ELECTRONIC BANKING SYSTEMS AND SERVICES IN ROMANIA IN THE CONTEXT OF THE WAR BETWEEN THE RUSSIAN FEDERATION AND UKRAINE

Brigadier-general (ret.) professor Viorel BUȚA, Ph.D*
Răzvan MANOLIU, Ph.D**

Abstract: *The war launched by Russia against Ukraine has created major implications for affecting security and stability in that country, but also in the region and, to some e tent, globally. After the end of the Cold War, the Russian-Ukrainian conflict led to various challenges of different natures, namely: military, political, economic, financial, legal, IT and humanitarian.*
Keywords: *conflict, Russia, Ukraine, financial.*

Despite all the negative effects, in the current situation, the European financial architecture shows that the banking sector is resilient, with solid capital and liquidity positions. The Banking Union has contributed significantly to this resilience.

Romania's electronic banking systems and services have experienced significant development in recent years, with a positive impact on the country's economy. These systems and services have become extremely important for commercial transactions and for the Romanian economy in general.

However, the existence of neighboring conflicts and tensions, such as the war between Ukraine and the Russian Federation, allowed the possibility of affecting this financial sector. Under these circumstances, it is important to analyze the current situation of electronic banking systems and services in Romania and to assess the impact of the war between Ukraine and the Russian Federation on them. no more.

Although important measures are taken, Romania is one of the countries vulnerable to cyber attacks from the Russian Federation. One of the most exposed sectors is banking, which has become increasingly dependent on information technology and has rapidly digitized in recent years. In this context, Russian hackers began to use advanced techniques to break the security systems of banks in Romania. This article aims to present some aspects of cyber attacks on banks in Romania, with an emphasis on the activities of Russian hackers as a consequence of Romania's position towards the Russian-Ukrainian war.

* Entitled member of the Romanian Academy of Scientists, email: vbuta49@yahoo.com.
** Unicredit Bank Romania,email: razvanmanoliu@gmail.com

The banking system, like many other sectors, has become increasingly dependent on technology. The digitization of banking operations has led to an increased risk of cyber attacks. As a result of the increased threat of cyber attacks, banks have prioritized cyber security measures to protect themselves from these threats. Romania ranks 38th in the world in terms of banking system assets, but Romania's banking system remains vulnerable to cyber attacks, especially from the Russian Federation. We set out to explore to what extent the banking system in Romania is vulnerable to cyber attacks from Russia intensified in the conditions of the war in our neighborhood.

The banking system in Romania is supervised by the National Bank of Romania (BNR) and consists of commercial banks, savings banks and credit cooperatives. There are approximately 30 banks operating in Romania, of which the first 5 banks hold approximately 70% of the market share. The Romanian banking system has undergone significant changes in recent years, after a period of consolidation and reforms following the global financial crisis of 2008-2009.

Although it is considered one of the most developed and modern in Europe, the banking system in Romania remains vulnerable to cyber attacks. Russian hackers have demonstrated, especially recently, that they are capable of attacking banks in Romania using a combination of sophisticated techniques such as phishing and ransomware attacks.

Cybersecurity is one of the most important issues of today, given the fact that technology and the Internet play an essential role in the global economy and modern society. Romania, like other countries, faces continuous cyber threats, which can affect both the public and private sectors. To deal with these threats, the Romanian state has developed a national cyber security strategy for the period 2019 - 2024, in which the Romanian Association of Banks and TRANSFOND S.A. are two fundamental institutions.

In recent years, Romania has become one of NATO's most important partners in terms of cyber security. The NATO Cyber Security Center of Excellence in Romania plays a vital role in improving Romania's ability to defend itself against cyber threats and in strengthening collaboration with NATO partner organizations and member states.

Electronic banking systems and services in Romania have experienced significant development in recent years, mainly due to the

increase in the use of the Internet and mobile phones. This growth has led banks to improve their services through electronic banking systems and services. Thus, customers have access to a wide range of services, including online banking, e-wallets and mobile applications.

Electronic banking services offer a number of different advantages to customers. For example, these services are available 24/7, customers can check Balance and transact online without having to visit the bank, which saves time and money. Also, these services are safe and convenient, allowing customers to make transactions of any size from anywhere in the world. Of course, these facilities can also attract some vulnerabilities.

The Russian Federation is renowned for its cyber capabilities, being able to carry out sophisticated and coordinated attacks. In recent years, especially during the Russian-Ukrainian war, Russian hackers began targeting banks from some countries considered "unfriendly". In Romania, they executed cyber attacks to gain access to sensitive information and block banking operations. These hackers often use advanced social engineering techniques to breach bank security systems and attempt to gain access to sensitive information such as customer data and financial information.

The Russian Federation has been accused of carrying out cyber attacks against some countries in Europe, for e ample Estonia and Ukraine, given the proximity of the two countries. Romania is also considered to be at risk of cyber attacks from the Russian Federation.

There have been several cases of cyber attacks on banks operating in Romania in recent years. One such case was in 2017, when the National Bank of Romania was the target of a distributed denial of service (DDoS) attack. The attack led to the unavailability of the bank's website for several hours. In 2020, Banca Transilvania, one of the largest banks in Romania, said it was the target of a ransomware attack. Although the bank reported that it was able to contain the attack, it admitted that customer data was compromised

Fortunately, so far, the war between Ukraine and the Russian Federation has not directly affected the electronic banking systems and services in Romania. However, there are some concerns about geopolitical risks and the prospect of a wider conflict that could affect the region's financial stability.

First, the unstable political situation in our region may negatively affect customer confidence in financial institutions and, therefore, in electronic banking services. As it is likely to affect the economy and finances of the region, customers may be more cautious while investing or making payments through e-banking services.

Second, the war between Ukraine and the Russian Federation could lead to restrictive measures and international embargoes that would negatively affect the financial sector. These measures would lead some financial institutions to reduce their exposure to this region or restrict their services if the situation becomes increasingly tense.

In addition to the geopolitical risks that affect them, the financial sector in Romania can also be subject to other cyber threats. In this sense, the Romanian authorities and financial institutions have strengthened their cyber security measures to protect electronic banking systems and services.

This involved strengthening digital infrastructures by increasing the security level of electronic banking and communication networks. Additionally, additional user authentication and transaction verification measures have been introduced to minimize the risk of cyber fraud.

There have been several cyber attacks on banks in Romania in recent years, and most have been attributed to Russian hackers. The sole purpose of these attacks was to obtain information and disrupt banking operations. In a few cases, hackers were able to gain access to sensitive information such as customer accounts and passwords, while in other cases the attacks were limited to the temporary unavailability of bank websites. Furthermore, Russian hackers have been able to create highly sophisticated malware to try to break bank security systems.

The Romanian banking system has taken various measures to protect itself against cyber attacks. The NBR has issued directives for banks to improve their cyber security posture. These directives include requirements for banks to have adequate cyber security policies and procedures, to conduct regular security assessments and to train employees on cyber security. The NBR also requires banks to comply with the European Union's General Data Protection Regulation (GDPR).

Individual banks operating in Romania have also invested in cyber security measures. For example, Banca Transilvania has a solid cyber security program. The bank has established threat intelligence capabilities and implemented a security operations center to monitor and respond to

security incidents. In addition, the bank provides ongoing cybersecurity training for its employees.

The Romanian Association of Banks (ARB) is one of the most important organizations in the Romanian banking system, representing the interests and needs of member banks. In the fight against cyber threats, ARB plays a critical role by providing advice and guidance to banks so that they can improve their cyber security systems.

As part of the national cyber security strategy, ARB is involved in identifying and assessing cyber risks for banks, developing and implementing cyber security policies and measures, and improving cooperation with relevant authorities to identify and prevent illegal activities.

TRANSFOND S.A. is a publicly owned company that administers the national electronic payment system in Romania. As a fundamental institution, TRANSFOND S.A. plays an important role in protecting the critical infrastructure of the electronic payment system against cyber threats. TRANSFOND S.A. is responsible for the development and implementation of cyber security policies and measures for the electronic payment system in Romania. These measures include improving infrastructure security, detecting and responding appropriately to cyber security incidents, and improving incident management.

Within the national cyber security strategy, the collaboration between ARB and TRANSFOND S.A. is essential so that financial institutions and the critical infrastructure of the electronic payments system in Romania can be protected.

ARB has an important consulting role for banks, while TRANSFOND S.A. is responsible for the security of the critical infrastructure of the electronic payment system. Collaboration between the two institutions is essential to improve the security of the financial system and to prevent increasingly sophisticated cyber attacks.

ARB and TRANSFOND S.A. are two key institutions in the national cyber security strategy, playing a key role in protecting financial institutions and the critical infrastructure of the electronic payment system. Together with other institutions and the private sector, they must continue to take proactive measures to identify and prevent cyber threats and to improve the cyber security of Romania and especially the banking sector.

In addition to ARB and TRANSFOND S.A., several institutions are involved in the national cyber security strategy, such as the Government of Romania, the Ministry of Internal Affairs, the Ministry of National Defense and the National Council for Cyber Security.

These institutions each have an important role in addressing cyber threats in Romania, by assessing risks, developing and implementing cyber security policies and measures, and improving cooperation between sectors.

To protect themselves against cyber attacks, banks in Romania have started to take measures such as investing in security technologies, improved cyber security policies and procedures, and stricter user verification and authentication processes. In addition, the National Bank of Romania has issued strict directives regarding the cyber security of banks, which must be respected by all financial institutions in the country. By working together and taking proactive cyber security measures, banks in Romania have prevented many of the cyber attacks that have occurred so far and can limit their financial and reputational losses.

Cyber attacks by Russian hackers are a major threat to banks in Romania. These attacks can cause significant data and information loss as well as significant financial losses. Despite these threats, banks in Romania have started to take proactive cybersecurity measures to protect themselves against attacks. It is very important that banks in Romania continue to improve and update their security systems and policies and collaborate with the relevant authorities to identify and prevent possible cyber threats.

While the Romanian banking system is vulnerable to cyber attacks, there are safeguards against such attacks. However, the threat of cyber attacks from the Russian Federation remains, and it is essential that Romania continues to prioritize cyber security to protect the banking system.

The NATO Center of Excellence for Cyber Security was established in 2010 as part of an effort to enhance the capacity of NATO and member states to protect national infrastructures and other critical systems against cyber threats.

Romania was selected to host this center due to its strategic geographic positioning and its ability to develop advanced skills in the field of information and communication technology.

The NATO Center of Excellence for cyber security aims to improve the cyber defense capacity of Romania and other NATO partner countries, through cooperation and collaboration in the field of cyber security.

In pursuit of its objective, the NATO Cyber Security Center of Excellence has developed a number of projects and activities, which include:

- Organization of training courses in the field of cyber security for military and civilian personnel from NATO and partner states;
- Elaboration and development of protocols and procedures in the field of cyber security;
- Participation in cyber attack simulation exercises within NATO and at the national level;
- Provision of consultancy and technical support in the field of cyber security for national authorities and private sector organizations;
- Development of advanced tools and technologies for monitoring and detecting cyber threats.

In addition to its own activities, the NATO Cyber Security Center of Excellence collaborates closely with other NATO organizations and Member States to improve synergy and develop advanced cyber security capabilities. Examples of such collaborations include:

- Participation in projects and activities organized by other NATO Centers of Excellence, as well as by the North Atlantic Alliance;
- Coordination of activities with the national Centers of Excellence in NATO member states;
- Cooperation with EU organizations and the states that are part of it, in terms of cyber security;
- Providing support and advice to national authorities and private sector organizations in partner states.

The NATO Center of Excellence for Cyber Security has had a significant impact on Romania's cyber defense capability, especially in terms of the training and education of specialists in the field. In addition, the NATO Cyber Security Center of Excellence has opened up new opportunities for the Romanian IT sector to develop and expand its value in cyber security.

The NATO Cyber Security Center of Excellence in Romania is a vital strategic partnership for NATO and its member states in protecting

national infrastructure and other critical systems against cyber threats. The Center's activities are essential for developing advanced capabilities and strengthening collaboration among nations in the field of cyber security. It is important to maintain and develop this collaboration to protect national security and promote a secure and prosperous digital world.

As a result of the war started by the Russian Federation against Ukraine, the European Union (EU) adopted, among others, the following measures:

-banned transactions with the Central Bank of Russia;

-banned access to SWIFT for seven Russian banks;

-banned the supply of euro banknotes to Russia.

Also, other countries, outside the EU, have undertaken financial-banking sanctions. For example, Switzerland, a neutral state, froze the assets of Russian oligarchs worth 7.5 billion Swiss francs.

In conclusion, electronic banking systems and services in Romania have had a significant development in recent years, being essential for the country's economy and, in general, for carrying out commercial transactions. However, there are geopolitical risks that could affect the financial stability of the region, especially in the context of the war between Ukraine and the Russian Federation.

However, Romanian financial authorities and financial institutions have taken steps to protect electronic banking systems and services by strengthening infrastructure and improving cyber security. Thus, Romania is prepared to face threats or risks, as they appear.

BIBLIOGRAPHY

"Six Romanian banks, including the largest, were the target of a cyber attack by Russian hackers", available at HotNews.ro, May 6, 2021;

"Cyber risks for the financial and banking sectors in Romania", available at CERT.ro, January 24, 2018;

"The government adopted the national cyber security strategy 2019-2024", Ministry of Communications and Information Society, June 18, 2019;

"Security recommendations for online banking and financial services", available at CERT.ro, January 30, 2020;

"Romania in the context of European cyber security", Institute of Political Studies and International Relations, University of Bucharest, 2018;

"The banking system in Romania, vulnerable to cyber attacks", Bloomberg Businessweek Romania, April 23, 2019;

"NATO launches a center of excellence for cyber security in Bucharest", NATO, September 18, 2018;

"Romanian banks, on alert! Russian hackers attacked the computer systems of several financial institutions in Romania", Antena 3, May 6, 2021;

"Cyber security, a priority for the NBR", National Bank of Romania, October 17, 2019;

"Banks must protect their customers and take cyber security measures", Wall-Street.ro, January 19, 2021.