2.4 Cyber risk and the national simulation exercise on cyber-security incidents

2.4.1 The cyber risk impact on the financial stability

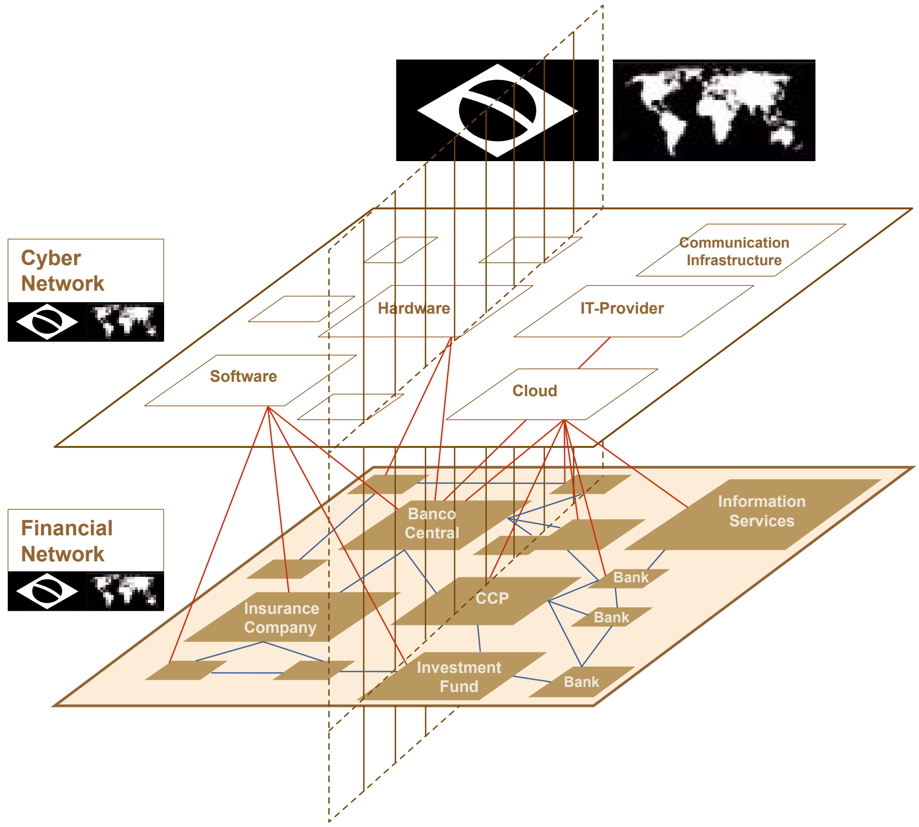
Financial systems are traditionally characterized by large investments in technology of information, aimed at the optimization of operational processes and the implementation of new business models. In recent years, it is noticeable the digital transformation process experienced by financial institutions, culminating in the development of financial services, which are increasingly digital. This technological dependency and inter-connection between systems and processes bring vulnerabilities to financial stability, since the risk of failures or cyber-attacks to these processes can have systemic proportions.

This risk is amplified to the extent that some services providers, such as cloud computing and data processing and storage services, become systemically relevant due to the potential concentration on certain companies. Technological development has created a relationships network between financial institutions, their service providers, hardware and software, both at national and international level, as presented in Figure 2.4.1.1. A cyber-attack targeted at a provider can affect all financial institutions that use its services. This concern is majored by the fact that these services providers are not subject to financial markets regulation.

The unpredictability, the immediate materialization and the growing complexity of cyber-attacks leverage the concern of regulators from different jurisdictions with this risk. Furthermore, due the attacks are not limited to physical borders and economies are increasingly interconnected, it is necessary to enhance articulation among supervisors, both at domestic and international level, aiming at information sharing and the development of joint actions, as well.

Data presented in different forums point to potential relevant losses to financial systems arising from electronic fraud (including cyber-attacks), in line with the discussions held during the Cyber Crimes investigation, held by the Brazilian Congress, and with different incidents targeting at the financial sector around the

Figure 2.4.1.1 – Cyber interconnectivity with the financial system



Source: Thilo Liebig, Deutsche Bundesbank, edited by BCB.

world (for example, attacks on the Bank of Bangladesh and some Mexican financial institutions).

In 2017, the Financial Stability Board (FSB) conducted a survey on existing regulation and supervisory practices[75]. The results showed that concerns regarding cyber risk are present in all surveyed jurisdictions. According to the study, cyber risk is usually handled within either operational or technological risk issues. However, there is a great diversity in terms of regulatory and supervisory frameworks (principles based x more prescriptive) and the disclosure on regulation is more frequent than on supervisory practices.

International organizations took the results of this survey as starting points for the development of several initiatives. Among them, Brazil has active participation in two working groups:

- FSB Cyber Lexicon – this group has recently released for public consultation a document with the consolidation of security and cyber resilience terms in the context of the financial sector; and

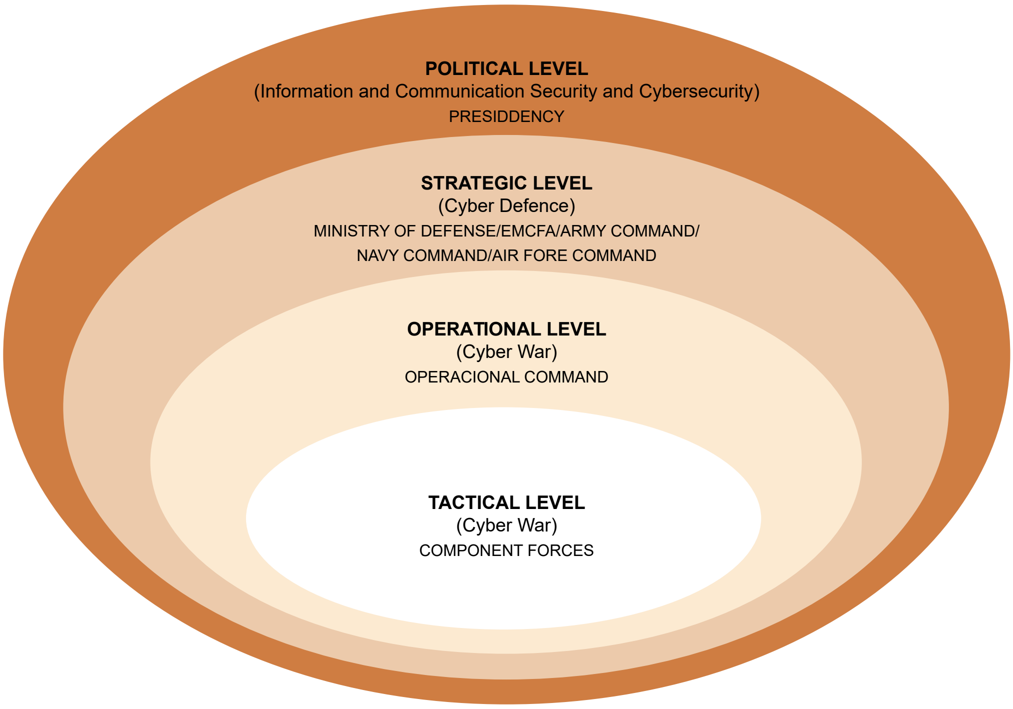
[75] "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices", published on October13th, 2017 (http: www.fsb.org/wpcontent/="" uploads/p131017-2.pdf="").

- BCBS Operational Resilience Group (ORG) – this group is working on the identification and definition of cyber resilience practices in the banking sector.

2.4.2 Managing and mitigating cyber risk in Brazil

Cyber risk is a priority concern of the Brazilian Government. In 2008, the National Strategy for Defense has established two levels on the decision-making process regarding cyber risk: political, in charge of the Presidency Institutional Security Cabinet (GSI); and strategic, in charge of the Ministry of Defense, also responsible for the definition of offensive, defensive and exploratory actions (Figure 2.4.2.1).

Figure 2.4.2.1 – Governmental decision levels on cybersecurity



Source: Cyber Defense Military Doctrine – Ministry of Defense, 2014

In the context of the NFS, issues related to technological risks, including aspects related to information security, have always been part of the BCB agenda.

In 1996, BCB has established a supervisory team specialized on the FI's technological infrastructure supervision, the IT Systems Auditor Team. Since then, the BCB has continuously developed various initiatives related to cyber security, as a response for the accelerated digital transformation observed in the financial system. These initiatives include the improvement of financial crisis management procedures for dealing with cyber-attacks that could affect the financial system; the review of MoU[76] established with supervisory entities from other jurisdictions, for the inclusion of specific agreements regarding cybersecurity; and the revision of its own supervisory procedures and routines, as well.

Since 2001, BCB coordinates the Subgroup for the NFS Security, which mission is to develop, consolidate and implement security standards for the electronic exchange of information among the NFS entities. Recently, following the evolution of cyber-attacks, BCB has intensified technical contact with other central banks, for experience exchange on the treatment of cyber threats, and started the exchange of information on threats and cyber-attacks among the NFS entities.

In the regulatory spectrum, issues regarding cyber security used to be treated under the operational risk scope. The exponential growth of its relevance in recent years culminated in the publication, in 2018, of Resolution No. 4,658, for financial institutions, and Circular No. 3,909, for payment institutions, with the objective of disciplining the use of important services for the innovation of the NFS technological framework, without despising cybersecurity issues. Both documents require regulated institutions to implement cyber security policy and to report cyber incidents to the supervisor. They have also established minimum requirements to be followed by regulated institutions, whenever hiring services on data processing and storing, and cloud computing.

In addition, the new regulation requires the report to BCB of information regarding the contracts on relevant data processing and storage services and cloud computing. This includes the identification of where those services are physically located, specifying the countries and the

[76] Memorandum of Understanding.

respective regions of each country. This information will allow BCB to map the NFS cloud services network and to identify any existing systemically important dependency on IT services providers.

2.4.3 The Cyber Guardian Exercise

Seeking to contribute to the integration among the government, the private sector and the academia for the improvement of cyberspace protection, the National Command for Cyber Defense (ComDCiber) of the Ministry of Defense developed and conducted, during July 3rd to 6th, the first national simulation exercise on cyber incidents: the Cyber Guardian Exercise.

This exercise was composed of the application of scenarios in a virtual simulator[77], with the objective of disclosing and disseminating best practices in the treatment of cyber incidents among participants; and tabletop[78] simulations, to train and integrate the high decision level of the participants with the cyber security national entities.

The incidents comprehended denial-of-service attacks, sabotage, informational leakage, fraudulent modification of systems and web pages, fake news, commitment to integrity of databases, among others.

The participants were encouraged to act in cooperation and integrated, with efforts focused on preventing and resolving incidents. They had to assess and solve not only the direct impacts on its informational assets, but also eventual indirect reputational and/or legal impacts, considering the existing technological and legal constraints. The teams comprised representatives from different hierarchical levels within each organization:

i) Representatives from decision-making staff (Crisis Committee): top managerial level, from the following areas: IT, communication, legal support and senior management. They were responsible for deliberating actions and measures to address the cyber events;

[77] ComDCiber has developed a virtual simulator tool, the Cyber Operations Simulator (Simoc), in which computing systems used by the participating entities were reproduced.

[78] Tabletop Tests are simulations where participants shall precisely follow the contingency plan instructions, for training purposes and adequacy assessment of the prescribed procedures, as well.

ii) Representatives from technical-operational staff: experts from the IT security area, responsible for responding to incidents at the virtual simulator; and

iii) Remote support team: experts from IT security and crisis monitoring areas, located at the headquarters of each participant entity, responsible for responding to the demands for information and executing the actions and measures commanded by their respective Crisis Committee.

In this first exercise, ComDCiber focused on the defense, financial and electronuclear sectors[79]. Other strategic sectors such as telecommunications, water supply and transport, shall also be tested in the future.

In addition to the simulations, a study group formed by representatives from all participating entities were in charge of drafting a proposal for the elaboration of the National Plan for the Treatment and Response to Cybersecurity Events, to be implemented in the future by GSI.

[79] This exercise comprehended representatives of the following entities: Ministries of Defence, Justice and Foreign Affairs; Presidency Institutional Security Cabinet (GSI); Navy, Army and Air Force; Federal Government agencies; Central Bank of Brazil; Banco do Brasil; Caixa; Itaú; Bradesco; [B]^3; companies from the nuclear sector; academic community and entities linked to the cyber sector.