CYBER RESILIENCE OF FINANCIAL INSTITUTIONS. PRIORITY OBJECTIVE OF "THE PATH TO THE DIGITAL DECADE - 2030"

Ruxandra Rîmniceanu[1]
[1]National Bank of Romania, Bucharest, Romania, ruxandra.rimniceanu@bnro.ro

ABSTRACT: The European Commission's report on the state of the digital decade 2025, published in June this year, reveals that progress is still needed to achieve the objectives set for the 2030 horizon, in particular in terms of artificial intelligence (AI), the cloud and big data (with 90% of the world's population expected to be online and a wide range of IoT devices in use). It also states that just over half of Europeans (55.6%) have a basic level of digital skills, while the availability of ICT specialists with advanced skills remains low and the gender gap is significant, while Europe depends on 80% of digital technologies and services from other countries outside the continent. Financial institutions coexist with a wide range of interrelated disruptive threats, such as technical failures, human errors and natural disasters, and cyberattacks are the result of malicious actions by cybercriminals (regardless of their sphere of activity). Added to these are the persistent challenges, such as fragmented markets, overly complex regulations, security and strategic dependence, meaning that the cyber resilience of financial institutions requires strengthening their capacity to prevent, detect and quickly recover from cyberattacks, maintaining their critical functionality and protecting sensitive customer data, in accordance with the incident regulations, as well as intensifying international partnerships to increase opportunities circumscribed by specific activities.
KEYWORDS: cybersecurity, digital operational resilience, digital technologies, systemic risks, cyber resilience.

DOI 10.56082/annalsarscieco.2025.4.41

1. INTRODUCTION

STATE OF THE ART

The times we are living in are increasingly marked by destabilizing factors or factors that can generate tense situations for the society as a whole and, especially, for the national, regional or international security, with the potential to reach a critical point in the next five to ten years, being favored, mainly, by:
• multiple and simultaneous crises, regardless of whether they are based on natural events or human actions, superimposed with various social movements and possible violent conflicts preceded by regional accumulations of power;
• increasingly unexpected political turmoil, resulted from the competition for power and the expansion or consolidation of nationalist currents in the east and south of the European continent, for the time being;
• uncertainties related to the evolution of new major economic trends, the weakening of the international framework regarding economic sanctions and even the decrease in the authority or relevance of global governance institutions (starting, for example, with the United Nations);
• climate changes and continuous environmental degradation, especially in arid and hot geographical regions that will expand and fuel existing conflicts in the Middle East, North Africa and Sub-Saharan Africa, and global warming is already opening a new area of competition and conflict in the Arctic region, so that the main actors - China, Russia and the USA - with the potential to attract other states, especially those from northern Europe that have interests in the region, favor the global spread of conflict zones and their three-dimensional development towards outer space;
• the new paradigm of hybrid warfare that is manifesting itself in the proximity of the Romanian border and which, from the American perspective (Hoffman, 2007) – "hybrid warfare", implied understanding the term as the "fusion of the effects of conventional and unconventional actions".
However, according to adopted policy and the reality in the Ukrainian theater of operations after February 24th 2022, the invasion of Ukraine was called a "special military operation". In this context, the concept of hybrid warfare itself was used, as an absolute war [1] and, in this way, the rigors of the international legal framework applicable until that moment were ignored. The concept covered the unclear area of insurrectionary war [2], based on seven subversive methods: propaganda, obstruction, sabotage, subversion, terror, guerrilla warfare and rebellion. Thus, at present, the semantics of this concept should be resumed and particularized, as well as adjusted the major differences between the two concepts, on the one hand, but also acted to strengthen regional and trans-Atlantic relations, in

order to consolidate a broader coalition of partners who share the same values, on the other hand.

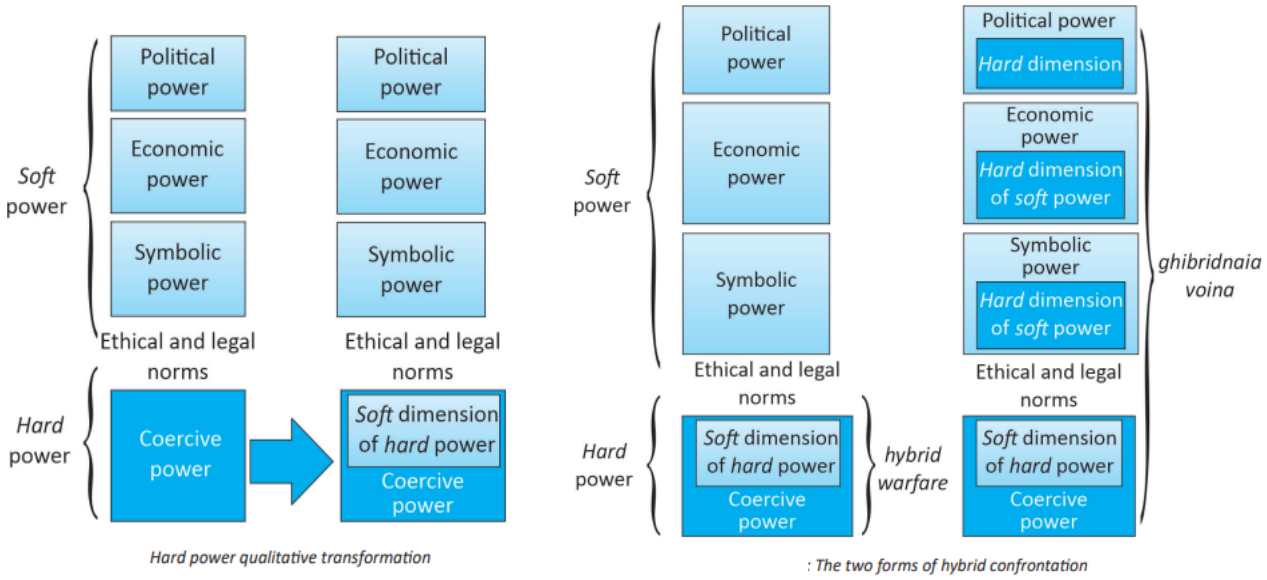

Figure 1. Traditional confrontation vs. Hybrid confrontation

In other words, given the DE FACTO SITUATION itself, we are outside the framework of hybrid warfare in the Western sense, but within the limits of the meaning from the Russian perspective, which REFLECTS THE CONDITIONS OF INSECURITY in which we carry out our professional and personal lives and REQUIRES THE USE OF ALL SKILLS TO IDENTIFY major trends in the evolution of regional and global security, in the shortest possible time, to counteract the risks and projected threats to protect society THROUGH EDUCATION AND SECURITY CULTURE and by "building the anti-ghibridnaia voina shield" THROUGH STRATEGIC COMMUNICATION and THROUGH SOCIETAL RESILIENCE.

2. CYBER RESILIENCE – AN INCLUSIVE PART OF SOCIETAL RESILIENCE

Before justifying the need for cyber resilience in the financial sector and the impact of cyber disruptions on financial institutions, I would like to remind of the importance of cooperation and the relevance of the efforts made at the diplomatic level, over time, to establish deeper and more equitable regional relations in the field of cyber resilience.

From this perspective, in the summer of 2014 (after the annexation of Crimea by Russia [3]), a Multinational Scenario Group of the Friedrich Ebert Foundation (FES) from Germany [4] developed four scenarios for relations between the EU, the Russian Federation and their common neighbouring states in 2030 [5]. The scenarios offered different possible and plausible visions for the developments foreseen at that time, but without being considered "forecasts" of this relationship. Until the Russian invasion of Ukraine, these scenarios constituted a "useful tool" in helping decision-makers and stakeholders adapt their strategies to achieve or avoid the situations circumscribed by the scenarios, namely:

Scenario I: The Divided House - All Europeans share the same house, for pragmatic reasons

After a «lost decade» marked by political crises and economic stagnation, starting in 2020, the EU and Russia are focusing on their common objectives. A new free trade agreement also integrates the Eastern Partnership states, which are no longer in a position to decide to be with or against one of the parties.

Scenario II: The Common House - Europe is the home of nations united around common values

A deep economic crisis in Russia leads to democratic and economic reforms, which pave the way for improving relations between the EU and Russia. As new economic powers assert themselves, Russia and the EU are joining forces, not only to end conflicts in Europe, but also to counter common threats.

Scenario III: The Ruined House - The European House Lies in Ruin

The current confrontations between the EU and Russia continue until 2030. A relatively successful authoritarian modernization of Russia and the EU-level transition in the energy sector offer both sides the opportunity to act independently. The common neighbouring states, which are the subject of intense competition between the EU and Russia, constitute a zone of instability.

Scenario IV: The Divided House - Europeans are neighbors living separately

The EU and Russia are stuck in a deadlock: a significant deterioration is prevented by continued economic interdependence. However, an improvement in the situation seems impossible, due to widespread distrust. No political and economic exchanges are taking place. Europe is increasingly losing touch with the new centers of global power.

After 11 years since the launch of the «EU and the East in 2030» scenario project, on August 2nd 2025 [6], a day after US President Donald Trump announced that Russian forces had lost 112,000 peoples since the beginning of this year, 14 times more than Ukrainian troops, Kyrylo Budanov, head of the Main Intelligence Directorate (DIU) of the Ukrainian Ministry of Defense, summarized the current situation in his country and appealed for national and international unity, presenting four possible scenarios for the evolution of the situation in Ukraine in a possible post-war period that could begin as early as 2025, namely:

Scenario I: the Georgian model (Georgia's evolution after the 2008 war - ed.), is "most likely in a proportion of 50%".

Ukraine does not receive stable support from the West, is faced with instability, slow post-war recovery, European integration fails and, once again, enters the Kremlin's orbit.

Scenario II: the Israel model, estimated at 20% chance.

"It implies strong and constant economic and political support for Ukraine from the allies, but without a significant presence of foreign troops. This is the scenario of the country's transformation into a fortress and rapid military modernization," Budanov said.

Scenario III: South Korea model, considered “most desirable for Ukraine now”.

Although it does not provide for NATO membership and the return of occupied territories, it is possible to allow the presence of allied troops on the territory of Ukraine and receive guarantees from the US. In this case, “on 80% of the territory, Ukraine can live, develop and have a certain security again”.

Scenario IV: Belarus model, not wanted.

“The US refuses support. Europe does not become more active. Ukraine, under Moscow’s demands, turns into a vassal state. Russia wins the war, the West staggers, the world order will be irrevocably undermined.”

According to the head of DIU, the “Georgian” and “Belarusian” scenarios would not satisfy Ukrainian society, also stating that “With the departure of the leader of the Russian Federation, nothing will change there. They have built a system so that the successor will be at least in the current paradigm. A whole class of people has already grown up in Russia, who were born, live, and some have already died under President Putin. They cannot imagine any other life”.
In this context, the concrete disputes and geostrategic connotations regarding the conception and conduct of future wars, tacitly declared, increasingly and clearly emphasize on the prospect of rapid and profound changes in terms of "high-performance combat means" that can determine substantial mutations in the conduct of modern military actions, given the affirmation of new data of technological progress (such as high-performance computing, common data infrastructure and services, blockchain technology, low-power processors, pan-European development of 5G corridors, high-tech partnership for digital skills, secure quantum infrastructure and the network of cybersecurity centers, digital public administration, testing facilities and digital innovation centers). All of this was also included in the European Union's 2030 policy programme, entitled "Roadmap to the Digital Decade" [7], which must ensure that the EU meets its objectives for an appropriate digital transformation, in line with its values, as well as support the development or production of critical technologies across the Union or the protection and strengthening of value chains in three areas of interest: deep and digital technologies, clean technologies and biotechnologies [8] and, respectively, their legal and institutional governance rules.
Thus, the common objectives for the mobilisation of public and private actors [9] proposed since March 2021 by the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, provide for - table no 1.

Table 1. EU objectives for 2030 and targets to be achieved

Nr. crt.	EU target for 2030	Size	Target to be achieved compared to the baseline situation
1.	***"A continent with good technological skills where everyone is digitally autonomous"***	ICT specialists	**20 million ICT professionals employed, with gender parity (2019 baseline: 7.8 million)**
2.	***"Secure and reliable state-of-the-art digital infrastructures"***	Connectivity	**All European households to have a gigabit network and all populated areas to have 5G.** **Baseline:** **— Gigabit coverage (2020 baseline: 59%).** **— 5G coverage in populated areas (2021 baseline: 14%).**
		semi-conductor	Production of advanced and sustainable semiconductors in Europe, including processors, to represent at least 20% of global production in value. (Baseline 2020: 10%).
		Edge/cloud nodes	**10,000 highly secure and climate-neutral edge nodes are to be deployed across the EU; they will be distributed in a way that guarantees access to low-latency (a few milliseconds) data services, regardless of where businesses are located.** **(Baseline 2020: 0)**
		Quantum computing	**By 2025, Europe will have its first quantum-accelerated computer, and Europe will be at the forefront of quantum capabilities by 2030.** **(Baseline 2020: 0)**
3.	***"The continent with a high percentage of digitalized enterprises"***	Adoption of digital technologies	**75% of European businesses have adopted:** **- cloud computing services (2020 baseline: 26%);** **- big data (2020 baseline: 14%);** **- artificial intelligence (AI) (2020 baseline: 25%).**
		Late adoption of digital technologies	**Over 90% of European SMEs reach at least a basic level of digital intensity.** **(Baseline 2019: 60.6%)**
		Innovative companies/scale -up companies	Europe will broaden its portfolio of innovative scale-up companies and improve their access to finance, leading to a doubling of the number of unicorns. (Baseline 2021: 122)
4.	***"Modernized public services that meet the needs of society"***	Public administration as a platform	– essential public services available to European citizens and businesses to be provided 100% online; – 100% of European citizens to have access to health records (e-records); – 80% of citizens to use a digital identification solution. **Baseline 2020:** – essential digital public services: 75/100 (citizens), 84/100 (businesses) – citizens having access to health records: N/A – electronic identification: currently there is no baseline for the adoption of electronic identification

All these goals, aimed at digitalisation and digital transformation, constitute an ambitious initiative, the success of which depends on the long-term commitment of the EU, the Member States and businesses, on the one hand, but also an exposure to several risks, on the other hand, through persistent strategic dependencies that threaten the EU's economic security and technological sovereignty, in particular in the areas of semiconductors, cloud and data infrastructure and cybersecurity technologies.

According to the European Commission's State of the Digital Decade 2025 Report [10], published in June this year, it is assumed that, although there is some progress, the deployment of connectivity infrastructure (such as fibre optics and independent 5G networks) is still delayed. More and more

companies are adopting artificial intelligence (AI), the cloud and big data, but at a slow pace. The report also states that just over half of Europeans (55.6%) have a basic level of digital skills, while the availability of ICT specialists with advanced skills remains low and there is a significant gender gap, hindering progress in key sectors such as cybersecurity and AI. In 2024, the EU made steady progress in the digitalisation of essential public services, but a substantial part of the government's digital infrastructure continues to depend on service providers from outside the EU, indicating that Europe is 80% dependent on digital technologies and services from third countries.

The published data shows that there are persistent challenges, such as fragmented markets, overly complex regulations, security and strategic dependence, meaning that it is estimated that additional public and private investment and easier access to venture capital for EU companies would accelerate innovation and scale-up.

Today, Europe is facing a new reality marked by increasing risks and uncertainties, which requires its readiness to react as urgently as possible. Based on the analysis of ways to increase preparedness for future crises, the Niinistö Report on EU Preparedness [11], presented in the last quarter of 2024, together with the Draghi Report on Competitiveness [12], contributed to the drafting of the main European proposals on defence, security and preparedness. As a consequence, in March 2025, the White Paper on European Defence Preparedness 2030 [13] was launched, which highlights the 7 critical areas that require defence capabilities and actions at EU level "to enable Europe to have a strong and sufficient European defence posture by 2030", as it is shown bellow.

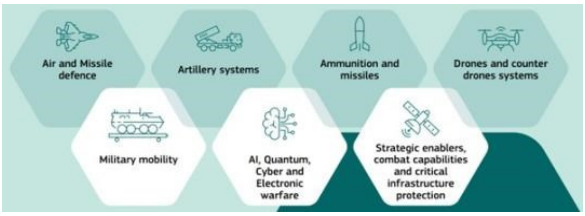

Figure 2. Critical areas of defense capabilities for actions at EU level

As a result, the White Paper on European Defence Preparedness 2030, together with the Rearmament Plan for Europe [14], introduces an ambitious package of financial measures to support EU Member States in significantly increasing their defence investment. The plan aims to increase spending from 102 billion EUR in 2024 - equivalent to 1.9% of the EU's combined GDP - to at least 800 billion EUR over the next four years.

The White Paper on EU Defence and the Preparedness Union Strategy for preventing and responding to emerging threats and crises [15] was followed by ProtectEU: an EU Internal Security Strategy [16], published in April 2025, which aims to provide a comprehensive and unified framework to effectively prevent, detect and respond to security threats. It includes:

• a new European governance on internal security, with regular evaluation and monitoring of security and preparedness initiatives;

• increased threat awareness, anticipation of security threats and improved information sharing;

• more effective law enforcement tools and stronger justice and home affairs agencies, with new mandates for Europol, ENISA, a new European Critical Communication System (EUCCS), legal and effective access to data for law enforcement and a roadmap on encryption;

• strengthening resilience against hybrid threats, fully implementing the Critical Entity Resilience Directive (CER) [17] and the Directive on measures for a high common level of cybersecurity across the Union (NIS2) [18], through a new Cybersecurity Act to improve the European certification framework [19] , a revision of the Cyber Solidarity Act [20], measures to reduce risks in supply chains from high-risk suppliers and guiding the development and uptake of new technologies such as post-quantum cryptography and quantum communication infrastructure (e.g. EuroQCI);

• combating serious and organised crime, by strengthening law enforcement capacities to track illicit finance, strengthening safety measures and implementing more effective strategies;

• countering terrorism and violent extremism, with a new agenda and a new set of tools;

• the EU as a strong global actor in the field of security, boosting international cooperation.

By referring to the proposals contained in the programmatic documents and those presented above, combating the cyber risk concentrated in our interconnected world constitutes the major objective of the field of cybersecurity and, equally, a challenge for the management of all institutions involved, regardless of the field and sphere of activity to which they belong - central or local administration or as a public or private institution, given that the critical infrastructure (operational technology) for businesses is threatened, the national security of each state is often underestimated and, recurrently, the global economy is affected.

The above statements are also supported by the results of one of the most comprehensive analyses conducted worldwide in 2024 by SecurityScorecard researchers in collaboration with the RSA 2024 President's Forum and McKinsey & Company from the United States of America [21], which reveals that:

• 90% of the global cyber attack surface [22] is dominated by 150 "top vendors" (determined based on detectable market share of technological products and services offered to customers) and by a "core" of 15 "heavyweights" (with an even greater concentration of market share), which reflects the dependence on "a handful" of vendors that shape the "foundation" of our global economy, themselves being the main targets of cyber attacks and, in turn, creating premises that can amplify the potential damage of security breaches that, recurrently, affect their vendors, customers, investors or partners;

• of the 150 companies, in the last year, 41% had evidence that at least one of their devices had been compromised, and 11% were victims of a "ransomware infection" [23];

• 62% of the global external cyber attack surface concentrates the products and services offered by just 15 companies;

• the top 15 third parties have below-average "cyber risk scores", indicating a higher likelihood of a data breach.

In spite of all this, societal resilience does not only mean the ability to withstand and cope with challenges, but also to achieve transitions in a sustainable, fair and democratic way, as the European Union must be prepared to face more complex, cross-sectoral and cross-border crises, which could be acute, multi-dimensional or hybrid and which could have cascading effects or occur simultaneously. Resilience to such challenges will have to ensure the adequate management of those events, in relation to known, foreseen or unexpected risks - to counteract or mitigate unwanted effects.

It is forecasted that the global financial order enters in a new era [24], in which the global financial system would fragment between state digital currencies (Europe promoting central bank digital currencies - CBDC, to maintain its monetary control) and private stablecoins (the USA supporting a decentralized system, developed by the private sector through regulated digital currencies [25] to strengthen the dollar and attract capital). Gita Gopinath, First Deputy Managing Director of the International Monetary Fund, had been warning about this issue since mid-2024, in a speech taken from the World Economic Forum report from January 2025 [26] and, with that occasion, she asked countries "to build resilience", arguing that "in the absence of sufficient safety barriers, we could end up with a severe fragmentation of the global economy and, consequently, lower productivity and income levels for everyone".

Given this, questions persist regarding the implications of the current geo-strategic, geo-political and geo-economic context for monetary policy, namely:

"How should central banks conduct monetary policy in this more shock-prone environment?"

"What is the role of additional instruments, such as foreign exchange intervention?"

"How should fiscal, financial and structural policies be implemented to support macroeconomic and financial stability?"

Thus, it is vital that, in the generally known context, marked by increased unpredictability, atypical challenges, diverse and emerging risks, as well as limited terms and conditions for making optimal decisions to anticipate/solve critical situations arising in the cyber security and defense segment, decision-makers, at the individual level, but also through inter-relationships with other competitors or with competent national and international authorities, support and strengthen the communities they lead or collaborate with in an integrated way, ensuring a rapid circulation of relevant information and capitalizing on the experience gained, through lessons learned.

The future Digital Package of the European Commission, expected in the 4th quarter of 2025, aims to reduce the administrative burden and simplify the legislation on cybersecurity.

3. CYBER RESILIENCE - BEYOND THE "PREDICT AND PROTECT" PARADIGM

In general, RESILIENCE is the ability to withstand, recover from and adapt to external shocks. The main principle of resilience is not to be able to accurately predict the future in order to protect SOMETHING against possible damage. Instead, it involves to develop a qualitative capacity to design and operate systems that can withstand adverse events, no matter how unexpected they may be.

Resilience has a broader scope than risk management and it is a concept based on a multitude of theoretical and practical traditions, noting that, for some, it implies the ability of a system to

withstand a shock and return to its initial state, while, for others, it implies an evolutionary process leading to adaptation and a new state of equilibrium. From a theoretical perspective, CYBER RESILIENCE often boils down to the engineering properties of information systems that can withstand sophisticated cyber attacks or to the incident response methodologies required to respond to such attacks. However, the specialized literature [27] contains numerous detailed models that provide a vast list of elements that can enable organizations to achieve cyber resilience, but from a "maturity level" perspective, they usually belong to one of the following five "high-level" dimensions, beeing dynamic, interconnected, practiced, adaptive and contested.

In practice, however, the same specialists who theorized [28] have identified four central ambiguities and uncertainties of cyber resilience (polysemantic meaning, turbulent risk landscape, contested organizational rationalities, and disparate regulatory requirements) which, in turn, determine five types of activities triggered by organizations' exposure to cyber risks (human resources, communication, networking, strategies and adaptation) that attempt to mitigate these "tensions" to improve the quality and reduce the uncertainty of the decision-making process.

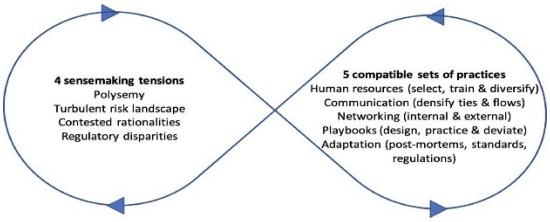

Figure 3. Cyber resilience cycle

Therefore, it was established [29] that the processes and technologies needed to increase cyber resilience apply to socio-technical systems defined by the interconnection of people and machines. This implies that in order to provide cyber resilience robust systems must be designed, that social practices must be applied and that human actions must be promoted to allow people to adapt systems to unpredictable attacks.

In response to the increasing number of cyber attacks targeting devices and networks, at the end of 2024, the European Union took a significant step towards ensuring the security of its digital environment by adopting the Cyber Resilience Act (CRA) [30], which aims to strengthen the cybersecurity of all products containing digital components, directly or indirectly connected to a network (from baby monitors to smartwatches), providing confidence to both consumers and businesses. The CRA builds on the EU Cybersecurity Strategy launched in 2020 and complements the NIS2 Directive. These new obligations ensure harmonised standards, security requirements covering the entire product life cycle and duty of care.

By 2027, manufacturers must ensure that their products comply with the CRA requirements and bear the CE marking, a guarantee of compliance with EU cybersecurity standards. This change places the responsibility directly on the shoulders of manufacturers, allowing consumers and businesses to make better-informed purchasing decisions based on the security features of CE-marked products.

4. THE NEED FOR CYBER RESILIENCE IN THE FINANCIAL SECTOR

The concept of CYBER RESILIENCE is particularly relevant for financial institutions which, incidentally, already coexist with a wide range of interrelated disruptive threats, such as technical failures, human error, and natural disasters. Financial institutions' digital assets are also subject to constant attacks from cybercriminals, government hackers, activist hackers, and disgruntled employees seeking to infiltrate or cripple IT systems. This unprecedented level of malicious activity can have a very significant impact on the most robust organizations.

Cyber resilience of financial institutions refers to their ability to prevent, detect, and rapidly recover from cyberattacks, maintaining their critical functionality and protecting sensitive customer data. This involves implementing strict security measures, such as those provided for by the EU Digital Operational Resilience Regulation (DORA) [31] and the Cyber Resilience Act (CRA), which require security by design and cybersecurity transparency for digital products.

We can affirm that through the rigor and complexity with which the approach to cybersecurity has been regulated in the financial and banking sector, "operational resilience is the new standard in cyber defense" and can be quantified as the sum of actions and activities regarding security, compliance and the integration of related protection measures for the compatibility/interoperability of information and communication systems serving this critical sector.

From this perspective, the competitive advantage and the difference on the "field of future confrontations" will not only consist in investments in new technologies, but, in particular, in the

capacity for strategic forecasting, based on a robust and well-regulated financial system, both at a national and institutional level which, in turn, must implement viable security and defense policies, prepared to respond to fundamental, surrounding dilemmas, from the external and internal environment, by approaching and treating risk management in an anticipative and pro-active manner, in order to prevent and mitigate the impact of systemic risks.

Therefore, the volume of the effort that will be made in the next period of time (until 2030), at the micro- and macro-economic level, will be based on concrete, measurable measures that will be adopted in relation to the systemic risk potential and the complexity of risk management, requiring to be oriented "towards a sustainable future", so that the interconnection of the various factors and their potential impact on the expected results can reveal the essential role and function of financial institutions in the development and growth of the Romanian economy, as well as their exploratory work regarding the dimension of cybersecurity [32] (Fig.4).

In this context, the financial institutions and the third-party IT service providers should prioritize the risk assessments of their IT&C systems, the governance mechanisms for risk management and incident response in the aim of ongoing resilience testing and monitoring.

"Early action" through Security Operations Centers (SOCs), Cybersecurity Incident Response Teams (CSIRTs), or other cyber teams also allows organizations to identify gaps, strategize, and allocate resources effectively, avoiding last-minute disruptions.

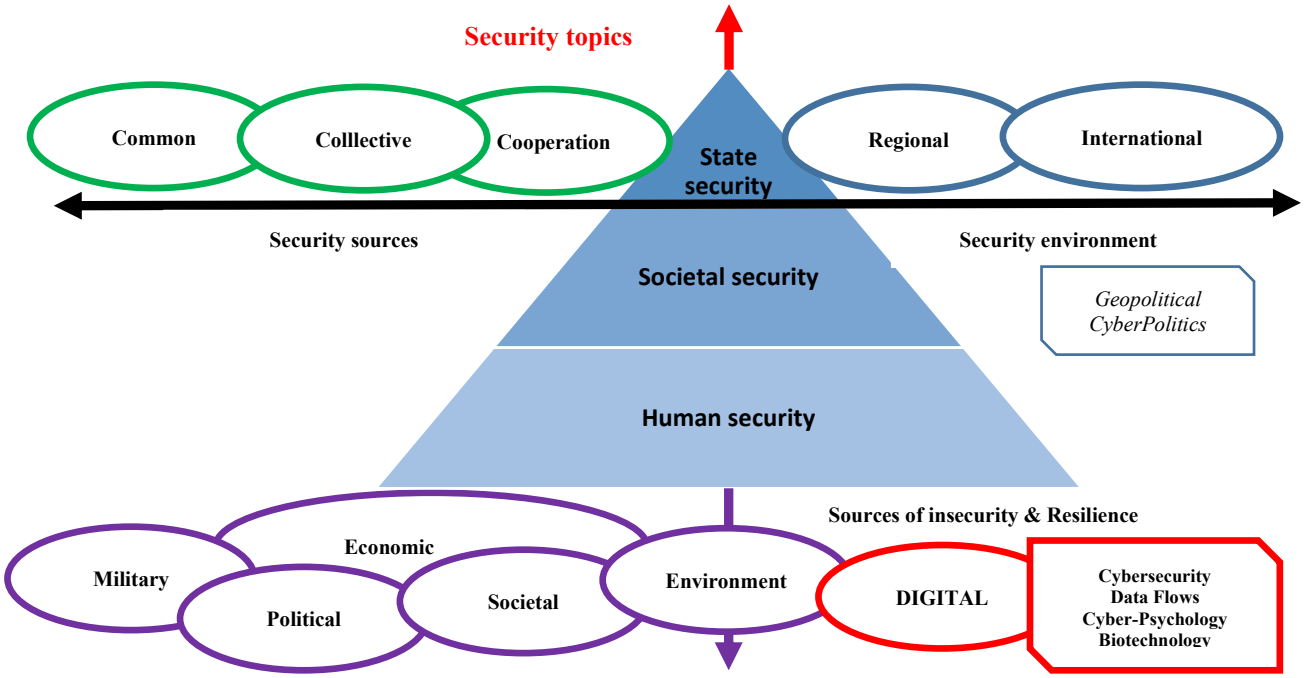

Figure 4. Dimensions of cybersecurity

THE PROCESS MUST CONTINUE because it is evident that the financial repercussions of non-compliance are greater than the costs of maintaining or meeting compliance requirements.

A recent benchmark study conducted by GlobalSCAPE, Inc. and Ponemon [33] in March 2025 showed that the internal risk management approach has clear benefits, namely the cost reduction, no fines and technology optimization through artificial intelligence and consolidation.

According to this study, the cost of risk for insiders continues to increase, reaching an annual average of $17.4 million – up from $16.2 million in 2023 – largely driven by increased spending on incident containment and response, and the incident containment times have decreased – from 86 days to 81, a clear sign of progress (Fig.5).

Essentially, cybersecurity is largely a human challenge, as human errors, misconfigurations, and human negligence are considered the main causes of cyberattacks. While there are also technical aspects that destabilize the functioning of IT equipment within parameters, the human factor plays a crucial role in the vulnerabilities of digital systems.

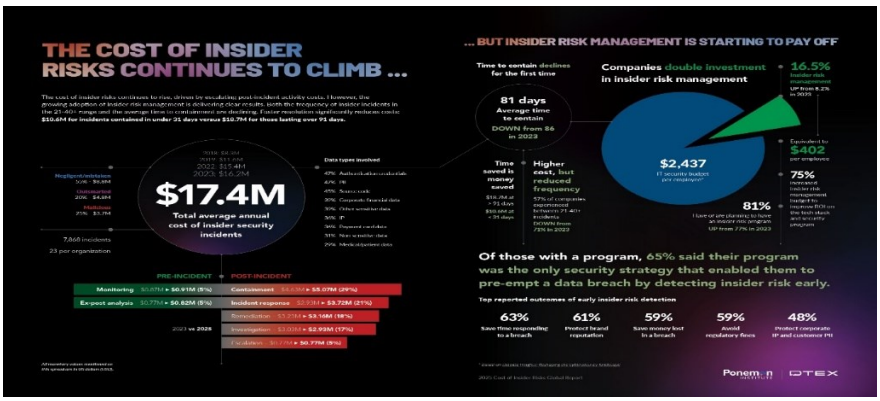

Figure 5. The cost of internal risk management

Therefore, the "key" to proactive defense lies in an internal risk management program, requiring a human-centric approach based on behavioral science. Financial entities must develop early warning indicators of risky behaviors and have adequate mechanisms in place to effectively detect and deter risks before they turn into security breaches that, unfortunately, can lead to business interruption, lost productivity, fines, penalties, and settlement costs, among other factors that come with a considerable cost (Fig.6).

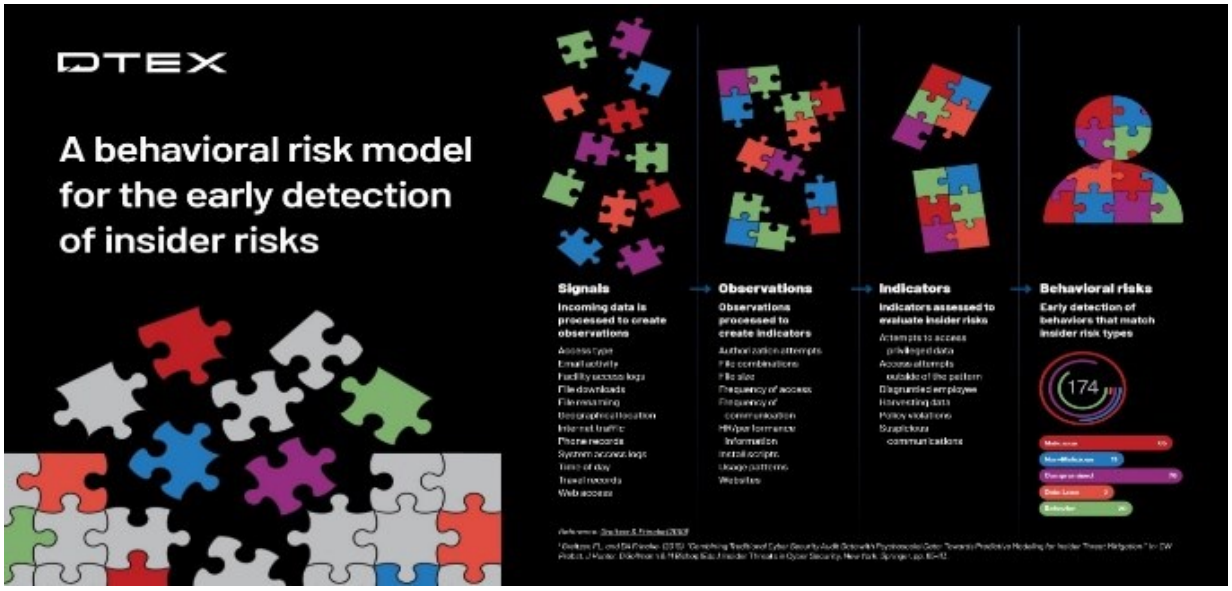

Figure 6. A behavioral risk model for the early detection of insider risk

Even DATA BREACHES ARE MORE COSTLY IF AN ORGANIZATION IS NOT COMPLIANT.

When considering this option, banks and financial institutions should consider:

- the costs of preparing for financial audits;
- potential "blind spots" in systems and their observability;
- the risks associated with supporting One Stop Shop (OSS) [34] security;
- the benefits of standardization, support, and service level agreements (SLAs) to help operationalize database automation at scale.

From the perspective of the above, the strategic actions to strengthen cyber resilience at the level of each financial entity primarily aim to:

• managing critical dependencies;
• improving cybersecurity policies;
• developing collaborative defense strategies;
• developing a security culture, both at the organizational level and at the level of the financial-banking community, to educate all personnel, because, it being well known that employees are the "weakest link in cyber defense" of any organization, but also the "first line of defense".

5. ESTIMATES OF THE IMPACT OF CYBER DISRUPTIONS ON FINANCIAL INSTITUTIONS

The conclusion of the EU Agency for Cybersecurity (ENISA) Report, published in March 2025 and entitled NIS360 [35], reinforces the fact that, at the European level, "The criticality of the financial sector, as a whole, is at a high level. (…) Maturity in the sector remains high or moderately high, with prospects of becoming very high. This is due to the implementation of EU Regulation 2022/2554

(DORA), which affects all entities in the financial sector [36], not just entities included in the scope of the NIS2 Directive". The results of the report are based on data reported by national competent or sectoral authorities, in particular by the entities responsible in the concerned sectors or on information from EU sources (such as Eurostat), assess the maturity and criticality of the vital sectors defined under EU Directive 2022/2555 concerning measures for a high common level of cybersecurity across the Union (NIS2 Directive) and provide both a comparative overview and a more in-depth analysis of each sector, with the aim of helping Member States and national authorities to identify gaps and prioritise their resources.

The aforementioned report also highlights that the financial sector:

• is dependent on information and communication technology (ICT) and critical infrastructure for its core operations, including transactions, data management, risk analysis and fraud detection, requiring the real-time processing of vast amounts of non-public data, with accuracy and ensuring the efficiency of services (such as online banking, trading platforms and payment systems), but also the establishment of cybersecurity measures to protect sensitive financial data from specific threats, against cybercriminals and prevent the leakage of such data to unauthorized persons;

• has robust cyber risk management practices in place, such as adopting cybersecurity policies and implementing measures to promote trust in the "supply chain", including real-time threat detection, to better protect their services, based on standards and guidance issued by the European Supervisory Authorities (ESAs) [37] prior to the applicability of the DORA Regulation, such as the EBA Guidelines on ICT and Security Risk Management [38], EIOPA Guidelines on ICT Security and Governance [39], Cyber Resilience Supervisory Expectations for Financial Market Infrastructures [40], etc.

Thus, banking institutions are perceived as having a higher level of maturity in managing cyber risks compared to financial market infrastructures (FMIs), which report lower levels of capability, mainly having cybersecurity plans but not testing them consistently and, as such, are only able to detect simpler attacks. This may also be motivated by the fact that the banking sector benefits from two very active Information Sharing and Analysis Centres (ISACs) [41], which encourage collaboration within the cybersecurity community and include a large number of banking institutions as members in FI-ISACs [42] and FS-ISACs [43], while FMIs do not benefit from the same level of organisation.

On the other hand, the maturity level of banking entities is measured and supported by:

• The European Central Bank (ECB) which, also in 2024, conducted a cyber resilience stress test for banks [44], based on the new TIBER-EU framework [45], thus helping competent authorities and financial entities to meet the requirements for threat-based penetration testing;

• The Cyber and Security Information Sharing Initiative (CIISI-EU) [46] which supports systemic actors in the financial ecosystem to protect the financial system by preventing, detecting and responding to cyber attacks, facilitating the exchange of information and best practices between financial infrastructures and raising awareness of cybersecurity threats;

• the three European Supervisory Authorities - EBA, EIOPA and ESMA - which, since November 2024, have created the EU Systemic Cyber Incident Coordination Framework (EU-SCICF) [47], in application of art. 49 par.(1) of the DORA Regulation, to facilitate an effective response of the financial sector to a cyber incident that poses a risk to financial stability and may lead to a systemic cyber crisis by strengthening coordination between financial authorities and other relevant bodies in the European Union, as well as with key actors at international level. The approach is recurrent to the recommendation of the European Systemic Risk Board (ESRB) of December 2021, with reference to the deficit in crisis management that could lead to a lack of coordination of the financial sector in the event of a significant cross-border incident, with the potential to disrupt critical financial services and operations, either as a result of the emergence of operational or financial contagion or through an erosion of confidence in the financial system. Thus, from the beginning of February 2025, the ESAs and the German Federal Financial Supervisory Authority (BaFin) are progressively developing this EU-SCICF framework by promoting and testing relevant tools (e.g. procedures, arrangements) to support effective coordination between authorities in the event of a systemic event. To this end, the forum will also support a network of authorities that would come together during such an incident or threat.

If appropriate measures are not taken, in relation to the type of systems, their geographical dispersion, the third parties involved, the security of the "supply chain", etc., the implications for financial institutions are alarming and, rightly, justify adding cyber resilience as a key tool in their risk management toolkit.

6. CONCLUSIONS

As early as 2022, some cited sources [48] predicted that, in 2030, 90% of the world's population (respectively 7.5 billion people) would be online, with the number of connected IoT devices estimated to be between 24.1 billion and 125 billion.

It is therefore becoming increasingly clear that cybersecurity will be an essential component of our lives so that the digital solutions we use are safe and reliable. However, the sharp deterioration of the international geo-political situation, generated by the Russian-Ukrainian military conflict, has led to the escalation of several security risks, the emergence of new waves of uncertainty, as well as the large-scale adoption of unprecedented economic and financial measures, the impact of which on the European and global economy is difficult to estimate, EVENTS CONTINUE TO DEVELOP RAPIDLY.

In this context, financial markets remain sensitive to the materialization of risks or to the worsening of macroeconomic prospects (given recent developments in energy or raw materials markets, as well as disruptions in distribution channels, under the pressure to find alternative sources of supply). All these factors keep several risks at a high level, new shocks being able to cause increased tensions and significant corrections in international and local financial markets:

- macroeconomic risk, given that it is expected that new sources of risk generated by the crisis caused by the armed conflict between Russia and Ukraine will affect the economy at a global level, and the prospects for recovery and consolidation of the economies of states, generating an attenuation of the economic growth rate and a rapid increase in inflation;
- market risk, with a growing probability of materialization, in the context of maintaining the decoupling of asset values from economic fundamentals amid increasing contagion and worsening macroeconomic prospects, along with the high degree of uncertainty manifested in the context of the current crisis and the reduction in consumer and investor confidence, which may cause the erosion of asset prices;
- operational risk, with a growing tendency, amid the intensification of large-scale cyber attacks, in the context of the military conflict between Russia and Ukraine.

International partnerships for the Digital Decade are proving to be not only a key factor in economic and societal resilience, but also in global influence, so that by 2030 they should lead to more opportunities for European businesses, increased digital trade through secure networks, respect for European standards and values, and a more favorable international environment for the kind of human-centered digital transformation that the EU and other partners want to see.

For the "Digital Decade of Europe" to be a success, unfair and abusive practices must be tackled and the EU's digital "supply chains" must be secure and resilient.

The EU's starting point is an open digital economy based on the flow of investment and innovation as a driver of prosperity. At the same time, the EU will firmly promote our fundamental interests and values, through three overarching principles: a level playing field in digital markets, a safe cyberspace and respect for fundamental rights online.

Trade policy and agreements will play a key role in this by setting global and bilateral rules for digital trade in an open but assertive manner, based on European values. As a central element of the renewed transatlantic relationship, the EU has proposed the establishment of a new EU-US Trade and Technology Council to deepen the trade and investment partnership, strengthen joint technological and industrial leadership, develop compatible standards, deepen research collaboration, promote fair competition and ensure the security of critical "supply chains

7. REFERENCES

1. The term “absolut war” admits the entire range of military actions defined 200 years ago by the Prussian general Carl von Clausewitz, being translated into the text “[Hybrid war] is a confrontation that aims to destroy the opponent, to annihilate the independence of its system of government and to bring it under your complete control. Hybrid war aims to reduce the opposing country [from its status as an independent state] to a territory under your own authority”, written by the Russian academician Mikhail Genadievich Deliagin on his blog, in 2013 - https://delyagin.ru/, before the annexation of Crimea (2014) and the conflict in Donbas (2014), respectively after proclamation of the Islamic Caliphate (2014).

2. "insurgency war" or "insurrectional war", terms consecrated by Evgeny Messner (1891-1974), colonel of the General Staff of the Tsarist army. The objective of "insurrectional war" is to induce panic in the enemy's mind, distrust in leaders, in one's own forces, opinions, feelings and demoralization of troops and the population.

3. The beginning of the occupation is considered to be the period February 20-22, 2014, when Russia began open aggressive actions.
4. The Friedrich Ebert Foundation (FES) is the oldest so-called party-affiliated foundation in Germany and is closely associated with the Social Democratic Party of Germany (SPD). According to the Association of German Foundations, the Friedrich Ebert Foundation is the second largest of all German political foundations, with total expenditures of 190.3 million euros in 2019. Like most other political foundations, it is not a foundation, both legally and economically, but a registered association. Its headquarters are in Bonn and Berlin, with 18 regional or state offices nationwide and 104 offices worldwide (as of 2024), https://de.wikipedia.org/wiki/Friedrich-Ebert-Stiftung, accessed on 14.09.2025.
5. Friedrich-Ebert Foundation (2014), EU and the East in 2030, https://library.fes.de/pdf-files/id-moe/11246.pdf, accessed on 14.09.2025.
6. Defence Romania (04.08.2025), The 4 post-war scenarios in Ukraine, presented by Ukrainian military intelligence itself. In the worst scenario, Ukraine ends up in Russia's orbit, https://www.defenseromania.ro/cele-4-scenarii-post-razboi-in-ucraina-prezentate-chiar-de-spionajul-militar-ucrainean-in-cel-mai-negru-scenariu-ucraina-ajunge-pe-orbita-rusiei_634863.html, accessed on 14.09.2025.
7. Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the 2030 Policy Agenda for the Digital Decade, https://eur-lex.europa.eu/eli/dec/2022/2481/oj?locale=ro, accessed on 02.08.2025.
8. Regulation (EU) 2024/795 establishing the Strategic Technologies for Europe (STEP) Platform, https://strategic-technologies.europa.eu/index_en, is complementary to Regulation (EU) 2021/241 establishing the Recovery and Resilience Mechanism, https://eur-lex.europa.eu/legal-content/RO/TXT/?toc=OJ%3AL%3A2021%3A057%3ATOC&uri=uriserv%3AOJ.L_.2021.057.01.0017.01.RON and aims to support projects that develop technologies that meet any of the following conditions:
• bring to the internal market an innovative, emerging and cutting-edge element with significant economic potential;
• contribute to reducing or preventing the Union's strategic dependencies.
By the Regulation (EU) 2023/435 amending the Recovery and Resilience Mechanism, https://eur-lex.europa.eu/eli/reg/2023/435/oj/ron, allows EU Member States to introduce REPowerEU chapters in their recovery and resilience plans to accelerate the EU's transition to clean energy.
9. Digital Compass 2030: European blueprint for the digital decade, https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=CELEX:52021DC0118, accessed on 14.09.2025.
10. European Commission Report on the State of the Digital Decade 2025, https://www.telefonica.com/en/wp-content/uploads/sites/5/2025/06/1__Communication_DD_2025_mkp5iXF3ISoSJGNyEGpsz6nW2k_116741-1.pdf, accessed on 15.09.2025.
11. Safer Together: A Path to a Fully Prepared Union, https://commission.europa.eu/document/5bb2881f-9e29-42f2-8b77-8739b19d047c_en, accessed on 15.09.2025.
12. A Competitiveness Strategy for Europe, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf, accessed on 15.09.2025.
13. White Paper on European Defence Readiness 2030, https://defence-industry-space.ec.europa.eu/eu-defence-industry/white-paper-future-european-defence-rearming-europe_en, accessed on 15.09.2025.
14. The European Rearmament Plan, https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769566/EPRS_BRI(2025)769566_EN.pdf, accessed on 15.09.2025.
15. EU Strategy on Preparedness for Prevention and Response to Emerging Threats and Crises, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_25_856/IP_25_856_EN.pdf, accessed on 15.09.2025.
16. ProtectEU: an EU Internal Security Strategy (2025), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0148, accessed on 17.09.2025.
17. Directive (EU) 2022/2257 on the resilience of critical entities (CER), https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32022L2557, accessed on 17.09.2025.
18. Directive (EU) 2022/2255 concerning measures for a high common level of cybersecurity across the Union (NIS2), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555, accessed on 17.09.2025.
19. Regulation (EU) 2019/881 on the European Union Agency for Cybersecurity and on cybersecurity certification for information and

communications technology (Cybersecurity Regulation), https://eur-lex.europa.eu/RO/legal-content/summary/the-eu-cybersecurity-act.html, accessed on 17.09.2025.
20. Cyber Solidarity Law, https://ec.europa.eu/newsroom/dae/redirection/document/95049, accessed on 17.09.2025.
21. Redefining Resilience: Concentrated Cyber Risk in a Global Economy (2024), https://library.cyentia.com/report/report_022715.html, accessed on 15.08.2025.
22. The global cyber attack surface represents the physical assets (”endpoint” devices that an attacker could physically access, such as desktop computers, hard drives, laptops, phones/mobile devices, USB sticks) and digital assets (hardware, software, and related components connected to its own network) that an organization owns and that could be compromised, potentially facilitating a cyber attack.
23. Specific type of software intentionally designed to damage or exploit computer systems, networks, and various electronic devices, with the aim of fraudulently demanding a financial ransom from victims, threatening to publish, delete, or block access to personal or non-public data that has been stolen or compromised.
24. Politico (July 9, 2025), There's New Hope for the Euro, but the Dollar Empire Strikes Back, https://www.politico.eu/article/genius-act-donald-trump-euro-dollar-stablecoin/, accessed 23.08.2025.
25. The Stablecoin Bill (GENIUS Act) passed by the US Senate on 06/17/2025 could be followed by a Market structure Bill.
26. World Economic Forum (2025), Navigating the Fragmentation of the Global Financial System, https://reports.weforum.org/docs/WEF_Navigating_Global_Financial_System_Fragmentation_2025.pdf (p.5), taken from Gopinath, G. (June 21, 2024). Navigating fragmentation, conflict, and large shocks. International Monetary Fund. https://www.imf.org/en/News/Articles/2024/06/21/sp062124-fdmd-nbu-nbp-annual-research-conference, accessed on August 23, 2025.
27. Benoît Dupont (2019), The cyber-resilience of financial institutions: A preliminary working paper on significance and applicability of digital resilience, https://globalriskinstitute.org/mp-files/the-cyber-resilience-of-financial-institutions-executive-summary.pdf/, accessed on 17.09.2025.
28. Benoît Dupont, Clifford Shearinga, Marilyne Bernier, Rutger Leukfeldt (2023), The Tensions of Cyber Resilience: From Understanding to Practice, https://www.sciencedirect.com/science/article/pii/S0167404823002821, accessed on 16.09.2025.
29. M. Dunn Cavelty, C. Eriksen, B. Scharte (2023), Increasing cybersecurity resilience: adding social aspects to technological solutions, https://www.tandfonline.com/doi/epdf/10.1080/13669877.2023.2208146?src=getftr&utm_source=sciencedirect_contenthosting&getft_integrator=sciencedirect_contenthosting, accessed on 16.09.2025.
30. Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847, accessed on 17.09.2025.
31. Regulation (EU) 2022/2554 on the digital operational resilience of the financial sector (DORA Regulation), https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32022R2554, accessed on 17.09.2025.
32. Proud, L.P. (2020). Security's Multidimensionality. Societal Security in the Age of Information Technology. In Romanian Military Thinking International Scientific Conference Proceedings. Military Strategy Coordinates under the Circumstances of a Synergistic Approach to Resilience in the Security Field (pp. 78-95). Bucharest: Technical-Editorial Center of the Army.
33. Ponemon Report on the Cost of Internal Risks 2025, https://ponemon.dtexsystems.com/, accessed on 15.09.2025.
34. In the field of public administration, at European level, the concept of a “One Stop Shop” (OSS) has emerged as a transformation approach to create and involve an optimization of government services. By consolidating a wide range of services under a single umbrella, OSS proposes to eliminate bureaucratic obstacles and fragmented interactions that often characterize traditional government structures.
35. ENISA NIS360 2024, ENISA Cybersecurity Maturity and Criticality. NIS Sectors Assessment2, https://www.enisa.europa.eu/publications/enisa-nis360-2024, accessed on 11.08.2025.
36. The EU financial sector includes entities responsible for managing financial transactions, granting credit and maintaining the stability of the European financial system. In the study carried out by ENISA, the financial sector integrates two sub-sectors:
• the banking sector, which includes credit institutions (banks) and
• financial market infrastructures (FMIs) limited to central counterparties and trading venues.
37. European Banking Authority (EBA), European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA)
38. EBA Guidelines on ICT and security risk management, EBA/GL/2019/04, https://www.eba.europa.eu/sites/default/files/docum

ents/10180/2522896/32a28233-12f5-49c8-9bb5-f8744ccb4e92/Final%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf, accessed on 11.08.2025.

39. Guidelines on Information and Communication Technology Security and Governance, https://www.eiopa.europa.eu/publications/guidelines-information-and-communication-technology-security-andgovernance_en, accessed on 11.08.2025.

40. Cyber resilience oversight expectations for financial market infrastructures, https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market _infrastructures.pdf, accessed 11.08.2025.

41. Information Sharing and Analysis Centres (ISACs) developed by ENISA.

42. The European Financial Institute – Information Exchange and Analysis Center (FI-ISAC) is an independent organization that was founded in 2008.

43. The Financial Services Information Sharing and Analysis Center (FS-ISAC) is an industry consortium dedicated to reducing cyber risk in the global financial system, established in 1999 in response to Executive Order 63, signed by President Clinton in 1998, which mandated the public and private sectors to share information about physical and cybersecurity threats and vulnerabilities to help protect U.S. critical infrastructure.

44. ECB concludes cyber resilience stress test, https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240726~06d5776a02.en.html, accessed on 11.08.2025.

45. What is TIBER-EU?, https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html, accessed on 11.08.2025.

46. The EU-CIIS Community is open to members of the Euro Cyber Resilience Board for Pan-European Financial Infrastructures (ECRB), i.e. Pan-European Financial Infrastructures, Central Banks (in their operational capacity), Critical Service Providers, ENISA and EUROPOL. The Third Party Cyber Threat Intelligence Provider is not a member of the EU-CIIS Community itself, but provides services to the EU-CIIS Community members and therefore participates in the information exchange. Thus, the Third Party Cyber Threat Intelligence Provider is a participant in the EU-CIIS, but not a member.

47. EU-SCICF Framework, https://www.eu-scicf.com/Links.html, accessed on 02.09.2025.

48. Adevărul (2022), Cybersecurity, one of the biggest challenges of the present, https://adevarul.ro/stil-de-viata/tehnologie/securitatea-cibernetica-una-dintre-cele-mai-mari-2159016.html, accessed on 16.09.2025.