JSEG

JOURNAL OF SMART ECONOMIC GROWTH

www.jseg.ro ISSN: 2537-141X Volume 7, Number 2, Year 2022

CONSIDERATIONS ON ARTIFICIAL INTELLIGENCE AND CYBERNETIC RISKS, A NEW PARADIGM OF THE BANKING FINANCIAL SYSTEM

Liliana Ciresica Stoica

Craiova University, Romania
Faculty of Economics and Business Administration,
Doctoral School of Economic Sciences,
Domain: Management,

Email address:
lilliana_stoica@yahoo.com

Summary: *The challenge facing the banking system is to identify a creative way to meet customer needs in an innovative way, using Artificial Intelligence while strengthening the security of banks in the face of cyber threats and risk.*

In this paper, we aim to study the overview of artificial intelligence technologies as a result of implementation in the financial-banking system, the opportunities generated by their creation and implementation but especially the consequences of the transformation process generated by the adoption of artificial intelligence and its consequences. generated by it, in the activity of defense and their resistance to possible cyber risks.

Our analysis focuses on the prospects of regulating financial markets, establishing a regulatory and supervisory framework with basic standards that will challenge banks to be more ambitious in their defense and resilience to potential cyber risks.

Keywords: Artificial intelligence, Digital economy, Information technology, Organizational culture - banking system, Code of ethics, Threats, cyber attack, Predictability, Decision-making processes

1. Introduction

Macro-financial developments, as well as endogenous and exogenous shocks, the current situation caused by the war in Ukraine, the coronavirus pandemic, the new international economic policies implemented in recent months have reconfigured the entire banking system generating structural changes at European and global level.

Also, in view of the significant increase in global public debt and in the prevailing context of unconventional monetary policies of central banks, fully implemented to counter possible fragmentation of financial markets and the elimination of exposure to risks on the continuity of the European Monetary Union Monday to an increase in banks' exposure to government debt instruments, the latter reaching record levels.

In this context, the measures implemented and the regulations decided by the Central Banks after the onset of the most severe economic and financial crisis since the end of the Second World War, determined a concentration of the entire financial-banking activity on the prudential component in a context without precedent, characterized by a high degree of exposure and risk. The current analysis contributes to a better understanding and clarification of some important aspects regarding the current situation and the perspectives of the financial-banking system in Romania.

The Romanian banking sector, a key player for resilience and economic recovery, severely affected by the SARS VOC 19 pandemic, when it had to adjust its customer policies through social distancing with a strong impact on its own activities and revenues, proved its resilience to various external and internal shocks, some of significant magnitudes (eg changes in the EUR / USD exchange rate, depreciation of the national currency, SARS VOC 19 pandemic - reduction / limitation of the program with the public, telework, etc.), amid proactive measures adopted by all financial banking institutions, but also in the face of the challenges determined / generated against the background of the war in Ukraine.

The resilience of financial-banking institutions as well as their impact on national and global economies reached a critical level during this period, which led to the emergence of a new culture of learning, so that "resilience plans" are constantly op Increasing the level of resilience is a complicated process in which all entities must work coherently, in a much more coordinated, integrated and prioritized manner. In this context, the strategies for implementing the new business plans were correlated with the financial-banking models and methods following the increase of Artificial Intelligence - AI in order to realize the financial projections.

In the last century there has been an openness and a concern, regarding the combination of conceptual notions with the strategies of development, promotion and technological evolution. In recent years, it has taken on a variety of forms, beginning to become virtually a ubiquitous component of economic and social life - a real set of computer disciplines designed to copy natural intelligence. The term artificial intelligence covers a wide range of fields such as: mathematics, computer science, medicine, biochemistry, aerospace, military, etc. timized according to the evolutionary nature of new risks, regardless of their nature and unforeseen.

The concept of Artificial Intelligence (AI) is no longer new, we already know that artificial intelligence helps us to identify strategies and implementation plans that increase the degree of resilience on several levels. In short: "Artificial intelligence (AI) systems are software (and possibly hardware) designed by humans, which, if given a complex objective, act in the physical or digital dimension, perceiving the environment through data retrieval, interpretation of the structured or unstructured data collected, by reasoning about knowledge or by processing the information obtained from such data and by deciding on the best action (s) to be taken to achieve the given objective. AI systems can either use symbolic rules, or learn a numerical model, and they can also adapt their behavior by analyzing how the environment is affected by their past actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (specific examples of machine learning are deep learning and enhanced learning), machine reasoning (which includes planning, programming, knowledge representation and reasoning, search and optimization). and robotics (which includes control, perception, sensors and actuators, as well as the integration of any other techniques into cyber-physical systems). ”

In this context, any organization that will promote its own moral principles, through the mandatory institutionalization of a highly efficient strategy, implicitly confers the means of a demanding practice of ethics and vice versa, already uses artificial intelligence.

This form of using artificial intelligence (AI) as a central element of the process of digital transformation and at the level of the banking financial system, generates along the value chain, added value for customers, products, services, employees and processes.

In this sense, we will conclude that there is undoubtedly a return on the application / implementation of artificial intelligence subject to ethics at the level of the banking system, which must be perceived as a medium-term and especially long-term investment while challenging banks to defend and their resilience to possible cyber risks and numerous threats such as phishing attacks, brute force, etc.

Artificial intelligence (AI), digital technologies have irreversibly changed people's lives - from the way we communicate to the way we live and work. Digitization has the potential to provide enormous opportunities by providing solutions to many of the challenges we face as it opens the door to cyberattacks and cybercrime that are becoming more and more sophisticated, taking various forms from taking control of devices. personal use of malware, up to the theft and / or compromise of personal data and intellectual property, in order to commit fraud.

2. Cyber risk considerations

At the same time, through the connected devices used by organizations as well as due to the large volume of data (big data) they generate, following the implementation of new artificial intelligence technologies, the premises for the emergence of opportunities and risks are created starting with the implementation, testing and last but not least during use, once they are put into production.

Violation of security regulations can lead to operational loss and / or data loss, and lead to a negative impact on the security, lifecycle costs and reputational risk of the organization. These, both together and individually, can have a significant impact on customer loyalty and implicitly on the final financial results.

As organizations move from traditional to digital, there is an urgent need to protect the availability, integrity and confidentiality of cybersecurity. Threats to cyber security must be viewed and treated with the utmost seriousness and proactively prevented with an approach. defensive at the level of computer system, approach specific to the needs of each organization depending on the field of activity.

We can also say that no method of protection is completely safe because, as we have seen, the effective protection mechanisms applicable today have lost their effectiveness since the next day, they have been obsolete given that, constantly, the means and methods of cyber attacks are changing, performing. This situation requires network controllers of macro control systems to always be alert to changes in cybersecurity and to act to prevent potential vulnerabilities.

Thus, the rapid pace of technological evolution has led to the inclusion of artificial intelligence in the process of securing the digital environment. Both the private and public sectors are interested in understanding and using artificial intelligence for data protection and creating more opportunities to optimize specific activities.

Given the progressive trend, there are a number of cyber security companies that have developed artificial intelligence-based solutions for protection against cyber attacks. Thus, products developed on the basis of artificial intelligence provide the necessary support for cybersecurity specialists in identifying and investigating complex cyber threats.

Assuming that artificial intelligence has the potential to provide the capabilities needed to detect, investigate and mitigate cybersecurity risks, organizations have begun to invest more and more resources in this area to develop solutions based on these technologies in cybersecurity. Thus, blocking, isolating and studying malicious activities with the help of artificial intelligence will require minimal involvement of the human factor.

At present, we can say that cyber risks are no longer a technological
problem, they have become constantly evolving systemic risks for organizations and societies, risks that need to be actively managed. Given the significant increases in remote activity, the need for digitization and the serious vulnerabilities of infrastructure, organizations are more exposed than ever. In order to protect and thrive, they need to reach a higher level of protection than resilience.

Cyber threats affect every field. Every organization, regardless of its business activity, now manages cyber risks. There is no one-size-fits-all answer to this problem: with the advent of new digital transformation technologies, there is an increased area of attack that cybercriminals can penetrate.

Many organizations view cybersecurity as an operational or technological issue and spend more each year on these cybersecurity solutions. However, the scale, frequency and economic impact of cyber events, whether ransomware, supply chain attacks or disruptions, continue to grow. Thus, every organization needs to anticipate cyber risk from the outset of developing a strategy for more effective information and technology risk management, given the significance and potential of the following:

- Cyber strategy involves the development of a cyber risk program in accordance with the strategic objectives and risk appetite of the organization.
- Cyber security involves establishing effective controls over the most sensitive assets of the organization and balancing the need to reduce risks, while improving productivity, increasing business and achieving cost optimization goals.
- Cyber surveillance involves the integration of threat data, IT data and business data to provide security teams with the contextual information needed to proactively detect and manage cyber threats and respond more effectively to cyber incidents.
- Cyber resilience involves combining proven proactive and reactive incident management processes and technologies to adapt quickly and respond to cyber disruptions, either internally or externally.
- Identify fully customizable security solutions, including advanced security event monitoring, threat analysis, cyber threat management, and incident response.

For an easier understanding we will specify that the field of cybersecurity is divided between several different sections / directions / departments, and their coordination within any organization is essential for the successful implementation of a cybersecurity program designed to detect possible threats. :

Malware - the classic virus that facilitates unauthorized access, in order to exploit a file / program or even equipment;

- Ransomware - another type of malware by which the attacker locks by encrypting the system of a computer subsequently requesting a fee for unlocking or decrypting;
- Social engineering - attack based on human interaction aimed at fooling users in violation of security procedures and obtaining sensitive information;
- Phishing - the form of social engineering through which fraudulent emails / text messages are sent for the purpose of stealing sensitive data such as credit card information, or connecting to various payment applications;
- Internal threats - which may be malicious or negligent, caused by employers, contractors or customers and represent serious security breaches;
- Distributed Denial of Service (DDoS) attacks - multiple systems send a large volume of messages with connection requests / packets to a targeted system / server / website / other network source, disrupting traffic which slows down or even system / server crash;
- Advanced Persistent Threats (APT) - through which a hacker infiltrates a network and remains undetected for long periods of time in order to steal sensitive data;
- Man in the middle (MitM) attacks - interception, in which the hacker positions himself between two systems, intercepts and transmits messages between them without the parties involved realizing it.

3. Testing the cyber resilience of financial-banking institutions with TIBER-EU

Financial institutions, attractive targets for attackers, have always been targeted given both access to financial assets and highly sensitive information. Increasing digitalization, online services, mobile applications, social distance, etc., determine the scalability of security tactics, techniques and procedures designed to deal with a threatening landscape that is constantly evolving and rapidly.

In this context, the European Central Bank (ECB) has jointly developed with the EU's national central banks the TIBER-EU framework, whose role is to address exactly this issue. Thus, in order to test the critical live production services of an organization / entity based on current, real-life attack scenarios that specifically relate to the type of activity of the tested organization / entity, the ECB published the TIBER-EU Framework in 2018 , after being approved in advance by the Governing Council of the ECB and being taken over for implementation in several European countries as well as Romania.

Schematically speaking, TIBER-EU is a test in which a special, dedicated team that has information about threats creates a personalized landscape of threats / cyber attacks for the organization that performs the test. Based on this “threat landscape”, the “red” team will perform penetration tests using real-life threat models / methods, as defined by the threat information team. Because the test was designed / developed on the basis of current threats, in real life it will simulate attacks on all critical functions / systems of the underlying systems in the application area, as agreed before the start of the exercise, including people, processes. and technologies.

The TIBER-EU framework tests and improves the cyber resilience of financial institutions by conducting a controlled cyber attack based on real-life threat scenarios, helping tested organizations / entities to understand their capabilities to protect, detect and respond to cyber attacks in scenarios / situations. from real life.

While individual testing is tailored to each organization, the test is conducted on the basis of a standardized framework created by the ECB and applied by each Member State.

The basic objectives of TIBER-EU are:

- Improving the cyber resilience of the entities tested and the financial sector in general
- Standardization and harmonization of the way in which entities perform TIBER-EU tests
- Regulating how authorities could establish, implement and manage this form of testing at national or European level
- Providing support / protocol in cross-border, cross-jurisdictional testing cases, providing information to multinational entities and sharing analysis results.
- Allow further debate on the equivalence of the authorities in terms of surveillance and / or exposure to cyber attacks if they are trying to rely on mutual assessments carried out using TIBER-EU.

The generic landscape of threats will be used later as a basis for conducting TIBER-EU tests have an optional stage and three mandatory phases:

Optional Stage - involves a generic assessment of the “overall national landscape of financial threats”, and includes an overview of all market participants, identifies relevant threat factors, their tactics / techniques and procedures (TTP).

Information report on targeted threats. If possible, the overall threat landscape will be validated and reviewed by national intelligence agencies and continuously updated to reflect any changes in the threat landscape.

Preparation Phase I: This is the phase in which the test entity will determine the teams responsible for conducting the tests and define the scope of the test. The scope will be submitted to the board of the financial institution for approval and validation by the respective regulatory authorities. Both the approval of the board and the validation of the regulations are mandatory in accordance with the TIBER-EU guidelines. Finally, Threat Intelligence and Red Team providers are procured for the TIBER-EU exercise.

Phase II testing: includes the activity of the intelligence provider to create the Targeted Threat Information Report, which the RT (red team) provider will use to create and implement attack scenarios against the entity.

Closing Phase III: The RT provider starts its scenarios, then prepares the Test Report in which it presents its approach, all the observations and findings during the test and finally makes recommendations for improvements. All observations and findings shall be brought to the attention of the Management Board, and the testing entity shall subsequently create a remedial plan in close cooperation with the supervisory authorities.

The TIBER-EU framework is designed for (supra) national authorities and entities that form a basic financial infrastructure, including cross-border ones, whose activities fall within the regulatory remit of several authorities.

This is applicable to all entities not only those in the financial sector, respectively financial-banking institutions, payment institutions, etc. but also those who operate in any other sector / critical field that can benefit from performing this cyber resilience test. In addition to a number of mandatory requirements, the framework also includes a number of options that can be adapted to / on the specifics of different jurisdictions / areas of activity, which facilitates mutual recognition but also reduces the burden on both authorities and entities.

Due to the complexity and multitude of test models / methods designed to achieve the basic objectives, the implementation of the TIBER-EU framework needs to develop new knowledge and skills, with a higher level of national analysis, integrity and flexibility, which will allow it to adapt to depending on the specifics of the financial institutions, of the respective system and structure, to establish the potential errors but also the degree of risk that can be taken at decision level to strengthen the security of banks in the face of cyber threats and attacks.

In the context of cognitive technologies, it is necessary to create a TIBER-EU framework and national / European implementation guidelines designed to build and manage strategies for testing and interconnecting the European financial system, revealing vulnerabilities, successful cyber incidents, leading to increased resilience to reduce the threat to the European financial system as a whole.

4. CONCLUSIONS:

The main objective of TIBER is to test and improve the protection, detection and response capabilities of financial institutions against sophisticated cyber threats, enabling organizations / entities to improve their operational and cyber resilience by raising awareness of strengths and especially weaknesses before real-life threat actors exploit them.

In short, the most significant benefit of TIBER-EU for financial institutions is to check their own vulnerabilities and defense capabilities through a test based on real-life attack scenarios / patterns, requiring personalized reports of information specific to each specific organizations / entities, taking into account the level of critical systems that the organization / entity uses and tests.

Additional benefits for organizations undergoing a TIBER-EU exercise include at least protecting organizations against indirect costs - such as fines imposed by regulators, loss of revenue and / or customer activity, and strengthening the European financial system.

BIBLIOGRAPHY

1. Al-Sanjary, O. I. et al.(2022) 'Challenges on Digital Cyber-Security and Network Forensics: A Survey', Lecture Notes on Data Engineering and Communications Technologies, 127, pp. 524–537. doi: 10.1007/978-3-030-98741-1_43.

2. Aliyu, A., Maglaras, L., et al.(2020) 'A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom', Applied SciencesSwitzerland), 10(10). doi: 10.3390/APP10103660.

3.Aliyu, A., He, Y., et al.(2020) 'Cyber Security Decision Making Informed by Cyber Threat Intelligence (CYDETI) : IEEE CNS 20 Poster', in 2020 IEEE Conference on Communications and Network Security, CNS 2020. doi: 10.1109/CNS48642.2020.9162162.

4.Alshaikh, M. (2020) 'Developing cybersecurity culture to influence employee behavior: A practice perspective', Computers and Security, 98. doi: 10.1016/J.COSE.2020.102003.

5.Annarelli, A. and Palombi, G. (2021) 'Digitalization capabilities for sustainable cyber resilience: a conceptual framework', Sustainability (Switzerland), 13(23). doi: 10.3390/su132313065.

6. Autonomus –May 2018- The Financial Brand

7. Garther Annual Report – 20188.

8. https://enterpriseedges.com/artificial-intellligence-banking-industry

9. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

10. https://thefinancialbrand.com/artificial-intellligence-banking-industry

11.https://universuljuridic.ro/etica-inteligentei-artificiale-premisele-cadrului-legal-pentru-inteligentei-artificiala-o-abordare-europeana-cartea-alba-a-comisiei-europene