The New Challenges of Romania's Cyber Security Policy

Ioana PETCU, Dragoş-Cătălin BARBU
National Institute for Research & Development in Informatics - ICI Bucharest
ioana.petcu@ici.ro, dragos.barbu@ici.ro

Abstract: The 21st century has presented us with not easy challenges for society. The global security strategy has entered a new era following the September 2001 attack on the World Trade Center. Breaking the real estate bubble in 2008 caused massive losses for international banks and investors, leading to a severe financial crisis and an impending recession. The Arab Spring was marked by demonstrations in the Islamic world in the early 2010s. The refugee crisis followed as millions of people migrated from the Middle East to Europe. A new challenge came at the end of 2019 when a contagious virus triggered the Covid-19 pandemic leading to a global health crisis. When we thought that everything was back to normal, the appearance of the military conflict on the borders of Romania led to the deepening of the energy and food crisis, creating premises for the beginning of a new economic recession. This international context has led to new challenges for Romania, and paradigm shifts in EU security policies and strategies have created favorable conditions for updating the legislative framework on national defense policies, including the approval of Romania's new Cyber Security Strategy.

Keywords: Cybersecurity Strategy, Financial Crisis, Energy Crisis, Hybrid War, Awareness, Threats, Vulnerability, Capability, Cyberattacks, Hacking, Resilience, Network, Ransomware, Malware, Rules and Regulations, Distributed Denial of Service, Defacement, Digital Transformation

INTRODUCTION
THE NEW PARADIGM OF CYBERSPACE

In today's international context, the second decade of the 21st century brings us new challenges posed by socio-economic and geopolitical crises. If two years ago we were facing an unknown virus that has generated a health crisis, starting with February of this year we are facing another crisis generated by the military conflict near Romania's borders. The refugee crisis, the food crisis or the energy crisis complete the overall picture of 2022, which could lead to an economic recession.

But threats come not only from the sea, ground field, airspace or cosmic space, but also from the fifth element, cyberspace, which has recently become the new field of operations, amplifying the risks and threats to the economy, and especially on critical infrastructure (Fig. 1).

http://doi.org/10.54851/v4i1y202207

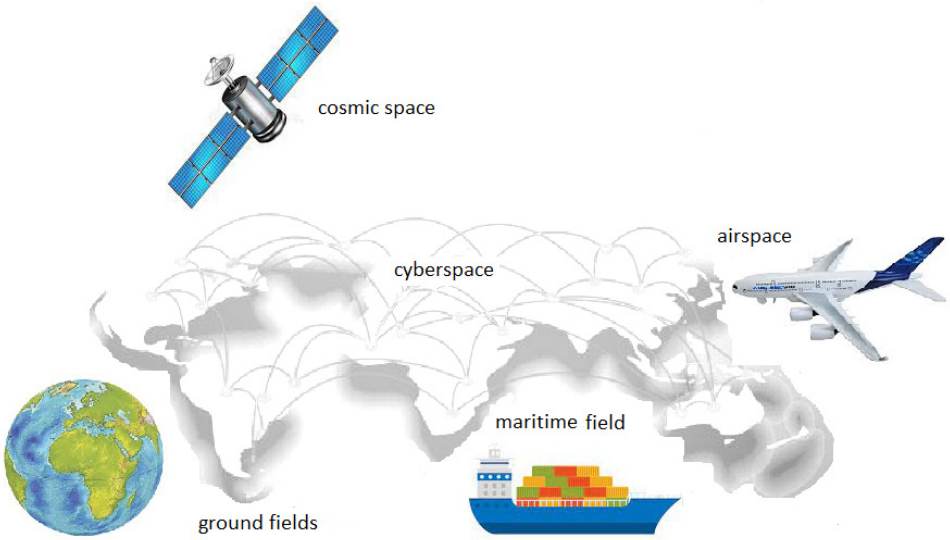

Fig. 1: *The map with field of operations*

Features of this new operational field, the cybernetic field, include remote erosion (oceans no longer provide protection), interaction speed (much faster than space rockets), low cost (which reduces entry barriers), and difficulty assignment (which promotes denial and which slows down the answers).

However, skeptics refer to cyberattacks as more of a nuisance than a major strategic issue. They argue that cyberspace is ideal for espionage and other disruptive forms of undercover action, but that it remains far less important than traditional areas of war; no one died in a cyber attack.

Allianz Risk Barometer, with the contribution of experts from countries on all continents, conducted an annual survey for 2022 and compiled a ranking of the most important risks that will affect countries and their economies. Thus, almost half of the experts claim that cyber attacks will be the most common risks, thus overcoming natural disasters, climate change or pandemics. The results of this study published by Statista are presented in Fig. 2.

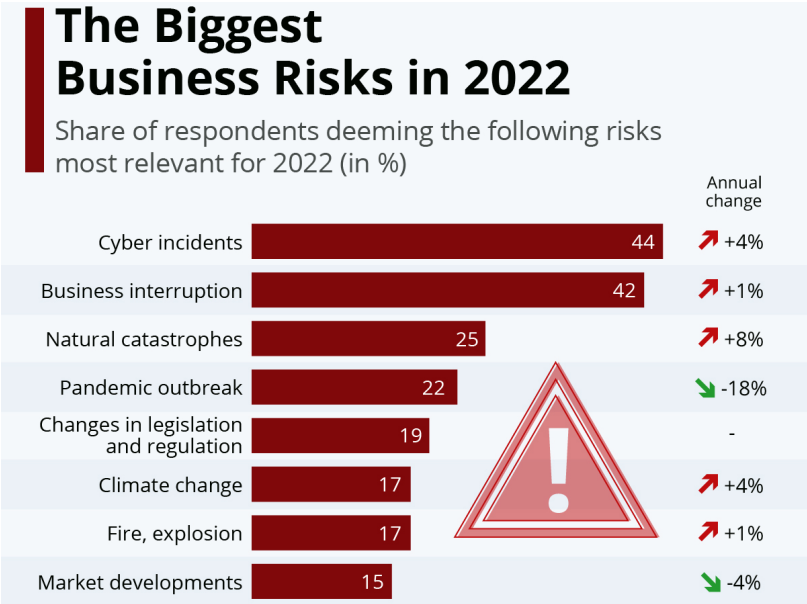

Fig. 2: *The most relevant business risk in 2022 (Statista, 2022)*

Ransomware attacks, the influence of electronic voting results in presidential elections, industrial espionage, threats to the national power system or attacks to banks or government agencies have caused huge damage, and action has been needed to clean up order to cyberspace anarchy. Cybersecurity authorities have agreed that measures are needed to bring new rules and regulations into created cyberspace anarchy. The bad news is that we have the image of an ungovernable online world, which is becoming more and more dangerous every day, with negative implications not only for cyberspace itself, but also for the country's economy, democracy, geopolitics, basic elements in uncertainty created to border between peace and war.

During the COVID-19 pandemic, hackers' favorite targets were national public health services through ransomware attacks. Hospitals and vaccine manufacturers have been targeted directly, computer data has been encrypted and rendered unusable, and thousands of patients have been forced to cancel their appointments.

In March 2022 we saw that the use of cyber tools and cyber attacks could escalate into military physical conflicts. It is well known that the military is heavily dependent on civilian infrastructure and that cyber penetration can severely degrade defensive capabilities in a crisis situation. Also from an economic point of view, the magnitude and cost of cyber incidents have increased exponentially in recent times.

Every day we see that the number of cyber attacks increases at an exponential rate due to the increasing use of IoT, Big Data, AI or machine learning. Cybersecurity experts estimate that the number of internet connections will be close to one trillion by 2030. The world has suffered cyber attacks since the 1980s, but the attack has expanded dramatically, from industrial control systems to autonomous cars or personal digital assistants.

If this not-so-optimistic reality is taken into account, the development of rules and the emergence of a new order for cyberspace may be viewed with skepticism because the very nature and essential attributes of cyberspace make it impossible to enforce rules and regulations.

INTERNATIONAL CYBERSECURITY POLICIES AND REGULATIONS

Violations of cybersecurity rules can be weakened if they are not taken into account, but they cannot be irrelevant. These rules create expectations about cyber behavior and help legitimize official actions when they come in response to a violation of the rules. Regulations do not appear suddenly and do not start to work so easily. Throughout history, we have seen that companies need time to learn how to respond to major disruptive technological changes and to implement rules that make the world safer from the new dangers of technology and digitalization. As cybersecurity rules and regulations come into force, certain voices will become increasingly important to reduce the risk of technological progress and digital transformation.

United Nations have introduced for the first time a set of 11 international cyber rules that are voluntary and non-binding. For Europe, ENISA is a union agency dedicated to achieving a high common level of cybersecurity. As part of the European cyber security strategy, the NIS Directive (EU 2016/1148) was adopted in 2016. The purpose of this Directive is to improve and provide legal measures to increase the overall level of cyber security in the countries of the European Union.

The main components of the NIS directive are:

- National capabilities;
- Cross-border collaboration;
- National supervision of critical sectors (energy, transport, water, health, digital infrastructure and finance sector) & critical digital service providers (online market places, cloud and online search engines).

In December 2020, the European Commission proposed an update of NIS Directive (NIS2) to replace the old one, which responds to the evolution of new threats and takes into account the digital transformation, which has been accelerated by the COVID-19 pandemic crisis. NIS2 will strengthen security obligations for

businesses, address security of supply chains, introduce stricter surveillance measures for national authorities and further intensify information exchange and cooperation.

In March 2021, the EU Council adopted conclusions on the Cyber Security Strategy, highlighting the important role that cybersecurity plays in achieving a resilient, green and digital Europe.

We will notice that the countries that have shown their openness to establish norms and regulations in the cyberspace, carry out in parallel cyber attacks against their opponents.

In order to see how cyber attacks have evolved in recent years, we will present 3 studies published by Statista. Thus, the first study conducted by a software company in 2019 shows us which of the EU countries are the most susceptible and the least susceptible to cybercrime. The study was conducted using the analysis of a total number of attacks received from cloud providers, as well as meetings of mining cryptocurrencies, malware and ransomware on cars in each country. (Fig. 3.)

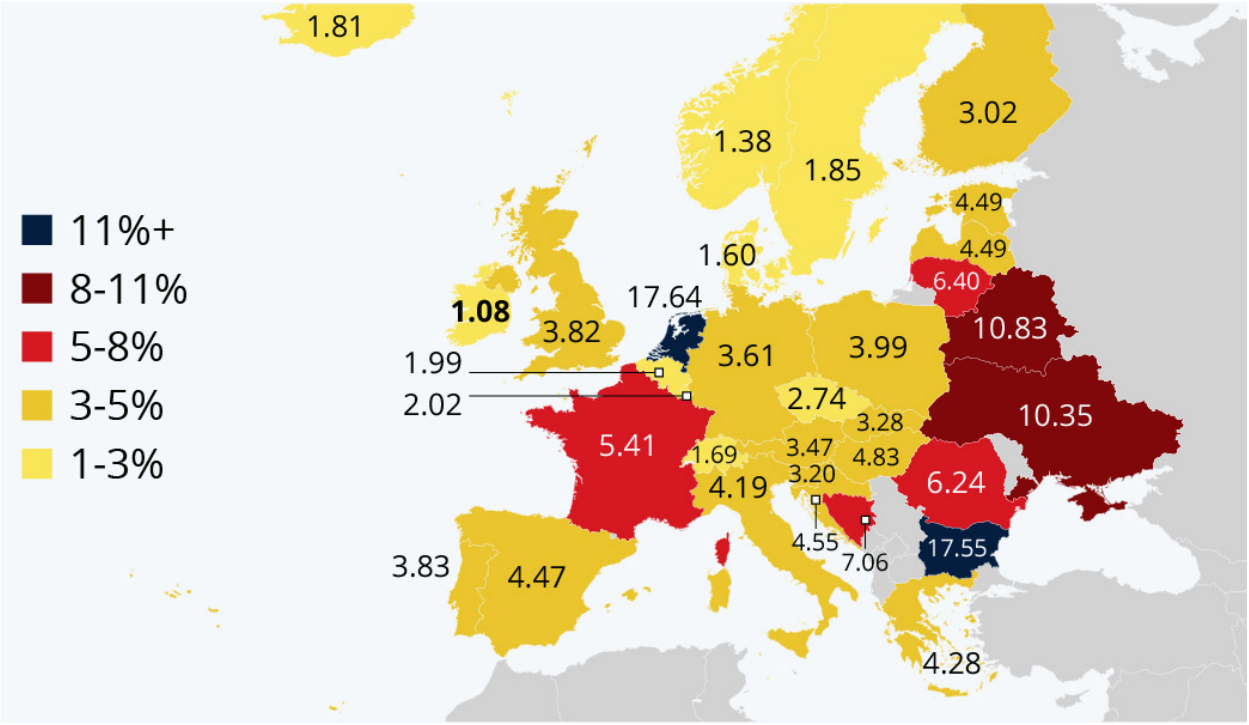

Fig. 3: *Cybercrime: Europe's Most & Least Secure Countries (Specops Software, 2019)*

The cyber attacks are becoming more complex, targeted, widespread and undetected. ENISA's Annual Report shows that the first 15 cyber threats we face in 2020 have been (see Fig. 4):

- Malware;
- Web-based Attacks;
- Phishing;
- Web Application Attacks;
- SPAM;
- DDoS;
- Identity Theft;
- Data Breach;
- Insider Threat;
- Botnets;
- Physical Manipulation;
- Damage, Theft, and Loss, Information Leakage;
- Ransomware;
- Cyber Espionage;
- Cryptojacking.

Fig. 4: *ENISA Threat Landscape – 15 Top Threats in 2020 (Enisa, 2020)*

Compared to 2020, in the context of the COVID-19 pandemic and the acceleration of the road to digitalization, the annual report for 2021 shows a slightly modified ranking. Thus on the first 7 places we have (see Fig. 5):

- Ransomware;
- Malware;
- Cryptojacking;
- E-mail related threats;
- Threats against data;
- Threats against availability and integrity;
- Disinformation – misinformation;
- Non-malicious threats;
- Supply-chain attacks.

Fig. 5: *ENISA Threat Landscape 2021 – Prime threats (Enisa, 2021)*

There are sites and applications that show us the map of cyber attacks in real time. Thus, on the Imperva website, we found for our country a series of statistics resulting from the analysis of cyber attacks at the level of a day.

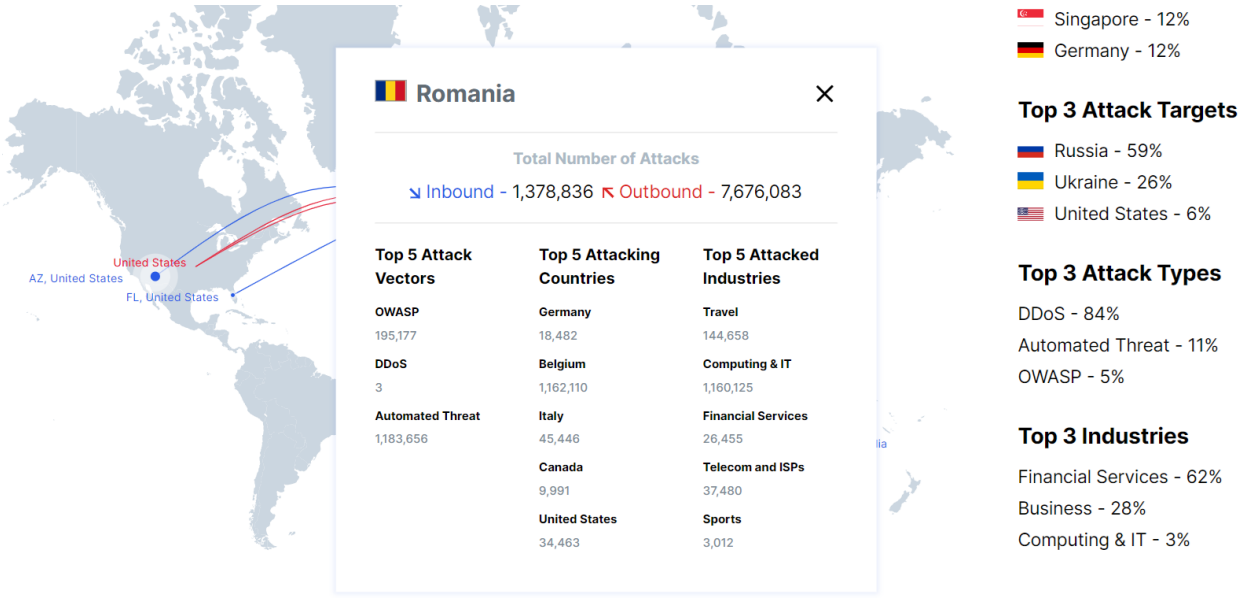

Fig. 6: *Total number of attack for Romania in March 2022 (Imperva, 2022)*

ROMANIAN GENERAL CONTEXT OF CYBER SECURITY

In the current context full of challenges from hackers that may threaten national security, Romania is facing a series of attacks in cyberspace, targeting the computer network vulnerabilities of strategic entities, such as those in the financial-banking sectors, transport, telecommunications, energy, or national defense.

The rapid adoption of digital technology has led to an increase in the influence of digital technology through awareness and the need to adapt to the new trend of digital transformation.

As cyberattacks have become more and more complex, Romania's strategy to defend itself against them must be updated to the new attacks and use new specific resources. A good strategy must have its roots in legislation, but at the same time recognize the inseparability of the domestic and international aspects of cyberspace - the field of cyberspace being essentially transnational. In addition, cyber security involves a blurring of both public and private vulnerabilities. The Internet is a network of networks, most of which are privately owned, and unlike conventional or unconventional weapons, governments cannot control this huge network. As a result, companies are making their own trade-offs between investing in cybersecurity and maximizing short-term profits. However, inadequate defense can have huge external costs for national security.

In order to have a more accurate picture of what a cyber attack on an essential service means, we will briefly present what happened at the beginning of this month (March 2022) in Romania, when we witnessed a cyber attack on the company's servers Rompetrol. This cyber attack was confirmed by the National Security Directorate (DNSC). The name Orange also appeared in the media space, the latter denying this information, stating that Telekom Romania Communications (TKR) is not associated with this attack, because it only offers Rompetrol

colocation services, respectively a physical space in a data center, dedicated exclusively to the client. TKR does not manage the servers and does not provide cyber security services for this Rompetrol, being important to mention the fact that there is no risk of spreading the attack to other servers in the data center, these being isolated both physically and digitally. In order to protect the data, the company temporarily suspended the operation of the Fill & Go sites and service, both for fleets and for individuals, and the activity of Rompetrol gas stations is carried out normally, as well as the operational activity of the Petromidia refinery which was not affected.

Lately, especially in the context of military conflicts and the energy crisis, cyber attacks on critical infrastructures (national electricity, gas, oil, water networks) have become more frequent and sophisticated.

The year 2021 was marked by the predilection of hackers for ransomware and infostealer attacks. These applications offer financial benefits to attackers either by paying ransom to having access to their own data, in the case of ransomware, or by selling stolen data on cybercrime forums, in the case of infostealer. Trojan applications have registered a large number of distributions in public institutions in Romania and the most common malware applications (DNSC, 2022):

- ransomware 35.03%;
- infostealer 28.95% ;
- trojan 20.67%;
- downloader 5.93%;
- backdoor 4.36%;
- exploit 4.23%;
- worm 0.83% for critical infrastructure.

For the distribution of these applications, the cyber actors carried out mainly phishing campaigns, being registered an average of 3813 phishing e-mails in the first half of 2021 as reflected in Fig. 7.

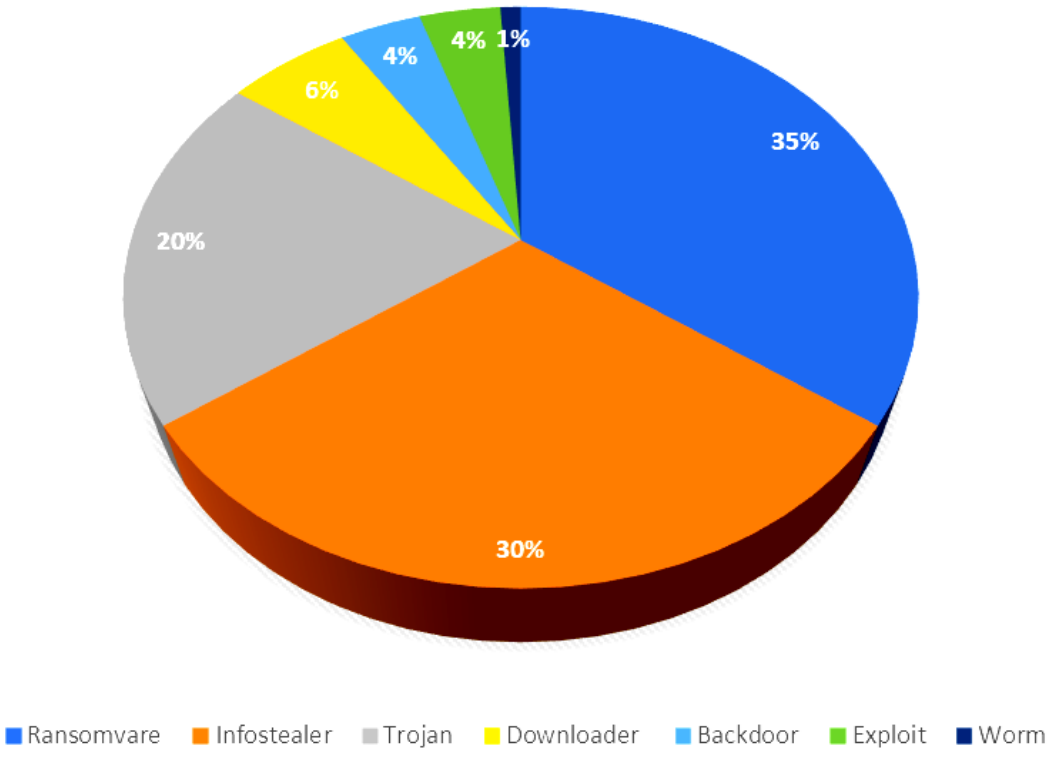

Fig.7: *Malware attacks on public institutions in Romania reported in 2021 (DNSC, 2022)*

ROMANIA'S NEW CYBER SECURITY STRATEGY 2.0

Cyber security of networks and information systems in key areas is a priority for Romania. Maintaining the availability, continuity and integrity in optimal parameters and ensuring their resilience, through cyber security policies and measures, contributes to the support in optimal conditions of all areas of economic and social life.

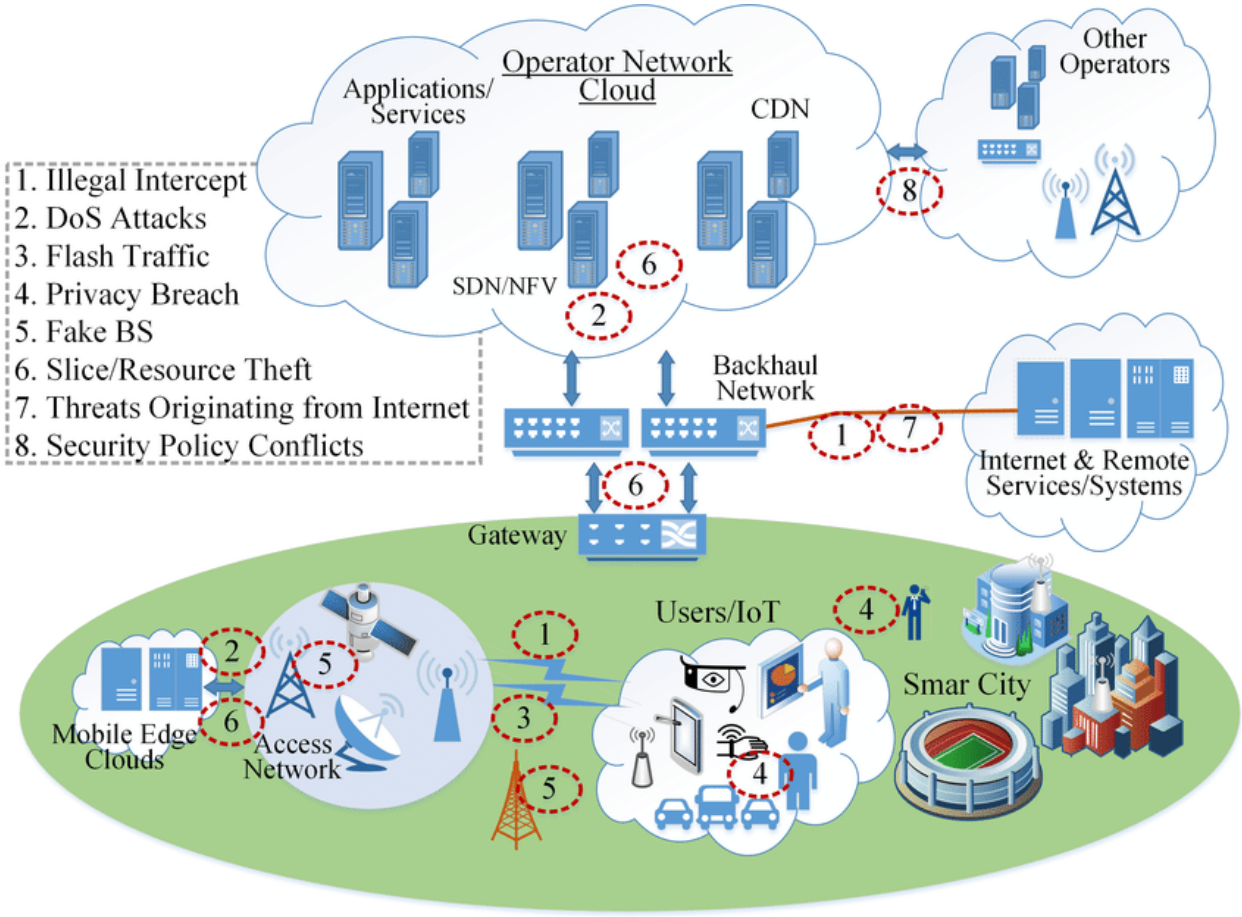

Fig. 8: *Security-threat-landscape-in-5G-networks*
(ResearchGate, n.d.)

Secure cyberspace is the responsibility of the state, through the competent authorities. Secure cyberspace is also the responsibility of the private sector and civil society. This strengthens the public-private partnership to ensure a global, open, and secure cyberspace.

At the end of last year, the Romanian Government approved the New Cyber Security Strategy of Romania 2.0 for the period 2022 - 2027, and on January 3, 2022, it was published in the Official Gazette. The goal of this document is to create the legislative context ensuring a high level of cybersecurity, aligned to the new challenges posed by cyber threats.

The vision of the Cyber Security Strategy is that, in the face of an increasingly complex cyber threat, Romania will be able to prevent, deter and respond effectively, including through a proactive approach, to hostile cyber actions against cyber targets on the territory of Romania or of the strategic allies.

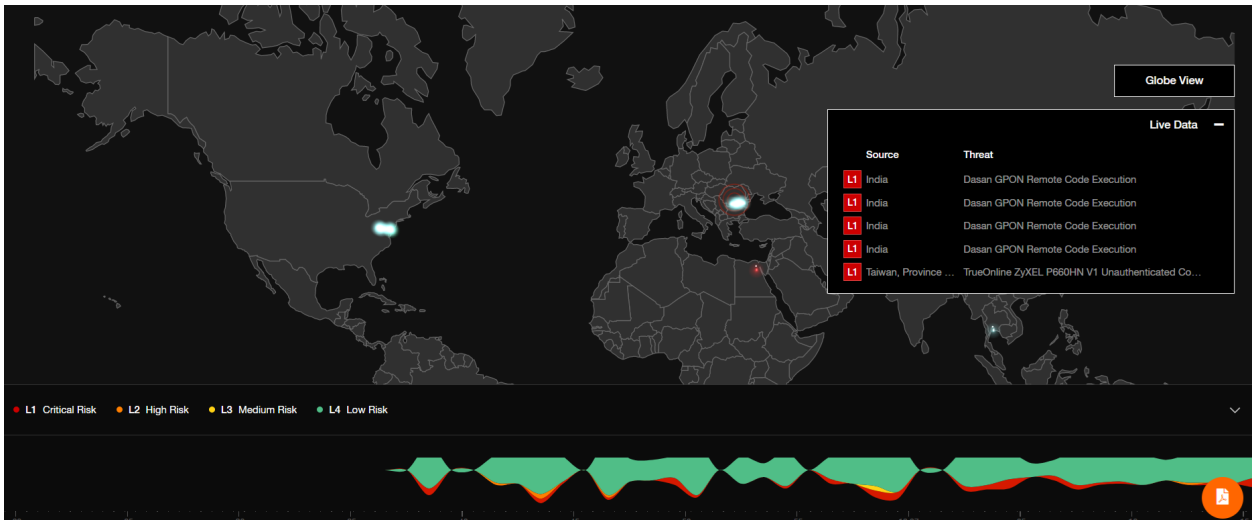

Fig 9. *– The real time cyberthreats analytics*
(Business Internet Security - Orange, n. d.)

The main directions to be followed in order to ensure Romania's cyber security are:

- Cyber security is an integral part of national security, being the responsibility of everyone from citizens to institutions in both the public and private sectors. Given that cyber attacks target computer networks and systems in Romania, this automatically means that those with an impact on national security are also targeted. Cyber security risk management must become an integral part of the organizational specifics of each entity. A key element in strengthening the coherence of the resilience of national networks and information systems is the sharing of information on cyber security risks, threats, vulnerabilities or solutions, both at the inter-institutional level and in the public-private partnership (Strategia, 2021).
- Cyber security supports the functioning of the state and society as a whole, increasing the competitiveness of the national economy, developing national research and development and innovation capabilities. It is known that the support of research, innovation and development initiatives in the field of cyber security, are opportunities to increase the competitiveness of the national economy and to recover economic gaps compared to other states, to create and maintain in Romania a highly specialized human resource in the field of cyber security, as well as increasing national research and development and innovation capabilities.
- Cyber security is based on establishing an appropriate regulatory framework by constantly updating and adapting, based on the European acquis and taking into account Romania's obligations, taking into account the constant evolution of technology and regulations at the international level (Strategia, 2021).
- Cyber security is strengthened through the cooperation of all actors involved at national, European and international level. Romania must continue to play an active and relevant role in major international structures and initiatives related to actions in the field of digital and cyber security and to strengthen its position as a center of excellence and relevant player for European and international cyber security (Strategia, 2021).
- In order to ensure cybersecurity, the maintenance of an open, free, stable and secure cyberspace is guaranteed, with the full application of human rights and fundamental freedoms and the rule of law, as well as the protection of individual freedoms and personal data. Ensuring cybersecurity requires

the application of the same rules and values in both cyberspace and physical space and must be based on respect for, promotion and protection of the exercise of human rights and fundamental freedoms, in particular as regards freedom of opinion, freedom of expression, the right to access and receive information, as well as the protection of personal data and the right to privacy, both online and offline. Particular attention will be paid by Romania to the EU-wide debates on the "digital environment and human rights" and "artificial intelligence and human rights" (Strategia, 2021).

CONCLUSIONS

It has been shown that in the current context of national security challenges, Romania is facing threats from cyberspace, targeting the IT network of strategic entities, such as the financial-banking, transport, telecommunications, energy, or national defense sectors. Maintaining cyber security in optimal parameters of availability, continuity, integrity, and resilience, through cyber security policies and measures is a priority for Romania.

By implementing Romania's new cybersecurity strategy, a high level of cybersecurity is ensured, adapted to the new challenges presented by the hostile entities in the cyberspace.

The existence of a set of policies and measures aimed at cyber security requires them to be constantly updated and correlated with the level of cyber threats and the rapid trend of technology development, including those from the IoT and AI area.

The rapid adoption of digital technology has led to an increase in the influence of digital technology through awareness and the need to adapt to the new context of digital transformation.

REFERENCE LIST

Albescu, A. R. & Perețeanu, G. C. (2019). Cultura de securitate cibernetică în România, *Romanian Journal of Information Technology and Automatic Control, 29*(4), 75-84.

Allianz Risk Barometer, Statista (2022). *The Biggest Business Risks in 2022*. Available at <https://www.statista.com/chart/26631/most-relevant-business-risks-in-2022/>.

Barbu D. C., Sipica A. & Candet I. (2019). Aspecte privind securitatea la nivelul SLA în serviciile de Cloud computing, *Revista Română de Informatică şi Automatică, 29*(3), 31-40.

Business Internet Security - Orange (n. d.). *Real-Time Cyberthreats Map*. Available at: < https://bis-threatmap.orange.ro/>.

Curtea de Conturi Europeană (2019). *Provocări pentru o politică eficace a UE în domeniul securității cibernetice, Document de informare*. Available at <https://eca.europa.eu>.

DNSC - Directoratul Naţional de Securitate Cibernetică (2022). Available at <www.dnsc.ro>.

ENISA Threat Landscape 2020 Report (2020). *European Union Agency for Cyber Security*. Available at <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape-2020-top-15-threats>.

ENISA Threat Landscape 2021 Report (2021). *European Union Agency for Cyber Security*. Available at <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>.

Mihai, I. C., Ciuchi, C. & Petrică (2018). *Provocări actuale în domeniul securității cibernetice – impact și contribuția României în domeniu*. Institutul European din România.

Minchev, Z. (2020). Digital Transformation - An Extended Future Outlook for the Balkans Region, *Romanian Cyber Security Journal, 2*(2), 39-48.

Petcu, I., Candet, I. B., Ştefănescu, C., Gruia, C. I. & Craioveanu, V. (2021). Security Risks of Cloud Computing Services from the New Cybernetics' Threats Perspective, *Romanian Cyber Security Journal, 3*(1), 89-97.

ResearchGate (n. d.). *Fig 4 - uploaded by Ijaz Ahmad*. Available at: < https://www.researchgate.net/figure/Security-threat-landscape-in-5G-networks_fig4_332970813>.

SDF (2020). *Securing Digital Future 21 Web Forum*. Available at <http://securedfuture21.org>.

Specops Software (2019). *Cybercrime: Europe's Most & Least Secure Countries*. Available at <https://www.statista.com/chart/20914/share-of-european-computers-that-experienced-cyberattacks/>.

Romanian Government (2021) *New Cyber Security Strategy of Romania 2.0 for the period 2022 - 2027.* Annex 1 at GD, published in O.M. no. 2 bis from 3.01.2022. Available at: <https://legislatie.just.ro/Public/DetaliiDocumentAfis/250235 >.

Smolenov, H. (2016). *Sharing Genius with the Universe. The Light-Second Code & the Golden Ratio*.

Tagarev, T. (2020). Cyber Protection of Critical Infrastructures, Novel Big Data and Artificial Intelligence Solutions, *Information & Security: An International Journal, 47*(1), 7-10.

Vevera, V. A. & Albescu, A. R. (2018). Factorul uman vs. securitatea cibernetică, *Romanian Journal of Information Technology and Automatic Control, 28*(4), 67-74.

Vevera, A. V., Cîrnu, C. E. & Georgescu, A. (2021). Construction 4.0 – a New Cybersecurity Paradigm, *Romanian Cyber Security Journal, 3*(2), 89-96.