

Digitalization of Romania's National Security Sector: A PESTLE Analysis

Eliana BULIGA*

Bucharest University of Economic Studies, Bucharest, Romania

**Corresponding author, buligaeliana24@stud.ase.ro*

Doina POPESCU

Bucharest University of Economic Studies, Bucharest, Romania

doina.popescu@man.ase.ro

Abstract. *The digitalization of sectors worldwide has been a compelling evolution and Romania's national security sector is no exception. This article delves into the intricacies of this digital shift, employing a PESTLE framework to analyze key factors influencing this trajectory, as temporary landmark the pandemic period and post-pandemic, and as the time axis from 2020 to the present. This transformation is not only reshaping the operations of security institutions but also altering the landscape that prepares professionals for these roles. While the importance of digitalization has been widely recognized, research focusing on its implications remains sparse. National security in Romania is a multifaceted issue that encompasses various dimensions, including legal frameworks, regional cooperation, and responses to external threats. As a member of NATO and the European Union, Romania's digitalization is deeply intertwined with its international commitments and regional partnerships.*

Keywords: national security, digitalization, digital-transformation, COVID-19, PESTLE.

Introduction

The dynamic nature of the technological field, as well as its rapid evolution, have aroused the interest of all actors involved in the use or development of digital tools, sensing the associated opportunities. Today, new technologies have already proven their ability to contribute to improving performance in all areas of social and economic life. The COVID-19 pandemic accelerated the digitization process, and it allowed the continuation of the activities undertaken by both, public institutions and the private sector.

The legal framework governing Romania's national defense is established by Law 45/1994, which outlines the components of the national defense system, including leadership, forces, resources, and territorial infrastructure (Matei, 2011). This legal structure facilitates Romania's participation in NATO missions and operations, reinforcing its strategic partnerships and contributing to regional security. The collaboration with allies, particularly in the context of the Black Sea region, is crucial for addressing security challenges posed by geopolitical tensions, especially following the events in Ukraine in 2014, which heightened security concerns in Eastern Europe (Wolff, 2015).

Romania's strategic position in the Black Sea region is pivotal for its national security policy. The Black Sea serves as a critical area for military cooperation and regional stability, with Romania actively participating in initiatives aimed at mitigating risks and threats in the area (Vladu, 2021). The country's involvement in NATO's eastern flank defense is particularly significant given the rising tensions with Russia, which has prompted Romania to enhance its military readiness and engage in closer cooperation with neighboring states (Puyvelde, 2020). This cooperation is

exemplified by the Bucharest Nine initiative, which seeks to bolster defense capabilities among Eastern European NATO members.

Furthermore, Romania's role as a bridge between the European Union and its eastern neighbors, particularly Moldova and Ukraine, underscores its strategic importance in regional security dynamics. Romania supports EU policies aimed at enhancing cooperation with these countries, facilitating their integration into European structures, and addressing shared security concerns. The cross-border cooperation initiatives between Romania, Moldova, and Ukraine are essential for fostering stability and addressing socio-economic challenges that could impact security in the region.

In addition to military and diplomatic efforts, Romania's national security strategy also encompasses cybersecurity. The country has developed its own cybersecurity strategy, which aligns with broader EU and NATO frameworks, reflecting the increasing importance of cyber threats in contemporary security landscapes. This proactive approach to cybersecurity is vital for protecting national infrastructure and ensuring resilience against hybrid threats, particularly in the context of the Black Sea region.

Literature review

National Security digitalization during COVID-19

National security in Romania from 2020 to 2025 has been significantly influenced by the COVID-19 pandemic, geopolitical tensions, and the evolving landscape of civil society and public health. The COVID-19 began in early 2020, prompting an urgent response from the government. A few months later, in March, began the lockdown and involved strict measures aimed at controlling the virus's spread (Vladu, 2021). This period was marked by a dual focus on public health and national security, as the government sought to manage both the health crisis and its implications for societal stability. The pandemic's impact on Romania's healthcare system was profound, leading to a substantial reallocation of resources towards emergency care and the cancellation of elective procedures, which resulted in significant financial losses for health institutions (Puyvelde, 2020). The healthcare crisis also exposed vulnerabilities in Romania's public health infrastructure, which had been underfunded and inadequately prepared for such a large-scale emergency (Carey, 2013). The government's response included the establishment of a vaccination campaign, which faced challenges such as vaccine hesitancy and misinformation, particularly among certain demographics influenced by religious beliefs (Vladu, 2021). These challenges underscored the importance of public trust in government initiatives as a critical component of national security.

National Security digitalization after COVID-19

In addition to public health concerns, Romania's national security strategy during this period has been shaped by external geopolitical factors, particularly the ongoing conflict in Ukraine and its implications for regional stability. Romania has positioned itself as a mediator in regional conflicts, leveraging its strategic location and historical ties to promote stability in the Black Sea region. The war in Ukraine has prompted Romania to enhance its military readiness and cooperation with NATO allies, reflecting a broader trend of increasing defense expenditures and strategic partnerships within the context of European security (Ivan and Cutler, 2021).

Furthermore, the role of civil society organizations (CSOs) has evolved in response to these challenges. The Romanian government has recognized the need for a more robust civil society to address issues of sustainability, public health, and community resilience. The transformation of

CSOs is seen as vital for enhancing national security by fostering community engagement and addressing socio-economic disparities exacerbated by the pandemic. This shift highlights the interconnectedness of health, economic stability and security in shaping Romania's National Strategy for 2020-2024 (National Defence Strategy for Romania, 2020).

Romania's national security landscape from 2020 to 2025 has been characterized by a multifaceted approach that integrates public health, geopolitical considerations, and the strengthening of civil society. The COVID-19 pandemic has served as a catalyst for change, prompting a reevaluation of national priorities and strategies to ensure the resilience and security of the nation in an increasingly complex global environment.

Methodology

A PESTLE analysis (Political, Economic, Social, Technological, Legal, and Environmental) can provide a detailed framework for understanding the impact of digitalization on Romania's national security during and after the COVID-19 pandemic. The rapid acceleration of digital technologies during the pandemic transformed how Romania addressed national security challenges, including cybersecurity, public health, law enforcement, and economic stability. The COVID-19 pandemic posed multifaceted challenges to Romania's national security, touching on political, economic, social, technological, legal, and environmental factors. The national security sector had to respond quickly and flexibly to address the immediate health crisis while also ensuring social order, economic stability, and cybersecurity. The PESTLE analysis highlights how Romania's security measures were interconnected with broader societal and governmental efforts, underscoring the complex nature of national security in times of unprecedented public health crises. The experience of the pandemic has likely influenced future national security strategies, particularly in terms of technological preparedness, resilience in the face of emergencies, and the importance of balancing civil liberties with public health and security needs.

Results

Political Factor

The pandemic has significantly influenced political stability and governance. Governments worldwide have enacted emergency measures to control the spread of the virus, which has sometimes led to tensions regarding civil liberties and public compliance. For instance, Mustață et al. highlight that government implemented regulations aimed at mitigating COVID-19's spread, reflecting a broader trend where states prioritize public health over certain civil liberties during crises. Similarly, the movement control order was deemed essential for public health, yet it raised concerns about the balance between security and individual freedoms. The political landscape has thus been reshaped, as governments are compelled to adapt their national security frameworks to include health crises as a core component (Mustață et. al, 2023).

The Romanian government declared a state of emergency in March 2020, allowing it to impose strict lockdowns, quarantine measures, and curfews. These measures were crucial for maintaining public health and security but also raised political challenges, such as balancing public health measures with individual freedoms.

The government faced the challenge of maintaining public trust during the pandemic. Discontent about lockdowns, restrictions, and delayed vaccine rollouts led to political tensions. Ensuring that political institutions acted in a transparent and effective manner was crucial for public compliance. The national security sector had to adapt to emerging political tensions, especially as the pandemic exacerbated social inequalities and unemployment, potentially affecting political

stability. Political leaders had to navigate the complex intersection of public health needs and national security interests.

Economic Factor

The economic landscape acts as a catalyst for digital transformation. Investment in technology and infrastructure is essential for supporting digital initiatives. In Romania, the national security sector has witnessed increased funding due to growing awareness of national threats and the necessity for modern solutions. The economic implications of digitalization also encompass job creation, with new skill sets required in areas such as cybersecurity, data analysis, and digital communication.

The pandemic severely disrupted Romania's economy, with declines in GDP, rising unemployment, and financial difficulties for many businesses. The national security sector had to maintain public order and deal with the economic fallout, such as potential social unrest resulting from financial instability.

The government allocated substantial resources to health and emergency measures, which impacted Romania's overall national security budget. Increased spending on medical supplies, support for the healthcare sector, and security-related measures drained resources that could have been allocated elsewhere. The economic downturn led to increased reliance on digital systems, which in turn led to a rise in cybercrime. The national security agencies had to address emerging threats, such as fraud and hacking, which could impact both economic recovery and security.

Social factor

The societal context cannot be overlooked when considering the implications of digitalization. Romanian society's adaptability to technology plays a significant role in the effectiveness of digital learning environments. As younger generations, adept at using technology, enter the workforce, there is a growing demand for educational programs that equip them with the necessary skills to operate in a digital security landscape. Furthermore, public perception of digital tools enhances or hinders their acceptance and implementation within the security apparatus.

The main concern was protecting public health, but social distancing and quarantine measures had a significant impact on daily life, mental health, and social cohesion. The national security sector had to balance enforcing public health measures with ensuring the social stability of the population.

The pandemic exacerbated existing social inequalities, with poorer communities disproportionately affected by the health and economic crises. This increased the risk of social unrest and civil disobedience, which the national security sector had to manage. Vulnerable groups (e.g., elderly, marginalized communities) were more exposed to health risks, further straining national security resources.

A rise in misinformation and conspiracy theories about COVID-19 led to confusion, fear, and resistance to government measures. The national security agencies (including intelligence services) had to monitor and counteract the spread of false information that could undermine public health efforts and contribute to social unrest.

Technological factor

Technology played a critical role in tracking the spread of the virus, managing quarantine measures, and delivering essential services. The national security sector adopted new technologies, such as contact-tracing apps, which raised privacy concerns but were deemed necessary for public health safety.

As the pandemic accelerated the use of digital platforms (e.g., remote work, online learning, e-commerce), the threat of cyberattacks increased. National security agencies had to address cyber threats targeting government systems, healthcare infrastructure, and private sector businesses.

National Cyber Security Index (NCSI) serves as a measure of a country's Digital Development Level (DDL). DDL is based on the E-Government Development Index (EGDI) and the Networked Readiness Index (NRI). DDL represents the average percentage obtained by the country from the highest value of the two indexes. This metric determines if the accountability for cybersecurity has been officially designated at the highest level of government or politics. Preferably, this should be permanently allocated via legislation or a national strategy to a role or organization wielding the country's executive authority with a governmental mandate, such as the cabinet, a government minister, or a ministry.

The index was created through 5 stages:

1. Recognition of cyber threats regarding the national level
2. Identification of cybersecurity strategies and capabilities
3. Choice of significant and quantifiable elements
4. Creation of cyber security metrics
5. Categorization of cyber security metrics (NCSI, 2023).

NCSI is arranged according to 3 sections, 12 abilities and 49 metrics.

Every metric has a value that indicates how important it is in relation to the index.

The expert committee determines the values based on the following factors:

- 2 points correspond to a law that governs a particular area;
- 2 to 3 points correspond to a specialized unit;
- 2 to 3 points correspond to an official cooperation format;
- 1 to 3 points correspond to an outcome or product (NCSI, 2023).

The NCSI account the summed points after that everything is divided by 100%. Romania features in 6th place with a National Cyber Security Index score of 89.61 out of out of 100. The research also revealed the following about Romania. Romania has been named the 3.81 most secure country for remote workers, with a remote worker security score of 3.81 out of 10. 79.80% of the population in Romania have internet access, which is the 10th lowest total of the countries profiled (NCSI, 2023).

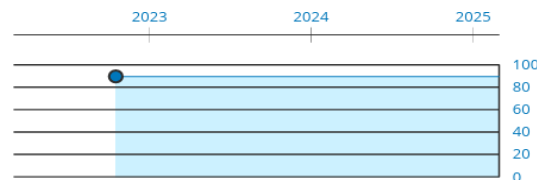


Figure 1. NCSI development timeline - Romania

Source: European Commission, NCSI 2023.

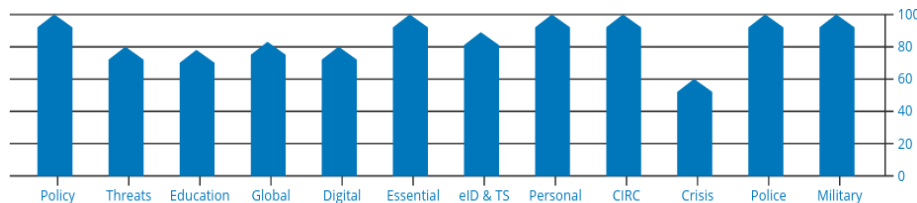


Figure 2. NCSI fulfilment percentage- Romania

Source: European Commission, NCSI 2023.

Legal factor

As digitalization progresses, legal considerations emerge as a significant concern. Data protection laws, privacy regulations, and international agreements must be carefully navigated to ensure compliance and maintain public trust. In Romania, aligning with European Union regulations serves as a foundation for developing legally sound digital practices within the national security sector, thereby reinforcing both security measures and public confidence.

The CSAT coordinates the strategic level of SNSC activity. The CSAT approves the Cybersecurity Strategy of Romania and the legal framework regarding the organisation and functioning of the Cybersecurity Operative Council (COSC), which is responsible mechanism of implementing the Cybersecurity Strategy of Romania. The permanent members of COSC are the Ministry of National Defence (MApN), Ministry of Internal Affairs (MAI), Ministry of Foreign Affairs (MAE), MTIC, Romanian Intelligence Service (SRI), Special Telecommunications Service (STS), Foreign Intelligence Service (SIE), Protection and Guard Service (SPP), National Registry Office for Classified Information (ORNIS) and the Secretary of the Supreme Council of National Defence. All the institutions that are part of COSC cooperate organizations such as EU, NATO and OSCE, each in its field of competence (National Defence Strategy for Romania, 2020).

Romania enacted special laws and decrees to deal with the public health emergency, including the establishment of quarantine zones, the imposition of lockdowns, and the temporary suspension of certain legal rights. This required legal frameworks that balanced public health and national security interests with the protection of civil liberties.

Law enforcement agencies, including the Romanian police and gendarmerie, had to enforce COVID-related measures such as curfews, lockdowns, and travel restrictions. The legality of these actions was scrutinized by the public, and legal challenges were raised regarding the duration and extent of restrictions.

With an increase in cyber threats, Romania had to bolster its legal frameworks around cybersecurity. This included tightening regulations around data protection, the monitoring of digital activities, and counteracting cybercrime, all of which had national security implications.

Environmental factor

Finally, the pandemic has underscored the interconnectedness of health and environmental security. The initial outbreak of COVID-19 has been linked to environmental factors, such as wildlife trade and habitat destruction, which can facilitate the emergence of zoonotic diseases (Ichim, 2024). As nations recover from the pandemic, there is an opportunity to integrate environmental sustainability into national security strategies, promoting resilience against future health crises.

While COVID-19 primarily impacted human health, there were also environmental implications, as the pandemic led to changes in industrial activity, travel, and resource consumption. The national security sector had to ensure that any environmental risks-such as the improper disposal of medical waste or pollution from emergency responses-were managed effectively.

The pandemic created disruptions in environmental monitoring systems. For instance, reductions in industrial and transportation activity during lockdowns led to temporary environmental improvements (e.g., reduced air pollution), but the longer-term effects on environmental governance and security required attention from national authorities.

Environmental security remained a priority, as the pandemic added another layer of complexity to Romania's ability to respond to natural disasters. Civil protection agencies, under the

Ministry of Internal Affairs, had to adapt their emergency plans for crisis situations, considering both the pandemic and other environmental risks such as floods or earthquakes.

National Security digitalization during COVID-19

The national security sector worked closely with healthcare authorities to bolster Romania's healthcare system. The Ministry of Health and national emergency services mobilized to ensure the continuity of medical services. In parallel, the Romanian Armed Forces and Civil Protection Units played a key role in establishing temporary hospitals and assisting with medical logistics. Intelligence Services (e.g., SRI, SIE) pivoted to monitoring new threats, including the spread of misinformation related to the pandemic and conspiracy theories that undermined government measures. They also focused on cybersecurity threats, which saw an increase as more people turned to online platforms for work and communication.

Law enforcement agencies, including the police and gendarmerie, were heavily involved in enforcing quarantine measures, monitoring the public for compliance with health protocols (such as mask mandates), and managing the movement of people across borders. The border police also ensured that travelers adhered to quarantine and testing regulations. While Romania maintained a relatively stable political environment, the economic strain and frustration over lockdown measures contributed to occasional protests and tensions. Security agencies had to balance enforcing restrictions with managing civil unrest and maintaining public order.

As the world moved online, cybersecurity became a critical issue for Romania's national security. The pandemic accelerated the adoption of digital technologies, including remote work and e-commerce. This shift made Romania more vulnerable to cyberattacks, such as ransomware attacks targeting public and private sector entities, including healthcare facilities. The National Cybersecurity Directorate (DNSC) worked to mitigate cyber threats, including hacking attempts on government systems and healthcare data, while intelligence services monitored for espionage or malicious foreign influence.

According to DESI (Digital Economy and Society Index), among the 28 EU Member States involved, Romania ranks 26th. Based on data prior to the pandemic, Romania's performance was the same in 4 of the 5 DESI dimensions measured. This is due to slow progress overall, but also due to political developments, as Romania had 5 different governments over the last 3 years.

Romania is recording notable results in terms of connectivity, especially in urban areas, based on the increased availability of fixed networks. Most homes are connected to internet services (in percentage terms 49%) with data traffic of at least 100 Mbps, Romania ranking fifth in the EU Member Countries. However, when it comes to digitalizing the economy, Romania is recording very low results. Regarding the digitalizing of the economy, Romania is performing very poorly. Unfortunately, a fifth of Romanians have never used the internet. With regard to basic digital skills, less than a third have mastered them. The results are also worrying in terms of the use of public services via internet, with Romania ranking at the bottom of the EU member countries. After all, Romania's results are encouraging in terms of graduates in the ICT field, with an average of 5.6% graduates, compared to level on Europe - 3.6 % (DESI, 2020).

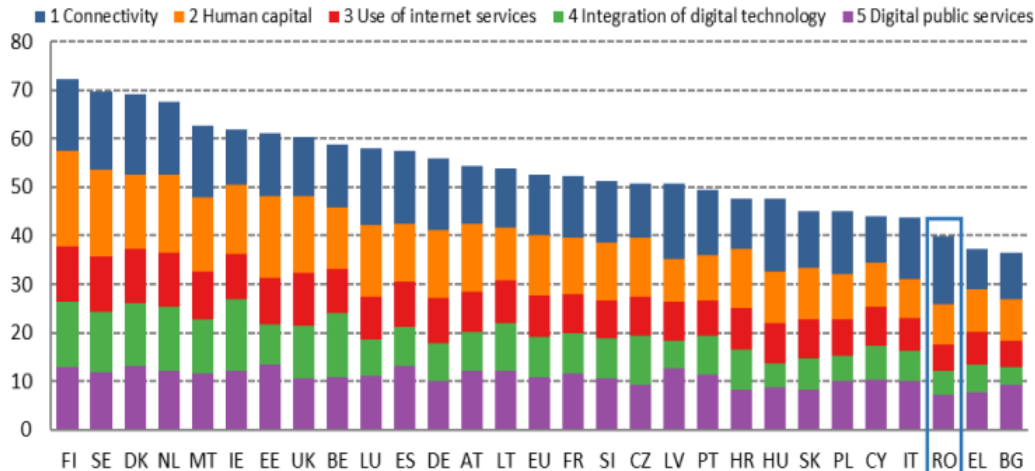


Figure 3: Incorporation of digital technology according to DESI 2020

Source: European Commission, DESI 2020.

National Security digitalization after COVID-19

Following the pandemic, Romania's national security sector had to help manage the economic recovery. The national security framework, including law enforcement, intelligence, and government agencies, focused on restoring stability by addressing economic vulnerabilities, including unemployment, supply chain disruptions, and business closures.

Romania navigated recovery, the national security strategy was reevaluated to address not only military and defense concerns but also non-traditional threats such as pandemics, economic crises, and cyberattacks. The National Security Strategy of Romania was updated to reflect these new priorities, placing a greater emphasis on health security, economic resilience, and cybersecurity.

The pandemic exposed vulnerabilities in Romania's national security system. Post-pandemic, there was a renewed focus on improving the country's healthcare infrastructure, stockpiling medical supplies, and investing in the resilience of medical institutions. The lessons learned from COVID-19 emphasized the need for stronger national health security policies. The government began working on strategies to handle future pandemics, which involved upgrading crisis management systems, improving emergency response protocols, and ensuring greater integration of health and security services. With the shift to remote work, e-commerce, and digital healthcare solutions during the pandemic, Romania's national security sector placed heightened importance on cybersecurity. National strategies have been developed to protect critical infrastructure from cyber threats, especially in areas like healthcare, energy, and government systems (Ivan et al, 2021).

Romania ranks 27th of the 27 EU Member States in the 2022 edition of the Digital Economy and Society Index (DESI). Romania ranks at the bottom of the EU average regarding the human capital size, as well as digital skills. A significant change of pace in Romania's digital skills readiness is crucial for the EU to reach the Digital Decade target on basic digital skills and ICT specialists. Romania performs comparatively well on connectivity, which is the dimension where it scores best.

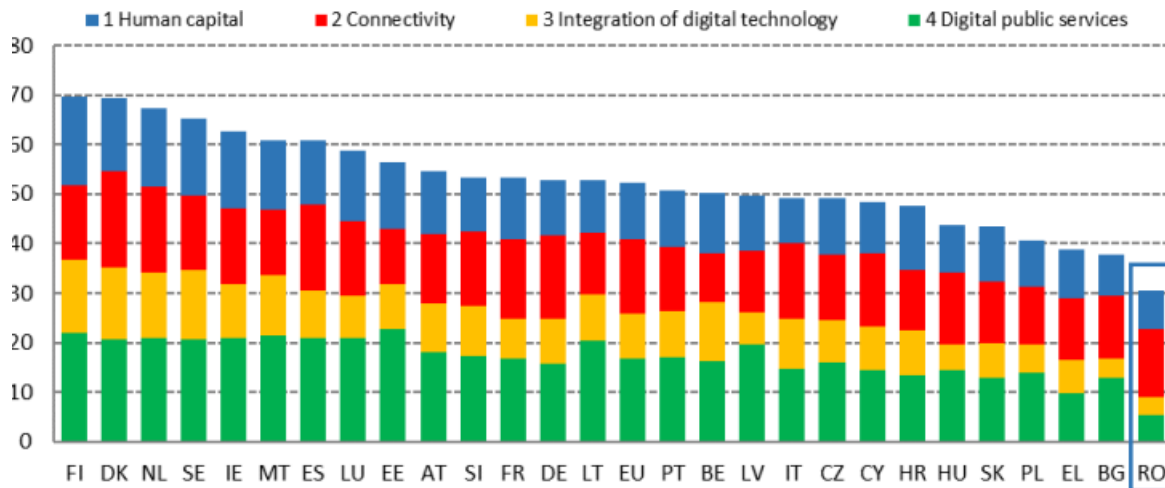


Figure 4: Incorporation of digital technology according to DESI 2022

Source: European Commission, DESI 2022.

The continuation of the COVID-19 pandemic in 2021 and the frequent changes in government (five governments within the last 4 years) represent a particular challenge for the country. Digitalization continues to be a key priority of the current government in power since 25 November 2021, along with simplifying legislation and creating a business-supportive regulatory environment. Digital Economy and Society Index 2022 Romania 4 government is driving the digital transformation of the public sector through the e-government public policy for 2021-2030 (adopted on 3 June 2021) the flagship project for establishing a framework for e-government services and tools. The policy is at the beginning of the implementation process. Immediately after the beginning of the hostile activities in Ukraine, the National Cybersecurity Directorate (DNSC) has initiated a standard process of monitoring and identifying the resources involved in cyber and malware attacks started in the context of the war in Ukraine.

As digital technologies and e-health solutions became more integrated into Romanian life, protecting citizens' personal data and ensuring privacy became a critical part of the national security framework. Romania strengthened its legal frameworks to safeguard against cyberattacks and data breaches. The pandemic left lasting social effects, including mental health challenges, poverty, and increased social inequalities. Post-pandemic, there was a focus on restoring social stability, addressing inequalities, and ensuring access to healthcare and social services for vulnerable groups. The government worked to rebuild public trust, especially in the wake of protests and frustrations related to pandemic restrictions. National security agencies helped maintain social stability by ensuring transparency, countering misinformation, and managing public health communication effectively.

Romania's geopolitical position in the Black Sea and its role as a NATO member remained central to its security post-pandemic. The national security sector continued to monitor the security environment in Eastern Europe, especially in light of tensions involving Russia and the conflict in Ukraine. Romania's cooperation with NATO and the European Union became even more crucial as the pandemic underscored the importance of multilateral security arrangements. Romania continued to participate in joint security and defense operations, while also playing a role in broader

European health and economic recovery initiatives. Romania strengthened its crisis management capabilities, integrating lessons learned from the COVID-19 pandemic into its disaster preparedness framework. This included improving coordination among emergency

services, enhancing medical response capabilities, and building resilience against future pandemics or other global emergencies. The pandemic highlighted the need for integrated approaches between civil protection services and the national defense system. Romania now prioritizes enhancing coordination between the military, intelligence agencies, police, and emergency services to respond quickly to health crises, natural disasters, or potential future pandemics.

Conclusion

Romania's national security during and after the COVID-19 pandemic evolved in response to a series of unprecedented challenges, including public health emergencies, economic disruptions, social instability, and emerging technological threats. The national security framework needed to adapt rapidly to manage the immediate crisis, as well as to lay the foundation for long-term recovery and resilience. Here's a conclusion of PESTLE analysis how Romania's national security was affected during and after the pandemic.

The PESTLE analysis highlights how digital tools influenced multiple aspects of national security, from governance and public safety to economic resilience and environmental impacts.

Technological advancements such as improved cybersecurity, digital surveillance, and AI-based systems bolstered Romania's capacity to manage national security risks but also introduced vulnerabilities related to data privacy, and cyberattacks.

Legal and political responses had to adapt to the fast-paced changes in digitalization, creating new frameworks to protect individual freedoms while maintaining security. Social challenges, such as the digital divide, privacy concerns, and the psychological effects of digital isolation, were central to Romania's efforts to ensure that digital tools served national security without infringing on civil liberties.

As Romania continues to integrate digital technologies into its national security strategy, it will need to strike a balance between efficiency, resilience, and sustainability, ensuring that its digital future supports the stability and security of the nation.

Romania's national security during the COVID-19 pandemic was heavily focused on managing the health crisis while maintaining public order, enforcing restrictions, and protecting citizens from new threats like cyberattacks. In the aftermath of the pandemic, Romania's national security strategy has expanded to incorporate new priorities such as pandemic preparedness, cybersecurity resilience, economic stability, and social cohesion. The country's security agencies have adapted to the changing nature of global threats, especially in areas of technology, misinformation, and cross-border cooperation, ensuring that Romania is better prepared for any future crises. Digitalization during and after the COVID-19 pandemic had profound implications for Romania's national security.

Statements

This paper was co-financed by The Bucharest University of Economic Studies during the PhD program.

References

- European Commission. (2022). The Digital Economy and Society Index (DESI). Retrieved from: <https://digital-strategy.ec.europa.eu/en/policies/desi>.
- Carey, H. (2013). The domestic politics of protecting human rights in counter-terrorism. *East European Politics and Societies and Cultures*, 27(3), 429-465. <https://doi.org/10.1177/0888325413480176>
- Ichim, A. (2024). An Empirical Analysis of the European Union's Economy and Politics in the Context of the War in Ukraine. *International Conference on Business Excellence*, 18 (1), 482 – 493. <https://doi.org/10.2478/picbe-2024-0042>
- Ivan, L. and Cutler, S. (2021). Older adults and the digital divide in Romania: implications for the covid-19 pandemic. *Journal of Elder Policy*, 1(3), 131 -154. <https://doi.org/10.18278/jep.1.3.5>
- Matei, F. and Bruneau, T. (2011). Intelligence reform in new democracies: factors supporting or arresting progress. *Democratization*, 18(3), 602-630. <https://doi.org/10.1080/13510347.2011.586257>
- Mustață, M., Răpan, I., Dumitrescu, L. Dobрева, H., Dimov, P., Lis, A., Révayová, E., Vasile Marineanu, V., Buluc, R., Olariu, C., Lucinescu, A., Buță, C. (2023). Assessing the truthfulness of security and defence news in Central and Eastern Europe: The role of cognitive style and the promise of epistemic sophistication, *Applied Cognitive Psychology*, 37(6), 1384-1396. <https://doi.org/10.1002/acp.4130>
- National Defence Strategy (2020). *Official Journal of Romania*. <https://www.presidency.ro/en/commitments/defence-and-national-security>
- Puyvelde, D., Wirtz, J., Holeindre, J., Oudet, B., Bar-Joseph, U. (2020). Comparing national approaches to the study of intelligence. *International Studies Perspectives*, 21(3), 298-337. <https://doi.org/10.1093/isp/ekz031>
- Vladu, M. and Popescu, S. (2021). Considerations on the impact of emerging and disruptive technologies on security policies. *Scientific Bulletin*, 26(2), 211-216. <https://doi.org/10.2478/bsaft-2021-0026>
- Wolff, A. (2015). The future of Nato enlargement after the Ukraine crisis. *International Affairs*, 91(5), 1103-1121. <https://doi.org/10.1111/1468-2346.12400>