THE IMPACT OF DIGITALIZATION ON NATIONAL SECURITY

PhD Student, Laurentiu-Eduard ION
"Valahia" University of Targoviște, Romania
Email: laurentiu.ion1992@yahoo.com

Abstract: *While digitalization considerably increases the risk of cyberattacks on the country's key infrastructures, it also offers novel solutions for detecting and responding as quickly as possible to threats, solutions for efficient cooperation between states, in order to help each other in critical situations and prevent cross-border attacks. Using the case study method, we identified and analyzed a major cyberattack against Romania in 2015, attributed to the Advanced Persistent Threat 28 group, also known as Fancy Bear/Sofacy, which aimed to obtain sensitive information and destabilize certain economic and political sectors of the country, among others. However, in situations such as the one mentioned above, the benefits of Romania's close collaboration with NATO and the European Union come to light, which provides support especially when it comes to an ATP-type attack, as is the case in this case. In recent years, this Romania-NATO alliance has been strengthened precisely because of the rapid evolution and diversity of risks to which we are exposed in the context of digitalization, which is why Romania is actively involved, participating in cyber attack simulation exercises, precisely out of the desire to prevent and limit their number. The digital age, viewed from the perspective of maintaining national order and security, can be considered both a threat and an opportunity, it depends on which angle we look at and which side we let weigh more. A decisive element is the state's position in the face of challenges and the degree of awareness of the dangers, as long as the government adopts innovative and effective protection strategies, appropriate to the context, the degree of national security is at least satisfactory.*

Keywords: *cyberattack, digitalization, cooperation, Advanced Persistent Threat, national security.*
JEL Classification: *F52, H56, O33.*

1. Introduction

The technological transformations of the last decades have led to a profound digitalization of society, with direct effects on all social areas. This transition has created not only opportunities, but also significant risks, especially in terms of the evolution of criminal phenomena. Criminology, as a science of studying deviant behavior and its causes, is challenged to adapt quickly to the new conditions imposed by digital technologies.

The integration of digital technologies into everyday life has directly influenced the nature of crime. The defining elements of cyberspace — transnationality, anonymity, information encryption, and ease of access to technological tools — have created an enabling environment for the development of new types of crime (Holt & Bossler, 2016). In this context, the rapid expansion of areas with criminogenic potential is noteworthy, especially within hidden networks such as the DarkNet.

At the same time, criminals use sophisticated digital methods to evade detection, turning to cryptocurrencies, artificial intelligence and other emerging technologies, which complicates the mission of the authorities in maintaining order and security (Europol, 2023).

Digitalization allows the implementation of a proactive law enforcement model, centered on prevention. By identifying behavioural signals associated with criminal activities early, authorities can intervene promptly and effectively. At the same time, new perspectives are opening up regarding the analysis of individuals' online activity in order to anticipate the risk of deviant or criminal behavior.

This preventive model, supported by predictive analytics and the ability to process large volumes of data, can contribute to the significant reduction of societal risks and the formulation of strategic security decisions (Babuta, 2019).

The extensive collection of commercial data, but also the commercialization of sophisticated digital files, intended for marketing, can be used by foreign entities for espionage, sabotage or destabilization of the country. The digital format of this information offers them a higher resolution, the possibility of automatic reading, integration into automated processes, real-time monitoring and superior efficiency, compared to traditional methods, all of which can be an advantage, but at the same time a disadvantage, in the situation where they are exploited for illegitimate purposes, exposing the nation to risks regarding cyber attacks.

Also, the accelerated digitization of society, the proliferation of smart devices and the logic of surveillance capitalism favor intrusive access to privacy. The wide availability of data is becoming a serious concern, while personal data handling and breach practices lead to significant consequences for both public and national security. Privacy must be approached as a collective responsibility, and robust privacy legislation could be a key pillar of national defence. For example, in 2020, the Consumer Council found that the Grindr app, known as one of the most used social platforms internationally by LGBTQ+ people, transmitted users' personal information to third parties without obtaining their prior consent (NTB, 2019). At the time, U.S. authorities warned of the risk of this sensitive data being exploited by state actors, particularly in China, in order to exert pressure on individuals with access to classified information (Wells & O'Keeffe, 2019). Another eloquent example from practice is the leak of data from a company affiliated with the United States Republican Party, which centralized information obtained through acquisition, for political marketing strategies, which led to the exposure of extremely sensitive data on approximately 200 million American citizens; among the information disclosed were aspects such as religious beliefs, ethnic origin, political orientations and attitudes towards controversial topics such as firearms legislation, abortion rights or stem cell research (Borgesius et al., 2018).

The case study presented in this study analyzes a significant cyberattack on Romania, committed by a cyber actor with alleged ties to Russian intelligence services. This attack was one of the most complex and sophisticated cybersecurity incidents in the region, aimed at obtaining sensitive information and destabilizing key economic and political sectors of the country. The research question underlying this study focuses on assessing how Romania responded to APT cyberattacks and analyzing the effectiveness of its collaboration with international institutions such as NATO and the European Union in the field of cybersecurity. This analysis will highlight the importance of a rapid and coordinated response at national and international level, as well as the need to improve cyber defense strategies in the face of increasingly sophisticated threats.

2. Literature review

According to Mayer-Schönberger and Cukier (2013), the digitalization of critical infrastructures, such as energy, transport, and communication networks, has brought both significant benefits and risks. On the one hand, digitalization facilitates efficient management of resources and faster communication between state institutions; On the other hand, it exposes these infrastructures to sophisticated cyberattacks, which can have devastating effects on national security.

A key aspect of digitalization is the increased vulnerability to cyberattacks, which have become a means by which state or non-state actors can undermine national security. Advanced Persistent Threats (APT) attacks, which are difficult to detect and can last for

months or even years, have increased in frequency and complexity. Groups such as APT28 and APT29, allegedly linked to the Russian Federation, have demonstrated the ability to compromise critical infrastructures and obtain sensitive information from governments and international organizations (Zetter, 2014). These cyber threats not only affect national security, but can also destabilize national economies by disrupting economic or government infrastructures.

To respond to the challenges posed by digitalisation and cyberattacks, states have started to work more closely together at international and national level. Partnerships within NATO and the European Union, as well as through dedicated cybersecurity institutions such as CERT-RO in Romania, have become essential for protecting critical infrastructures and ensuring a rapid response to cyber threats. In addition, international regulations, such as the Budapest Convention on Cybercrime, provide a framework for collaboration between states to combat cybercrime and APT attacks (UNODC, 2020).

Another significant aspect of digitalization in the context of national security is data management and protection. The massive digitization of personal and government data increases the risk that sensitive information will be accessible to malicious actors, which can compromise national security and citizens' trust in state institutions (Kuner, 2017). Regulations such as GDPR in the European Union were created to protect personal data, but challenges remain, especially in the face of increasingly sophisticated cyberattacks that can circumvent traditional security measures.

According to Frolov (2019), ATP attacks have a particular impact on national critical infrastructure, with the potential to disrupt key economic sectors such as energy, transport, health and finance. In the report published by the FSB in 2019, it is pointed out that ATP groups can face a single target and infiltrate computer systems to obtain sensitive data, disrupt activity or even manipulate the internal economic processes of a state. This ability to confront critical infrastructures deepens national vulnerabilities and raises questions about the effectiveness of existing defence measures.

APT groups are often associated with geopolitical interests, especially in the context of information warfare and cyber espionage. Analysis of ATP attacks suggests that these groups are used by states to protect their strategic interests, obtain sensitive information, or destabilize opposing states. ATP attacks by groups such as APT28 and APT29 (also known as Fancy Bear and Cozy Bear) are often attributed to Russian intelligence services and have targeted governments in the European Union and the United States, causing significant damage to the economy and political security (Berghel, 2018). Thus, ATP attacks become a foreign policy tool, used to advance or defend the national interests of a state on the global stage.

According to a report by IBM (2020), the difficulty of preventing and combating such attacks lies in the use of advanced cyber tools and persistent infiltration methods, which are able to avoid detection by traditional security solutions. The report also points out that collaboration between multiple state and non-state entities is often found, which further complicates international responses.

Digitalization brings both significant opportunities for the development of national economies and for the improvement of government processes, as well as considerable risks for national security. As more and more critical infrastructures become digitally interconnected, cybersecurity is becoming a national priority, and states need to adopt a dynamic and adaptable security framework to face the new digital challenges. Moreover,

international cooperation is essential to build a global defense against cyber threats that threaten national and global stability.

3. Methodology and data related to the case study

In this research, the case study method was used, in a qualitative approach, to analyze a major cyber incident with implications for national security. The study focuses on the attack carried out in 2015 against strategic infrastructures in Romania, attributed to the APT28 (Advanced Persistent Threat 28) group, also known as Fancy Bear or Sofacy. Following the detailed analysis of the above-mentioned situation, the author wishes to answer the following research question: to what extent did the 2015 APT28 cyberattack on Romania highlight the vulnerabilities of the national cybersecurity system and what was the role of international cooperation in managing and mitigating its impact?

The case study method was chosen because of its ability to provide an in-depth understanding of a complex phenomenon, in a real, specific and dynamic context.

The research hypothesis of this case study is as follows: if APT (Advanced Persistent Threat) cyberattacks target critical infrastructures and strategic institutions of a state, then international cooperation in the field of cybersecurity — especially within NATO and the European Union — becomes an essential factor for preventing, managing and mitigating their effects on national security.

APT (Advanced Persistent Threat) attacks are, by their nature, sophisticated and extensive over time, involving advanced data infiltration, reconnaissance and extraction tactics. In this context, the case study provides the right framework for:

- detailed analysis of the technical mechanisms and strategic goals of the attack;
- assessing the institutional response of the Romanian state and international partnerships;
- identifying lessons learned and implications for cybersecurity policies.

The analyzed case took place in 2015, targeting information systems belonging to government institutions, strategic economic and political infrastructures and attempts to obtain sensitive information with geopolitical value.

The attack is attributed to the APT28 group, considered affiliated with the Russian military intelligence services (GRU), having previously been involved in attacks on NATO, EU and other allied institutions. The methods used included spear-phishing, zero-day exploits, and advanced malware such as *X-Agent* and *CHOPSTICK* (FireEye, 2015).

The analysis was based on:

- technical reports published by cybersecurity firms (FireEye, CrowdStrike, Kaspersky);
- information provided by CERT-RO (the current National Directorate of Cyber Security);
- NATO and EU documents on coordinated responses to cyber-attacks;
- interviews and public statements by Romanian officials and international partners.

In fact, Romania was the target of a complex cyberattack in 2015, orchestrated by the APT28 advanced group (see Table no. 1 for details on the key elements of the attack). This entity is associated, according to analyses from Western sources and cybersecurity organizations, with the military intelligence services of the Russian Federation (GRU) (Rid, 2020; FireEye, 2017). The attack was specifically directed against government institutions, strategic structures and sensitive areas of the central public administration, particularly targeting the IT infrastructures of ministries and agencies involved in the external and national defense decision-making process.

Table no. 1. Key elements of the 2015 cyberattack on Romania (APT28 group – Fancy Bear)

Date of the attack	Affected sectors	Specific targets	Methods used	External support (NATO/EU)	Major consequences
Summer 2015	Government sector, foreign policy, critical infrastructure	Ministries, strategic institutions, diplomats	Spear-phishing, malware (X-Agent), exploitation of software vulnerabilities	NATO technical assistance, exchange of information with the EU, CERT-RO cooperation	Increased security measures, initiation of attack simulations, increased awareness, strengthening international relations

Source: author's own creation

The APT28 campaign used spear-phishing techniques (sending personalized emails with infected files), exploiting software vulnerabilities, and implanting remote access trojan malware (such as X-Agent), which allowed prolonged and discreet access to compromised networks (CrowdStrike, 2018).

The main purpose of the attack was to steal classified or sensitive information, as well as to generate instability in the political and economic sphere by compromising critical digital infrastructures. Although the exact extent of the damage has not been made public in detail, cybersecurity experts believe that the incident represented an inflection point in the national cyber defense strategy (Dinu, 2021). Consequently, Romania has intensified partnerships with NATO and European Union structures, actively participating in cyber attack simulation exercises and strengthening its role as a regional actor in the field of digital security (CERT-RO, 2016).

The APT28 group has been active for over a decade and has been involved in numerous cyberattacks globally, particularly targeting government institutions, international organizations, the military, and the media in Europe and North America. The general purpose pursued by this entity is to obtain strategic intelligence and influence democratic processes, as observed in the attacks against the Democratic National Committee in the US (2016) or institutions in Germany and France (FireEye, 2017). Romania, as a NATO and EU member state, has become a strategic target in the regional geopolitical logic.

APT28 used advanced computer network infiltration techniques, such as spear-phishing combined with sophisticated malware such as X-Agent, XTunnel, and Zebrocy. These tools enable persistent cyber espionage and data theft without being detected by conventional IT defense systems. The malware used has been adapted to evade detection, intercept communications, and exfiltrate sensitive files (CrowdStrike, 2018). Exploiting vulnerabilities in the software used by the public administration was the key to penetrating compromised networks.

This case study provides a contextualized and applied perspective on how Romania manages highly complex cyber risks. The method also highlights the essential role of

international partnerships and integration into a collective cyber defense system. This analysis model can be replicated for other similar incidents, contributing to the development of a theoretical and practical framework for assessing APT threats.

Romania, as a NATO member state, benefited from support under the Alliance's Cyber Defense Platform, and subsequently, as a result of this incident, strengthened its commitments in the field of digital security. In the following years, the country actively participated in international cyberattack simulation exercises, such as the Cyber Coalition and Locked Shields (NATO CCDCOE, 2021), developed to test the capacity to react and resilience to APTs

4. Results and discussions

To the research question we raised at the beginning of this study, we got the following answer: the cyberattack attributed to the APT28 group (also known as Fancy Bear or Sofacy), attributed to the Russian military intelligence service (GRU) against Romania in 2015 demonstrated the country's significant vulnerabilities to sophisticated cyber threats and underscored the importance of international collaboration, in particular with NATO and the European Union, in protecting critical infrastructures. This incident also highlighted the need to strengthen internal cybersecurity capacities and a faster and more independent reaction from the Romanian authorities

The main targets of the attack included government institutions, political actors, and strategic economic entities, demonstrating the ability of state actors to launch complex cyber espionage campaigns aimed at obtaining sensitive information and influencing domestic decision-making (Rid, 2020; FireEye, 2016).

The campaign used sophisticated spear-phishing methods and personalized malware, taking advantage of the lack of a cybersecurity culture among the employees of the targeted institutions and the absence of robust real-time detection and response systems (Mitre ATT&CK, 2023). The attack was persistent and well-coordinated, signaling the acute need to strengthen the defense of critical infrastructures and to adopt a proactive approach in cyber risk management.

At the same time, this incident underlined the critical importance of international cooperation in the field of cybersecurity. Romania benefited from technical and informational support from the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and the EU Agency for Cyber Security (ENISA), which facilitated the exchange of information on indicators of compromise and defence methods (ENISA, 2016). In addition, Romania's involvement in international exercises such as the "Cyber Coalition" and in real-time data sharing initiatives has allowed for a faster and more coordinated response, given an ever-evolving threat landscape.

In the long term, the APT28 incident has contributed to accelerating institutional and strategic reforms in Romania, including the strengthening of CERT-RO, the adoption of national cybersecurity policies and the strengthening of public-private cooperation. Moreover, Romania has intensified its engagement within NATO, hosting the Euro-Atlantic Resilience Center (E-ARC) and becoming an active actor in defining European cyber defense policies.

So, the APT28 attack in 2015 worked as a catalyst for identifying and correcting deficiencies in Romania's cybersecurity architecture. It also confirmed the strategic value of international alliances, especially in the face of complex and persistent threats generated by state actors.

The analysis of the cyber attack carried out by APT28 against Romania in 2015 reveals, in the author's opinion, a series of essential realities about the persistent vulnerabilities of states in the face of cyber threats coordinated by state actors. Despite a developing legislative framework and institutional strengthening efforts, the attack demonstrated that Romania, like other states in the region, remains exposed to systemic risks, especially when it comes to protecting critical information infrastructures and sensitive data.

I believe that Romania's reaction to this incident, although relatively prompt, was largely reactive and relied on external support rather than mature domestic capabilities. This raises questions about the level of operational autonomy that a state can have in the context of a sophisticated cyber threat. I also note that this case has brought to the fore the need for continuous education in the field of cybersecurity, both at the level of public administration and in the private sector.

On the other hand, collaboration with NATO and EU structures has proven crucial not only in limiting the effects of the attack, but also in recalibrating national cyber defense policies. In my opinion, Romania has correctly understood the message sent by this attack and has taken important steps towards strengthening its strategic position within the European and Euro-Atlantic digital security architecture.

From a broader perspective, the author believes that this case study confirms that cybersecurity can no longer be treated as an isolated technical subfield, but must be integrated into the national and international security paradigm. In the absence of a coherent, multidimensional and forward-looking effort, the risk of such attacks intensifying and diversifying remains high.

In the end, the APT28 attack in 2015 can be considered a turning point in Romanian cybersecurity policy, and the lessons learned from this event should be the basis of a national cyber defense doctrine based on prevention, cooperation and resilience.

5. Conclusions and recommendations

As I have tried to highlight throughout the study, I believe that the widespread integration of digital technologies in all key areas of society has generated not only significant progress, but also profound changes in the nature of crime and the drivers that drive it. Thus, this evolution requires a reassessment of approaches in criminology, adapted to the new technological realities, as well as a strengthening of the contribution of science to the protection of national security. Reinventing criminology in order to integrate it into the digital age is not only a theoretical necessity, but also a practical urgency to ensure public security.

At the same time, there is a need to develop up-to-date and efficient research methods. In this context, this study highlights the main criminal risks that threaten the digital environment, among which the accelerated trend of transforming it into a space increasingly vulnerable to criminal activities stands out.

Referring to the case study carried out within the study, it was found that the cyberattack attributed to the APT28 group in 2015 on Romania provided a unique opportunity to examine not only the vulnerabilities of the Romanian state's cybersecurity system, but also the importance of international partnerships in protecting critical infrastructures and sensitive data. The analysis of this attack revealed a number of deficiencies in cybersecurity, especially in terms of internal detection and response processes, but also in the continuous education of staff in vulnerable institutions.

Romania's response was swift, but largely dependent on external support, thus underlining the need for a more robust national cybersecurity framework that would allow for a faster and more independent response. International partnerships, in particular with NATO and the European Union, played a fundamental role in managing this attack and preventing possible major collateral damage. This highlighted that cybersecurity cannot be tackled in isolation, and a global and cooperative vision is essential for success in the face of complex cyber threats.

In particular, it is clear that APT attacks pose a significant challenge not only from a technical point of view, but also in terms of cyber defence policy. Romania, through this incident, understood the importance of strengthening internal defense structures and, implicitly, strengthening relations with international partners in the field of cybersecurity.

As recommendations, the author suggests the following:

- Strengthening internal detection and response capacities: Romania needs to invest more in developing and implementing advanced technological solutions for the continuous monitoring of critical infrastructures. The implementation of real-time threat detection systems, as well as the training of technical staff within public and private institutions, would help reduce vulnerabilities to APT attacks.
- Intensifying cybersecurity education and training: It is essential for Romania to develop continuous training programs for employees in vulnerable public and private institutions, in order to prevent spear-phishing attacks and other methods of cyber infiltration. The development of cybersecurity curricula at all levels would also contribute to the formation of a culture of digital protection.
- Increasing international collaboration: Given the complexity and transnational nature of cyber threats, Romania needs to continue and strengthen cooperative relations with international partners, especially NATO and the European Union. Participation in international exercises and simulations, such as the "Cyber Coalition" and other intelligence-sharing initiatives, is essential to improve the collective response to cyberattacks.
- Adoption of a national legislative framework adapted to new cyber challenges: Romania should adopt clear cybersecurity policies and regulations that impose protection standards for all entities involved in critical infrastructures. Implementing a regular cyber audit system and stricter security measures would significantly reduce the risks of attack.
- Implementation of a preventive defense model: Romania should adopt a preventive approach to cybersecurity, integrating predictive analytics and artificial intelligence methods into protection systems. This would allow for early identification of threats and reduction of exposure periods to attacks.

These recommendations are meant to contribute to strengthening Romania's cybersecurity, given the lessons learned from the APT28 attack and its analysis. If implemented correctly, these measures will strengthen the country's resilience to future cyber threats and contribute to national security in the context of rapid digitalization.

That said, ATP attacks pose an ongoing and expanding threat to national security, with major implications for governments, economies, and societies. While there is significant progress in preventing and combating them, the lessons learned suggest that cybersecurity must become a constant priority and be based on a dynamic, adaptable framework that takes into account technological and geopolitical developments. In addition, coordinated

international approaches and cross-border partnerships remain essential for effectively preventing and countering these threats.

References:

1. Babuta, A., 2019. *Big Data and Predictive Policing: An Assessment of Law Enforcement Use of Data Analytics*. Royal United Services Institute (RUSI).
2. Berghel, H., 2018. The impact of APTs on national security and geopolitics. *Journal of Cyber Policy*, 3 (4), pp.106-120.
3. Borgesius, F.J.Z., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B., & de Vreese, C., 2018. Online political microtargeting: promises and threats to democracy. *Utrecht Law Review*, 14 (1), pp.82–96.
4. CrowdStrike, 2018. *APT28: A Window Into Russia's Cyber Espionage Operations?*
5. Dinu, A., 2021. Cybersecurity: Romania's National Response to Advanced Threats. *Cybersecurity Journal*, 15(2), pp.34-45.
6. ENISA, 2016. *Threat Landscape 2016*. European Union Agency for Cybersecurity.
7. Europol, 2023. *Internet Organized Crime Threat Assessment (IOCTA).*
8. FireEye, 2015. *APT28: A Window Into Russia's Cyber Espionage Operations?*
9. FireEye, 2016. *APT28: A Window Into Russia's Cyber Espionage Operations?*
10. FireEye, 2017. *APT28: Targeting Governments and International Organizations*.
11. Frolov, V., 2019. Cybersecurity in the era of APT: The evolving nature of state-sponsored cyber attacks. *International Journal of Cyber Security*, 10 (2), 34-47.
12. Government of Romania, 2016. *National Cybersecurity Strategy*. Bucharest: Ministry of Internal Affairs.
13. Holt, T. J., & Bossler, A. M., 2016. *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. Routledge.
14. IBM, 2020. *The 2020 IBM X-Force Threat Intelligence Index*. IBM Corporation.
15. Kuner, C., 2017. *Transborder data flows and data privacy law*. Oxford University Press.
16. Mayer-Schönberger, V. and Cukier, K., 2013. *Big Data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.
17. Mitre ATT&CK, 2023. *APT28 Group Profile*.
18. NTB, 2019. *The US orders the Chinese company to sell Grindr.* Aftenposten*, 28 March 2019.*
19. NATO CCDCOE, 2021. *Locked Shields – The World's Largest and Most Complex International Live-Fire Cyber Defence Exercise*.
20. Osipenko, A.L. and Soloviev, V.S., 2021. The main directions of development of criminological science and crime prevention practice in the context of the digitalization of society. *Russian Journal of Criminology,* 2021, 15(6), pp.681–691.
21. Rid, T., 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux.
22. Rid, T., 2020. *Cyber War Will Not Take Place*. Oxford University Press.
23. United Nations Office on Drugs and Crime (UNODC), 2020. *The Budapest Convention on Cybercrime*. Available at: https://www.unodc.org
24. Wells, G., & O'Keeffe, K., 2019. The U.S. is ordering a Chinese firm to sell dating app Grindr due to the risk of blackmail. *The Wall Street Journal*, March 27.

25. Wilhelmsen, V. R., 2022. Trade tracking – national risk. International Politics, 80(1), 53–77. http://dx.doi.org/10.23865/intpol.v80.3096.
26. Zetter, K., 2014. *Countdown to zero day: Stuxnet and the launch of the world's first cyber war*. Crown Publishing Group.