [2] Maestro [2]		Card payment schemes Bancontact [1]
			Payment processors [3] Mastercard Europe equensWorldline Worldline SA/NV Worldline Switzerland ltd
			Payment systems Centre for Exchange and Clearing (CEC) [1]

Post-trade infrastructure	Securities clearing	Payments	Payment systems
	Securities settlement		Payment institutions and electronic money institutions
	Custody of securities		Payment processors
Other infrastructures	T2S		Card payment schemes
	Swift		

Source: NBB.

1 Peer review in Eurosystem/ESCB.

2 The NBB and the ECB act jointly as lead overseers (authorities responsible for oversight).

3 Only for certain Belgian activities – Act of 24 March 2017 on the oversight of payment processors.

BOX 1

Evolutions in the financial sector cyber threat landscape

The European financial sector has always been a target of choice for cyber threat actors. While their motivations remain the same (financial gain, information theft and service disruption), the last two years have shown notable evolutions in the associated threat actors and the way they operate. This article seeks to highlight specific developments that should be part of risk management activities of entities in our sector.

The rise of ransomware

Over the last few years, financially motivated threat actors have widely adopted ransomware and double or triple extortion attempts. In this modus operandi, the ransomware victim is first requested to pay to obtain the decryption key to recover the encrypted data. If negotiations fail, the threat actor requests a payment from the victim (double extortion) and/or pressures third parties involved (triple extortion) to avoid selling or making sensitive data public. The adoption of this modus operandi by several cyber-criminal groups and its profitability led to notable evolutions such as (i) the wider development of modular multi-stage malwares (comprising a first stage infection with the capability to download and execute more specific ones later), (ii) the leverage of cloud-based attack infrastructure (for phishing, malware delivery and command-and-control communication), (iii) the introduction of the ransomware-as-a-service model and (iv) the proliferation of initial access brokers (threat actors reselling a victim's network access to other actors).

While ransomware activity continues unabated, regardless of the geopolitical situation, it is crucial for the sector to adopt a defence-in-depth strategy including among other efficient backup, data loss/leak prevention, network segmentation, granular access management or threat hunting strategies. It is also worth noting potential changes in legal frameworks and cyber insurance policies which might evolve into forbidding ransom payments or no longer insuring losses due to ransomware attacks. Although these initiatives may lead to a reduction in the number of ransomware campaigns, it could also lead to ransomware incidents being kept quiet instead of reported.

Targeting the perimeter and beyond

Attack surface management has become increasingly complex nowadays for financial institutions, given threat actors not only exploit externally facing infrastructure but also the supply chain and third parties of these institutions. Targeting widely used technologies or third parties to get access to as many victims as possible becomes a more frequently used attack strategy.

On the one hand, mass exploitation of impactful zero- and N-days vulnerabilities (thus only recently known and potentially not patched yet) occurred widely in internet facing software such as mail servers or remote working solutions, as both are increasingly deployed since the pandemic. The exploitation of commonly used software and libraries highlights a concentration risk which must be kept under control via robust enterprise asset management, vulnerability management, patch management and secure development lifecycles.

On the other hand, advanced actors have increasingly been observed targeting the supply chain to infiltrate target companies. These attacks can take many forms, where notable cases range from the compromise of remote access technologies (e.g. SolarWinds), managed service providers (e.g. Okta) or the exploitation/backdooring of commonly used third party libraries integrated in a victim's software development lifecycle (e.g. Log4J vulnerabilities or backdoored Python packages). Addressing these attack vectors can be extremely challenging but can however be supported by a solid third-party risk management process and a secure software development lifecycle, as well as the "assumed breach" principle.

Payment chain manipulation and cryptocurrency attacks

Over the last two years, a significant decrease has been observed in successful campaigns manipulating the traditional payment chain of financial institutions (e.g., Central Bank of Bangladesh case in 2016). This is likely a consequence of the increased difficulty for threat actors to compromise such critical economic function since the establishment of customer security programmes such as the Swift CSP.

Threat actors known for targeting the traditional payment chain have since been shifting to attacking cryptocurrency assets. While this trend is currently still ongoing, recent regulatory initiatives (e.g., Market in Crypto-Assets) or cryptocurrency mining bans (e.g. Microsoft Azure bans) may turn this type of attack more difficult or less profitable. The financial sector might in such a scenario expect a resurgence of payment chain manipulations or an increase in Business Email Compromise (BEC) attacks and malicious insider coercion attempts, or even a surge in Credit Card fraud.

Cyber impact of the geopolitical crisis

Several potential scenarios were envisioned by cyber security experts since the beginning of the war in Ukraine. This section highlights two of the many types of observed cyber events that the sector could expect again in the future.

The first type is distributed-denial-of-service (DDoS) attacks performed by hacktivists. These were first targeting entities located in the countries directly involved in the war but are now also targeting nations and institutions supporting those countries or those that have imposed sanctions. While these attacks are having no or only minimal impact on institutions with robust DDoS mitigations in place, they could cause disruption by abusing unprotected internet facing hosts, misconfigured protection mechanisms or exploiting internet facing application vulnerabilities. The current situation emphasises the importance of reviewing the controls in place against this type of attack.

The second type is the risk of the sector being directly or indirectly targeted by destructive malware. While a scenario where destructive malware would indirectly spread (spillover effect, like the NotPetya case in 2017) outside the direct targets is now being regarded as unlikely, there were notable disruptive campaigns in 2022 such as the Gamaredon threat actor targeting Ukrainian government entities with destructive WhisperGate malware, initially disguised as ransomware. This type of threat is particularly relevant for national critical infrastructures and government institutions but should also be considered by the financial sector should the geopolitical situation worsen.

Conclusion

The developments highlighted in this article show the adaptability and opportunistic nature of threat actors targeting the financial sector. The cyber threat landscape is rapidly evolving, and institutions are advised to continue their efforts in bolstering and assessing their cyber resilience against such threats. These are also objectives of the Digital Operational Resilience Act and the TIBER framework that are presented respectively in chapters 5 and 8 of this Report.