# A Comparative Analysis of the Cybersecurity Landscape in Azerbaijan and Romania: Collaboration, Legal Framework and Protection of Critical Infrastructures

**Andreea DINU[1], Carmen Elena CÎRNU[1] and Tural MAMMADOV[2]**
[1]National Institute for Research and Development in Informatics – ICI Bucharest
[2]Special Communication and Information Security State Service
andreea.dinu@ici.ro, carmen.cirnu@ici.ro, mt@gov.az

**Abstract:** In the digital age, the cybersecurity is a crucial aspect of the national security, with conflicts increasingly extending into the digital sphere. A key priority is the protection of the critical infrastructure, which is vital for the national stability and functionality. Over the past decade, Romania has strengthened its cybersecurity through international cooperation, particularly with non-EU countries. Azerbaijan has emerged as a key partner due to its strategic role in the energy sector and its investments in cyber defense.

This article examines the cybersecurity landscapes of Romania and Azerbaijan, focusing on the critical infrastructure protection and the bilateral cooperation. It reviews past and present initiatives that have enhanced cyber resilience and explores future opportunities for collaboration. Romania's expertise in EU-driven cybersecurity initiatives provides Azerbaijan with technological support, while Azerbaijan's strategic significance and cybersecurity investments offer Romania opportunities to expand partnerships beyond the EU. Through this cooperation, both nations can strengthen their digital defense, advance cybersecurity strategies, and contribute to the global efforts in protecting the critical infrastructure.

**Keywords:** cybersecurity, critical infrastructure, Azerbaijan, Romania, collaboration

## INTRODUCTION

In the modern world, the rapid advancement of the digital technologies has transformed the way nations operate, communicate, and secure their national interests. As the digital infrastructure becomes increasingly integrated into daily life, cybersecurity has emerged as a fundamental pillar of the national security. The rise of the cyber threats has redefined

https://doi.org/10.54851/v7i1y202506

the nature of conflicts, shifting the warfare beyond the traditional battlegrounds into the digital domain. Now, the cyberattacks target government institutions, private enterprises, and, most critically, national infrastructure systems, posing significant risks to the economic stability, public safety, and political sovereignty.

One of the most pressing concerns in the realm of the cybersecurity is the protection of the critical infrastructure, which includes essential sectors such as energy, telecommunications, transportation, financial services, and healthcare. These systems form the backbone of a nation's functionality, and any disruption due to cyberattacks could have severe consequences, including financial losses, service outages, and threats to human lives. As the cyber threats grow more sophisticated and pervasive, the governments must adopt robust security measures to safeguard their infrastructure. However, given the increasingly interconnected nature of the cyber threats, individual national efforts may not be sufficient. Instead, the international cooperation has become imperative for building resilient cybersecurity frameworks capable of effectively countering cyber risks.

Recognizing the necessity of the international collaboration, Romania has taken significant steps in recent years to strengthen its cybersecurity posture through partnerships beyond the European Union (EU). The country has actively engaged in cybersecurity cooperation with non-EU states to exchange knowledge, develop joint initiatives, and establish a collaborative response to the emerging cyber threats. One of Romania's most prominent cybersecurity partners outside the EU is Azerbaijan, a nation that has also prioritized the security of its critical infrastructure. Given its geopolitical significance as an energy hub and its increasing investments in cybersecurity defense mechanisms, Azerbaijan has sought to develop advanced cybersecurity strategies to mitigate potential threats.

This article aims to provide an in-depth analysis of the cybersecurity landscapes of Romania and Azerbaijan, with a particular emphasis on the protection of the critical infrastructure and the benefits of the bilateral collaboration. It examines the cybersecurity policies and initiatives undertaken by both nations, highlighting their shared objectives and the potential advantages of their strategic partnership. By exploring past, present, and future areas of cooperation, this article sheds light on how Romania and Azerbaijan can enhance their cybersecurity resilience, strengthen their digital defense, and contribute to broader international efforts in securing their critical infrastructure.

To comprehensively address the subject, this article is structured into several key chapters, each focusing on a specific aspect of the cybersecurity and collaboration between Romania and Azerbaijan. The first chapter provides an overview of the growing role of the cybersecurity in the modern national security strategies. It discusses how cyber threats have evolved to become a central aspect of internal and external conflicts, requiring governments to develop proactive and adaptive security measures. The chapter also emphasizes the global shift toward prioritizing cybersecurity and the necessity of securing national digital assets. The second chapter focuses on the critical infrastructure and outlines the sectors most vulnerable to cyberattacks and the potential consequences of any security breaches. It examines real-world examples of cyber incidents that have targeted essential services and discusses how such attacks can destabilize the national economies, disrupt daily life, and pose significant risks to human security. The chapter further highlights the importance of robust cybersecurity policies and technologies to protect the critical infrastructure from cyber threats. The third chapter explores Romania and Azerbaijan national cybersecurity strategy, including its policies, regulations, and investments in securing the critical infrastructure. Additionally, the chapter addresses the specific cybersecurity challenges that both countries face due to their geopolitical positioning and the increasing reliance on the digital infrastructure across various critical sectors. The fourth chapter provides a detailed analysis of the bilateral cybersecurity cooperation between Romania

and Azerbaijan. It explores the past and current initiatives, including joint cybersecurity exercises, knowledge-sharing agreements, and collaborative projects aimed at strengthening the national and regional cybersecurity resilience. The chapter also identifies the strategic benefits of this partnership, emphasizing how each country's expertise and resources contribute to their shared cybersecurity objectives. The final chapter explores the potential for the future cybersecurity collaboration between Romania and Azerbaijan. It discusses emerging cyber threats, including the rise of the artificial intelligence-driven cyberattacks, cyber espionage, and ransomware incidents. The chapter examines possible areas of expanded cooperation, such as joint research projects, cybersecurity training programs, and the development of advanced cybersecurity infrastructure. Additionally, it considers how Romania and Azerbaijan can leverage their partnership to contribute to broader international cybersecurity initiatives.

## THE IMPORTANCE OF CYBERSECURITY IN NATIONAL SECURITY

In the digital age, cybersecurity has become a fundamental aspect of the national security, influencing economic stability, defense capabilities, and public welfare. Governments, corporations, and individuals increasingly rely on digital infrastructure for essential functions, making cybersecurity a national priority. As cyber threats grow more sophisticated, nations must implement comprehensive cybersecurity strategies to safeguard critical infrastructure, prevent cyber warfare, and ensure resilience against evolving cyber threats. Cybersecurity is particularly crucial for protecting critical infrastructure, which includes essential services such as energy, telecommunications, finance, healthcare, and transportation. The cyberattacks targeting these sectors can cause widespread disruptions, leading to economic losses, service outages, and public safety risks (Clarke & Knake, 2010). The 2015 cyberattack on Ukraine's power grid, attributed to Russian hackers, left thousands of people without electricity and demonstrated the potential of a cyber warfare to destabilize a nation (Lee, Assante, & Conway, 2016). Similarly, the 2021 ransomware attack on Colonial Pipeline in the United States disrupted fuel supply chains, causing economic and logistical challenges (Kumar, 2021). These incidents highlight the necessity of robust cybersecurity frameworks to protect critical infrastructure from cyber threats. State-sponsored cyber threats have become an increasing concern, with governments using cyber operations to conduct espionage, disrupt political processes, and undermine adversaries. Major cyberattacks such as the Stuxnet virus (2010), which targeted Iran's nuclear facilities, and the SolarWinds cyberattack (2020), which infiltrated multiple U.S. government agencies, illustrate the growing role of the cyber warfare in international conflicts (Zetter, 2014; Goodin, 2021). Countries such as the United States, China, Russia, North Korea, and Iran have been accused of engaging in cyber warfare and espionage, forcing governments to enhance their national cybersecurity postures (Sanger, 2018). In response, the other nations have established dedicated cybersecurity agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. and the European Union Agency for Cybersecurity (ENISA), to coordinate the cyber defense efforts and mitigate threats (European Commission, 2019). Given the transnational nature of the cyber threats, the international cooperation has become essential in strengthening the global cybersecurity resilience. The cyberattacks often impact multiple countries simultaneously, necessitating collaborative efforts to combat cybercrime and share intelligence. The Budapest Convention on Cybercrime (2001), established by the Council of Europe, provides a legal framework for the international cooperation in cybercrime investigations and harmonizing the cybersecurity laws (Council of Europe, 2001). Additionally, the United Nations' Group of Governmental Experts (GGE) on Cybersecurity and INTERPOL's Cybercrime Directorate work towards establishing global cybersecurity norms and improving cross-border responses to cyber threats (UNODA, 2020). Emerging technologies

such as artificial intelligence (AI), quantum computing, and 5G networks present both opportunities and risks for the cybersecurity. AI-driven cyberattacks, deepfake technology, and quantum decryption could undermine the existing security measures, necessitating advanced defense strategies (Brundage et al., 2018). Governments are increasingly adopting Zero Trust Architecture (ZTA), which assumes that no entity within a network should be automatically trusted, to enhance cybersecurity resilience (NIST, 2020).

The importance of the cybersecurity in the national security cannot be overstated. The cyber threats pose significant risks to the national stability, requiring proactive measures to protect the critical infrastructure, deter cyber warfare, and collaborate internationally. Governments must invest in cybersecurity policies, workforce development, and advanced defense technologies to mitigate cyber risks. By prioritizing the cybersecurity, nations can safeguard their digital assets, maintain public trust, and ensure a secure digital future in an increasingly interconnected world.

## CRITICAL INFRASTRUCTURE AND CYBERSECURITY THREATS

The critical infrastructure serves as the foundation of the national security, economic stability, and public welfare. It encompasses essential sectors such as energy, telecommunications, finance, healthcare, water supply, and transportation. As these sectors become increasingly digitalized and interconnected, they are also exposed to the growing cybersecurity risks. The threat landscape has evolved to include sophisticated cyberattacks that can disrupt operations, compromise sensitive data, and weaken the national resilience. Given the potential consequences of such threats, securing the critical infrastructure has become a top priority for governments, organizations, and international bodies (Clarke & Knake, 2010).

The cybersecurity threats targeting critical infrastructure have grown in complexity, ranging from ransomware attacks and state-sponsored cyber operations to supply chain vulnerabilities and distributed denial-of-service (DDoS) attacks. Each of these threats poses unique challenges to the security and functionality of the essential services. The ransomware, for example, can paralyze critical operations by encrypting data and demanding payment for their release. The state-sponsored cyberattacks often aim to infiltrate sensitive government or corporate networks, seeking intelligence or causing disruptions. The supply chain attacks exploit vulnerabilities in software or hardware dependencies, leading to widespread security breaches. Meanwhile, DDoS attacks overload digital services, causing service disruptions and financial losses (Kello, 2017).

One of the primary reasons the critical infrastructures are vulnerable to cyber threats is the increasing reliance on the digital control systems such as the industrial control systems (ICS) and the supervisory control and data acquisition (SCADA) networks. While these systems enhance the operational efficiency, their connectivity to external networks creates security risks. The rapid adoption of the emerging technologies, including the Internet of Things (IoT) and the artificial intelligence (AI), has further expanded the attack surface for the cybercriminals and the nation-state actors. If not properly secured, these technologies can be exploited to gain unauthorized access, disrupt services, or manipulate the critical systems (Rid, 2013).

As the cyber threats continue to evolve, governments and organizations must remain vigilant and adaptive. The emerging technologies, such as the quantum computing and the AI-driven cyber threats, present new challenges that require advanced cybersecurity measures. The cyber resilience must be integrated into the national security strategies, ensuring that the critical infrastructure remains operational and secure against any potential cyber disruptions. By investing in the cybersecurity research, workforce development, and international collaboration, the nations can enhance their ability to protect their vital infrastructure from the evolving cyber threats.

## OVERVIEW OF BOTH ROMANIA'S AND AZERBAIJAN'S CYBERSECURITY LANDSCAPE

The cybersecurity has become an essential component of the national security as countries worldwide seek to protect their digital assets, critical infrastructure, and sensitive data from cyber threats. Both Romania and Azerbaijan have recognized the increasing importance of the cybersecurity and have taken significant steps to develop comprehensive national strategies to enhance their cyber resilience. While Romania's approach has been shaped by its membership in the European Union (EU) and its adherence to the EU cybersecurity frameworks, Azerbaijan has focused on strengthening its cybersecurity policies through the national legislation and international partnerships.

### Romania's Cybersecurity Landscape

Romania has positioned itself as a leader in cybersecurity within the EU, playing a crucial role in the regional and international cybersecurity efforts. As an EU member state, Romania adheres to the Network and Information Security (NIS) Directive, which establishes a common cybersecurity framework for the member states (European Commission, 2016). Additionally, the country has aligned its cybersecurity strategies with the European Union Agency for Cybersecurity (ENISA) and actively participates in EU cybersecurity initiatives.

One of Romania's key cybersecurity institutions is the National Directorate for Cybersecurity (DNSC), formerly known as the National Cyber Security Incident Response Team (CERT-RO). The DNSC is responsible for coordinating national cybersecurity efforts, responding to cyber incidents, and ensuring the compliance with the cybersecurity regulations (DNSC, 2022). Romania has also developed a National Cybersecurity Strategy, which outlines the country's objectives in enhancing cybersecurity resilience, strengthening cooperation between public and private sectors, and improving incident response mechanisms (Romanian Government, 2020).

In addition to its national efforts, Romania has become a major player in the international cybersecurity cooperation. The country hosts the European Cybersecurity Competence Centre (ECCC), which aims to support innovation and investment in cybersecurity across Europe (European Commission, 2021). Romania is also a member of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), contributing to the cybersecurity research and capacity building within the alliance (NATO CCDCOE, 2021).

Another important aspect of Romania's cybersecurity landscape is its growing cybersecurity industry. The country is home to several cybersecurity firms and research institutions that specialize in cybersecurity solutions, vulnerability assessments, and cyber defense technologies. Romanian cybersecurity companies have gained international recognition, with some providing cybersecurity solutions for governments and private organizations worldwide (ENISA, 2022).

Despite these advancements, Romania continues to face cybersecurity challenges, including cybercrime, ransomware attacks, and vulnerabilities in its critical infrastructure. The country has made efforts to combat these threats through improved cyber regulations, awareness campaigns, and partnerships with the international cybersecurity organizations. However, ongoing investment in cybersecurity education, workforce development, and infrastructure security remains crucial for Romania to maintain its strong cybersecurity posture.

### Azerbaijan's Cybersecurity Landscape

Azerbaijan has also recognized the importance of cybersecurity in the national security and economic stability, implementing various policies and initiatives to strengthen its digital defenses. As a country with strategic geopolitical significance and a growing digital economy, Azerbaijan has been actively developing its cybersecurity infrastructure to protect the government institutions, businesses, and its critical infrastructure from cyber threats. One of Azerbaijan's primary cybersecurity institutions

is the State Security Service of the Republic of Azerbaijan (SSS), which oversees the national cybersecurity efforts and works to prevent cyber threats against the country's digital infrastructure (SSS, 2021). In addition, the Electronic Security Service (ESS) under the Ministry of Digital Development and Transport is responsible for coordinating cybersecurity policies, monitoring cyber threats, and implementing cybersecurity awareness programs (ESS, 2022).

Azerbaijan has also adopted a National Cybersecurity Strategy, focusing on strengthening cybersecurity regulations, enhancing digital resilience, and increasing public-private cooperation in cybersecurity efforts. The strategy emphasizes securing government networks, financial institutions, and the country's energy sector, which is a major target for cyber threats due to Azerbaijan's role as a leading energy exporter (Azerbaijan Government, 2021).

Azerbaijan has actively participated in regional and international cybersecurity initiatives. The country collaborates with the Organization for Security and Co-operation in Europe (OSCE) to enhance its cybersecurity capabilities and improve the cyber incident response mechanisms (OSCE, 2021). Additionally, Azerbaijan is a member of the International Telecommunication Union (ITU) and contributes to the global cybersecurity initiatives under the Global Cybersecurity Agenda (GCA) (ITU, 2022).

The country has also taken steps to address cybercrime through its legislative framework. Azerbaijan's Law on Information, Informatization, and Protection of Information provides legal mechanisms to prevent cybercrime and regulate digital security practices (Azerbaijan Parliament, 2018). Furthermore, Azerbaijan has established cybersecurity education programs to train professionals in cyber defense and enhance the public awareness of cybersecurity threats.

Despite its progress, Azerbaijan faces several cybersecurity challenges, including cyber espionage, data breaches, and vulnerabilities in the digital infrastructure. The country has been targeted by cyberattacks aimed at disrupting its government systems and economic activities. In response, Azerbaijan has strengthened its cyber defense capabilities and continues to invest in cybersecurity technologies, workforce development, and international cooperation.

## Comparative Analysis

While Romania and Azerbaijan have distinct cybersecurity landscapes shaped by their geopolitical positions and regional alliances, both countries have recognized the increasing importance of cybersecurity and taken proactive steps to enhance their digital defense. Romania's cybersecurity approach is deeply integrated with the EU regulations and international cybersecurity frameworks, making it a key player in the European cybersecurity efforts. The country benefits from strong institutional frameworks, international partnerships, and a well-developed cybersecurity industry.

Azerbaijan, on the other hand, has focused on developing its national cybersecurity capabilities to protect its critical infrastructure and economic assets. The country's cybersecurity efforts are driven by national security concerns, energy sector protection, and international cooperation. While Azerbaijan has made significant progress in establishing cybersecurity regulations and institutions, further investment in cyber resilience, cross-sector collaboration, and workforce development is needed to address the evolving cyber threats.

Both countries share common cybersecurity challenges, including the need to combat cybercrime, strengthen their critical infrastructure security, and improve the cyber awareness among businesses and citizens. By continuing to invest in the cybersecurity initiatives and fostering international cooperation, Romania and Azerbaijan can enhance their cybersecurity resilience and contribute to the global efforts in securing the cyberspace.

Considering the similarities and differences between the cybersecurity ecosystems from both countries, below it is defined a brief table of the current situation of their cybersecurity:

***Table 1.*** *Comparison between cybersecurity ecosystems of Romania – Azerbaijan.*

| Aspect | Romania | Azerbaijan |
|---|---|---|
| National Cybersecurity Strategy | Focuses on prevention, deterrence, resilience, and EU alignment (Romanian Government, 2022). | Emphasizes national security, digital resilience, and energy sector protection (Azerbaijan Government, 2021). |
| Key Institutions | National Cybersecurity Directorate (DNSC), former CERT-RO (EU-HYBNET, 2023). | Electronic Security Service (ESS), State Security Service (SSS) (DCAF, 2023). |
| International Collaboration | Active in EU cybersecurity efforts (NIS Directive, ENISA), hosts ECCC, NATO CCDCOE member (European Commission, 2021; NATO CCDCOE, 2021). | Collaborates with OSCE, ITU, and participates in GCA initiatives (OSCE, 2021; ITU, 2022). |
| Cybersecurity Industry | Mature, growing industry; global presence of Romanian cybersecurity firms (Research and Markets, 2024). | Emerging industry with skills development focus (Azerbaijan Cybersecurity Center, 2023) (Wikipedia, 2024a). |
| Cybersecurity Challenges | Ransomware, cybercrime, infrastructure vulnerabilities (Statista, 2024). | Cyber espionage, targeted energy sector attacks, data breaches (Deloitte, 2022). |
| Global Cybersecurity Index Score | 85–95 range, classified as “Advanced” (Wikipedia, 2024b). | 93.76/100 in 2024, showing marked improvements (AKTA, 2024). |
| Emphasis of Cybersecurity | Strategic, EU-wide coordination, innovation in cyber capabilities (ENISA, 2022). | National sovereignty, energy security, defense readiness (Azerbaijan Government, 2021). |
| Proactive Defense | Strong CERT ecosystem, proactive threat detection via DNSC, participation in EU threat intelligence sharing (DNSC, 2022; ENISA, 2022). | Ongoing capacity-building, regional drills, cybersecurity exercises with OSCE (OSCE, 2021). |
| Cybersecurity Regulations | Compliant with EU’s NIS2 Directive and GDPR; dedicated national legislation (European Commission, 2016; DNSC, 2022). | Regulated under Law on Information and national digital protection acts (Azerbaijan Parliament, 2018). |
| Strengthen Critical Infrastructure Security | Prioritized in strategy; collaboration between public-private sectors and EU institutions (Romanian Government, 2022). | Major focus on protecting energy and finance sectors, critical for economy (DCAF, 2023; Deloitte, 2022). |

## Romania-Azerbaijan cybersecurity collaboration

In today's interconnected world, cybersecurity has become a critical aspect of the national security and international relations. Recognizing the importance of safeguarding the digital infrastructures, Romania and Azerbaijan have embarked on a collaborative journey to enhance their cybersecurity capabilities and promote cyber diplomacy. This chapter outlines the key initiatives and agreements that define the cybersecurity collaboration between these two nations.

In April 2023, a significant step was taken to formalize the cooperation between Romania and Azerbaijan. The State Service of Special Communication and Information Security of the Republic of Azerbaijan and Romania's National Cyber Security Directorate signed a Memorandum of Understanding (MoU). This agreement focuses on strengthening joint activities of the Computer Emergency Response Teams (CERTs), combating cyber threats, and facilitating the exchange of information and experiences related to cybersecurity incidents (State Service of Special Communication and Information Security of the Republic of Azerbaijan, 2023).

Expanding their collaborative efforts, the National Institute for Research & Development in Informatics (ICI Bucharest) of Romania and Azerbaijan's State Service of Special Communication and Information Security agreed to conduct joint research in several cutting-edge areas. These include the cybersecurity policy and the development strategy, cyber diplomacy, cloud security, the Internet of Things (IoT), the cybersecurity within smart city concepts, Big Data, and the application of the blockchain technology in the top-level domain systems. Additionally, the collaboration extends to the artificial and augmented intelligence, reflecting a comprehensive approach to addressing the contemporary cybersecurity challenges (Azerbaijan State News Agency, 2023).

A landmark development in the Romania-Azerbaijan cybersecurity partnership is the establishment of the Cyber Diplomacy Twinning Center in Azerbaijan. This initiative was formalized through a tripartite MoU signed between Azerbaijan's State Service of Special Communication and Information Security, the Azerbaijan Diplomatic Academy (ADA) University, and the National Institute for Research and Development in Informatics (ICI Bucharest). The center aims to promote research, education, and capacity-building in the field of cyber diplomacy, thereby expanding the international cooperation in information security and digital governance (ICI Bucharest, 2024).

Demonstrating their commitment to advancing cyber diplomacy, Azerbaijan hosted the first International Conference on Cyber Diplomacy on September 25, 2024, in Baku. Organized jointly by Azerbaijan's State Service of Special Communication and Information Security and the Cyber Diplomacy Center (ICI Bucharest), the conference served as a platform for diplomatic representatives, cyber ambassadors, and global stakeholders to discuss the role of the diplomacy in the information security. This event underscored the importance of the international dialogue in addressing the complexities of the cybersecurity (Azerbaijan News Agency, 2024).

The collaboration between Romania and Azerbaijan also extends to addressing the contemporary cybersecurity challenges such as deepfakes and disinformation. The discussions between the Head of Azerbaijan's State Service of Special Communication and Information Security, Lieutenant-General Ilgar Musayev, and the Director of Romania's National Institute for Research and Development in Informatics, Adrian Victor Vevera, focused on the mechanisms able to combat these issues. They also explored the development of training programs for leaders and the implementation of joint projects (Caliber.Az, 2024).

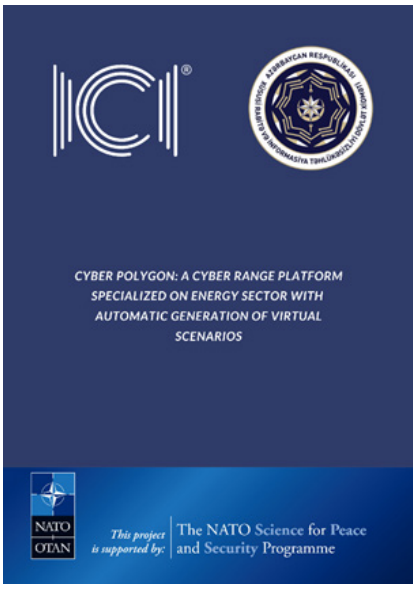


***Figure 1.*** *Project poster*

Further enhancing their collaborative efforts, ICI Bucharest and Azerbaijan's State Service of Special Communication and Information Security have engaged in a research project titled Cyber Polygon: A Cyber Range Platform Specialized on Energy Sector with Automatic Generation of Virtual Scenarios. The project aims to develop a cyber range platform for seamless integration of organizations' operational technology (OT) environment. It facilitates realistic training, technology testing, and process evaluation under high-pressure scenarios. By integrating OT systems into the cyber range, the organizations enhance their cybersecurity preparedness and response capabilities. The proposed platform will offer a simulated environment for hands-on training, rigorous technology testing, and real-time process evaluation, ensuring robust cybersecurity measures. This project is funded by NATO Science for Peace and Security Programme which is a key initiative that promotes the scientific collaboration and innovation between NATO member states and partner countries. Established to enhance security and stability through research, technology, and knowledge-sharing, the SPS Programme focuses on addressing emerging security challenges, including cybersecurity, counterterrorism, defense against chemical, biological, radiological, and nuclear (CBRN) threats, and advanced technological development.

The outcomes of the project are depicted in the following figure:


***Figure 2.*** *Outcomes of the NATO CYBER RANGE project*

## Future prospects for cybersecurity cooperation

As cyber threats evolve, Romania and Azerbaijan have the opportunity to expand their cybersecurity collaboration through joint initiatives in research, policy, and technology. Strengthening their partnership will enhance the national security and contribute to the global cyber resilience. Considering the interest of both countries in the cybersecurity and the common challanges that they face, some joint activities have been identified that will contribute to the increasing national cybersecurity tools and expertise and to strenghten the collaboration.

- Cybersecurity Training and Workforce Development
  - Establish a joint cybersecurity academy offering training in cyber defense and ethical hacking.
  - Develop university exchange programs between educational institutions.
- Joint Cyber Threat Intelligence Sharing
  - Create a Cyber Threat Intelligence Sharing Platform to exchange real-time data on cyber threats.
  - Integrate AI-driven threat detection for automated incident response.
- Critical Infrastructure Protection
  - Conduct joint resilience simulations for energy, finance, and transportation sectors.
  - Enhance secure cloud infrastructure for government and financial institutions.
- Cyber Diplomacy and Policy Alignment
  - Develop joint cybersecurity policies aligned with the EU NIS2 Directive and NATO strategies.
  - Establish an annual Romania-Azerbaijan Cybersecurity Summit to foster policy dialogue.
- AI-Powered Cybersecurity Solutions
  - Develop an AI-driven Security Operations Center (SOC) for advanced threat detection.
  - Create deep-fake detection tools to combat misinformation.
- Public Awareness and Cyber Hygiene Programs
  - Launch a National Cyber Awareness Month to educate citizens and businesses.
  - Provide free online cybersecurity training for the public.
- Blockchain for Cybersecurity and Digital Identity
  - Implement blockchain-based digital identity protection for secured government services.
  - Explore smart contracts for automated cybersecurity compliance.
- Joint Participation in Cybersecurity Exercises
  - Engage in NATO Locked Shields and EU Cyber Europe drills to enhance cyber defense readiness.
  - Conduct joint Red-Blue Team cyber simulations between Romania and Azerbaijan.

## CONCLUSIONS

The evolving cybersecurity landscape demands continuous adaptation and collaboration, particularly in safeguarding the critical infrastructure from cyber threats. This comparative analysis of Romania and Azerbaijan has highlighted the significance of the international cooperation in addressing the cybersecurity challenges. Both nations have demonstrated a commitment to strengthening their cybersecurity frameworks through legal measures, strategic investments, and cross-border partnerships.

Romania, leveraging its integration within the European Union and NATO, has positioned itself as a key player in the cybersecurity initiatives. The country benefits from EU-driven regulatory frameworks, such as the NIS Directive and the Cybersecurity Act, which reinforce its national and regional cyber resilience. Additionally, Romania hosts the European Cybersecurity Competence Centre (ECCC) and actively participates in NATO cyber defense programs, showcasing its dedication to advancing cybersecurity at an international level.

Azerbaijan, recognizing the critical role of the cybersecurity in the national security and economic stability, has made substantial progress in developing its cybersecurity policies. The country has prioritized securing its digital infrastructure, particularly within the energy sector, and has taken legislative steps to combat cyber threats. The establishment of the national cybersecurity agencies and strategic alliances with global partners, including Romania, underscores Azerbaijan's commitment to enhancing its cyber resilience.

The bilateral cybersecurity collaboration between Romania and Azerbaijan serves as a model for international cooperation in the cyber domain. The signing of a Memorandum of Understanding (MoU) between the two nations has facilitated knowledge exchange, joint research initiatives, and cybersecurity training programs. The establishment of the Cyber Diplomacy Twinning Center and participation in NATO-led projects further exemplify the depth of their partnership. Such initiatives not only strengthen their national cybersecurity but also contribute to broader regional and global security efforts.

Looking ahead, Romania and Azerbaijan have the opportunity to expand their cooperation by focusing on the emerging cyber threats, including the artificial intelligence-driven attacks, deepfake manipulation, and cyber espionage. Joint initiatives in the cyber workforce development, advanced threat intelligence sharing, and critical infrastructure protection will be crucial in mitigating future risks. Additionally, aligning their cybersecurity policies with the international standards and fostering cyber diplomacy will enhance the effectiveness of their collaborative efforts.

In conclusion, the cybersecurity partnership between Romania and Azerbaijan underscores the importance of the proactive and strategic approaches to cyber defense. As the cyber threats continue to evolve, the sustained collaboration, technological innovation, and regulatory advancements will be essential in building a secure digital future. By strengthening their joint efforts, both nations can not only fortify their cybersecurity landscapes but also contribute meaningfully to the global cybersecurity ecosystem.

**ACKNOWLEDGEMENT**

This article is supported by The NATO Science for Peace and Security Programme, under SPS G6313 – "Cyber Polygon: A Cyber Range Platform Specialized on Energy Sector with Automatic Generation of Virtual Scenarios" project.

**REFERENCE LIST**

Azerbaijan Government. (2021) National Cybersecurity Strategy of Azerbaijan.

Azerbaijan Parliament. (2018) Law on Information, Informatization, and Protection of Information.

Azerbaijan State News Agency. (2023) Azerbaijan, Romania to conduct joint research in cybersecurity and artificial intelligence. *AZERTAC*. Available at: https://azertag.az/en/xeber/azerbaijan_romania_to_conduct_joint_research_in_cybersecurity_and_artificial_intelligence-2101234

Brundage, M., Avin, S., Clark, J., et al. (2018) T*he Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Future of Humanity Institute. https://maliciousaireport.com/

Caliber.Az. (2024) Azerbaijan, Romania discuss mechanisms to combat deepfakes, disinformation. *Caliber.Az.* https://caliber.az/en/post/azerbaijan-romania-discuss-mechanisms-to-combat-deepfakes-disinformation

Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It.* HarperCollins.

Council of Europe. (2001). *Budapest Convention on Cybercrime.* Council of Europe Treaty Series No. 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

DCAF. (2023) *Cybersecurity Governance Assessment: Azerbaijan.* Geneva: Geneva Centre for Security Sector Governance. https://www.dcaf.ch [Accessed 7th April 2025].

Deloitte. (2022) *Cybersecurity in Azerbaijani Banks*. Available at: https://www2.deloitte.com/az/en/pages/risk/articles/azerbaijani-banks-cyber-security.html [Accessed 7th April 2025].

DNSC. (2022) *National Directorate for Cybersecurity of Romania*. https://dnsc.ro/

Electronic Security Service (ESS). (2022) *Cybersecurity Policy and Coordination.* Ministry of Digital Development and Transport of Azerbaijan. https://www.digital.gov.az/en

ENISA (2022). *Romania's Role in the European Cybersecurity Competence Centre.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu/news/enisa-news/romanias-role-in-the-european-cybersecurity-competence-centre

EU-HYBNET. (2023) *National Cybersecurity Directorate – Romania.* https://euhybnet.eu/directory/national-cybersecurity-directorate/ [Accessed 7th April 2025].

European Commission. (2016) *Directive on Security of Network and Information Systems (NIS Directive).* https://eur-lex.europa.eu/eli/dir/2016/1148/oj

European Commission. (2019) *Cybersecurity Act: Strengthening Europe's Cyber Resilience.* https://ec.europa.eu/digital-strategy/our-policies/cybersecurity-act_en

European Commission. (2021) *European Cybersecurity Competence Centre (ECCC).* https://digital-strategy.ec.europa.eu/en/policies/european-cybersecurity-competence-centre

Goodin, D. (2021) *How the SolarWinds Hackers' Exploits Might Have Escalated into Full-Scale Cyberwar.* Ars Technica. https://arstechnica.com/information-technology/2021/01/how-the-solarwinds-hackers-exploits-might-have-escalated-into-full-scale-cyberwar/

ICI Bucharest. (2024) ICI Bucharest establishes Cyber Diplomacy Twinning Center together with ADA University and the Special Communication and Information Security State Service of the Republic of Azerbaijan. https://ici.ro/en/announcements/ici-bucharest-establishes-cyber-diplomacy-twinning-center-together-with-ada-university-and-the-special-communication-and-information-security-state-service-of-the-republic-of-azerbaijan/

ITU. (2022) *Global Cybersecurity Agenda (GCA).* International Telecommunication Union. https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

Kello, L. (2017) *The Virtual Weapon and International Order.* Yale University Press.

Kumar, M. (2021). *Colonial Pipeline Ransomware Attack: A Wake-Up Call for Cybersecurity.* The Hacker News. https://thehackernews.com/2021/05/colonial-pipeline-ransomware-attack-wake.html

Lee, R. M., Assante, M. J., & Conway, T. (2016) *Analysis of the Cyber Attack on the Ukrainian Power Grid.* SANS Institute, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

NATO. (2024) *NATO's scientific cooperation with Azerbaijan.* NATO. https://www.nato.int/cps/en/natohq/news_229121.htm

NATO CCDCOE. (2021) *Romania's Participation in NATO Cyber Defense Initiatives.* https://ccdcoe.org/uploads/2020/11/NCS_organisation_ROM-2020_FINAL.pdf

NIST. (2018) Cybersecurity Framework Version 1.1. National Institute of Standards and Technology.

NIST. (2020) Zero Trust Architecture (ZTA). National Institute of Standards and Technology.

OSCE. (2021) *Cybersecurity Cooperation with Azerbaijan.* Vienna: Organization for Security and Co-operation in Europe.

Research and Markets (2024) *Romania Cybersecurity Market – Share*. Analysis and Forecast (2024–2029). https://www.researchandmarkets.com [Accessed 7th April 2025].

Rid, T. (2013) Cyber War Will Not Take Place. Oxford University Press.

Romanian Government. (2020) National Cybersecurity Strategy of Romania.

Romanian Government. (2022) *Romania's National Cybersecurity Strategy 2022–2027.* Bucharest: Government of Romania.

Sanger, D. E. (2018) *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age.* Crown Publishing Group.

SSS (2021). Cybersecurity Policies of the State Security Service of Azerbaijan., Available at: https://www.dtx.gov.az/

State Service of Special Communication and Information Security of the Republic of Azerbaijan. (2023, April 27). The State Service of Special Communication and Information Security of the Republic of Azerbaijan and the National CyberSecurity Directorate of Romania have signed a Memorandum of Understanding (MoU). *SCIS.* https://scis.gov.az/en/news/view/252/the-special-communications-and-information-security-state-service-continues-its-cooperation-in-the-international-arena

Statista. (2024) Number of Cybercrimes Investigated by DIICOT in Romania 2014–2023. https://www.statista.com/statistics/1258159/romania-cyber-crimes-diicot/ [Accessed 7th April 2025].

UNODA. (2020) *Report on the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace. United Nations Office for Disarmament Affairs.* https://www.un.org/disarmament/report-of-the-group-of-governmental-experts-on-advancing-responsible-state-behaviour-in-cyberspace-in-the-context-of-international-security/

Zetter, K. (2014) *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown. https://www.penguinrandomhouse.com/books/316214/countdown-to-zero-day-by-kim-zetter/

Wikipedia. (2024a) *Ministry of Digital Development and Transportation (Azerbaijan).* https://en.wikipedia.org/wiki/Ministry_of_Digital_Development_and_Transportation_(Azerbaijan) [Accessed 7th April 2025].

Wikipedia. (2024b) *Global Cybersecurity Index 2024*. https://de.wikipedia.org/wiki/Global_Cybersecurity_Index_2024 [Accessed 7th April 2025].