Romanian-Azerbaijani Cyber Diplomacy: Emerging Cooperation in the Black Sea Extended Region*

[Diplomația cibernetică româno-azeră: cooperare emergentă în regiunea extinsă a Mării Negre]

Ciprian Constantin IFTIMOAEI

Abstract: *The extended Black Sea Region is considered one of the most volatile geopolitical areas in the world, where conventional conflicts, frozen disputes, and hybrid threats intersect with cyberattacks and disinformation campaigns. In this complex landscape, cyber diplomacy has become a vital component of foreign and security policy. This paper explores the evolving collaboration between Romania and Azerbaijan, two countries with different geopolitical ties but shared interests in protecting critical infrastructure, enhancing cyber resilience, and countering hybrid threats. A particular emphasis is placed on the Cyber Diplomacy Twinning Center, established through a partnership among ICI Bucharest, ADA University, and Azerbaijan's State Service for Special Communications and Information Security. This center serves as an innovative initiative that merges academic, governmental, and technical expertise. The findings show that both countries have improved transparency, built institutional capacity, and aligned with international standards, despite differing methods in incident reporting. The analysis indicates that bilateral cyber diplomacy initiatives, when executed efficiently and with minimal bureaucracy, can act as policy laboratories for enhancing regional resilience and governance.*

Keywords: *cyber diplomacy, cybersecurity, Extended Black Sea Region, international cooperation, hybrid threats, critical infrastructure protection.*

Introduction

The extended Black Sea Region has become one of the most complex and tense geopolitical spaces in the contemporary world, where traditional security challenges intertwine with new, hybrid threats. Military conflicts, energy vulnerabilities, and political instability intersect with cyberattacks, disinformation campaigns, and the weaponization of digital technologies. In this volatile environment, cyber diplomacy has emerged as a crucial component of foreign and security policy, shaping the way states, international organisations, and non-state actors negotiate norms, manage risks, and foster cooperation in cyberspace.

Romania and Azerbaijan, located at the crossroads of European, Eurasian, and Middle Eastern geopolitical dynamics, face convergent challenges in safeguarding critical infrastructure, ensuring the resilience of digital ecosystems, and addressing cross-border cyber threats. Romania, as a member of both the European

Union and NATO, has harmonized its cybersecurity policies with Euro-Atlantic standards, actively participating in instruments such as the EU Cyber Diplomacy Toolbox and NATO's cyber defence strategies. Azerbaijan, a pivotal actor in the South Caucasus and a major regional energy supplier, has adopted its first comprehensive cybersecurity strategy (2023–2027), thereby consolidating its institutional framework through entities including the State Service for Special Communications and Information Security and CERT-AZ.

Against this backdrop, bilateral cooperation between Romania and Azerbaijan in the field of cyber diplomacy represents an innovative and timely response to regional and global challenges. The launch of the Cyber Diplomacy Twinning Center, established through a trilateral partnership between ICI Bucharest, ADA University, and Azerbaijan's State Service for Special Communications and Information Security, exemplifies the potential of academic, governmental, and technical collaboration in addressing digital vulnerabilities. Through education, research, knowledge transfer, and policy dialogue, this initiative seeks not only to strengthen bilateral relations but also to contribute to the resilience and stability of the wider Black Sea Region.

This paper analyzes the evolution, institutional frameworks, and strategic implications of Romanian–Azerbaijani cooperation in cyber diplomacy and cybersecurity. It situates the partnership within the broader context of regional security dynamics, examines comparative data on cyber incidents in both countries, and highlights the emerging role of bilateral initiatives in shaping multilateral cyber governance. By doing so, it argues that cyber diplomacy is not merely a technical or sectoral policy area, but an essential pillar of contemporary international relations, capable of fostering stability, trust, and innovation in an era defined by digital interdependence and geopolitical competition.

The Black Sea Region: probably the most tense geopolitical space

The diplomatic collaboration between Romania and Azerbaijan should be examined in the context of the growing risks, vulnerabilities, and threats in the Extended Black Sea Region (EBSR). This region encompasses the riparian states (Romania, Bulgaria, Turkey, Georgia, Russia, and Ukraine) as well as its strategic neighborhood (the Republic of Moldova, Armenia, Azerbaijan, the Eastern Mediterranean, and the South Caucasus). The EBSR functions as a geostrategic hub where NATO and EU interests—represented by Romania, Bulgaria, and close partners such as the Republic of Moldova, Georgia, Ukraine, and Azerbaijan—intersect with Russian strategic objectives, marked by military and geopolitical competition with the West. It is also an area where Turkey, both a NATO member and an independent regional actor with its own diplomatic agenda, plays a significant role, and

where vital energy corridors, trade routes, and transport links between Europe, Central Asia, and the Middle East converge.

Until the collapse of communism in Central and Eastern Europe (1989), followed by the dissolution of the Union of Soviet Socialist Republics (USSR) in 1991, the Black Sea appeared to be a relatively stable area, primarily traversed by commercial vessels and occasionally affected by the military manoeuvres of the Soviet fleet stationed in Sevastopol. Despite belonging to opposing security alliances —the USSR to the Warsaw Pact and Turkey to NATO— the main strategic actors did not engage during the Cold War (1947–1991) in ways that raised significant concerns among the other Black Sea states or attracted substantial international attention. However, in the aftermath of the September 11, 2001 terrorist attacks on the World Trade Center in New York, the United States and its NATO allies recognized that many emerging threats to international security stemmed from the Extended Black Sea Region, the South Caucasus, and the Middle East[1].

The illegal annexation of Crimea by the Russian Federation in 2014, followed by the large-scale war against Ukraine launched in 2022, has transformed the Extended Black Sea Region into one of the most tense geostrategic areas worldwide. Additional instability stems from conflicts in the Middle East, notably the war between Israel and Hamas in Gaza (2023) and the Israel–Iran confrontation (2025), during which the United States conducted strategic airstrikes against the nuclear facilities of the Tehran regime. At present, the war in Ukraine has turned the Black Sea into a zone of heightened military and strategic competition—on the one side, Russia supported by North Korea, Iran, and China; on the other, Ukraine backed by EU and NATO member states. This conflict already undermines maritime security, disrupts trade and transport routes between Europe, Central Asia, and the Middle East, and threatens the energy and critical infrastructures of the Black Sea riparian states, including oil and gas pipelines, submarine cables, communication networks, and port facilities.

Beyond the ongoing war in Ukraine, a series of so-called “frozen conflicts” in the Extended Black Sea Region further exacerbate instability, as they may be reactivated at any moment within this tense geopolitical environment. These conflicts are largely orchestrated by the Russian Federation to deter or intimidate political actors in states such as the Republic of Moldova, Armenia, Azerbaijan, and Georgia. In the broader Black SeaRegion, instability is sustained not only through conventional military means (hard power), but also through hybrid warfare instruments, including so-called “active measures” such as manipulation, disinformation, propaganda, and cyberattacks, systematically employed by the authoritarian regime in the Kremlin.

The analysis of Romanian-Azerbaijani bilateral cooperation in cyber diplomacy must therefore consider all the above insecurity hotspots in the extended Black Sea Region. So far, the negotiations between U.S. President Donald Trump and Russian President Vladimir Putin (the aggressor of Ukraine), held in Alaska on August 15th, 2025, have produced no concrete results, not even a temporary cessation of hostilities[2].

Table 1. Frozen conflicts in the extended Black Sea Region (EBSR)

Conflict	Actors involved	Origin	Current situation
Transnistria	Republic of Moldova vs. Transnistrian separatist authorities (supported by Russia).	War started in 1992, after Transnistria proclaimed autonomy (a separatist region in eastern Moldova).	Ceasefire agreement; Russian military presence in Transnistria; '5+2' negotiations blocked.
Abkhazia	Georgia vs. Abkhaz separatist authorities (supported by Russia).	War started in 1992–1993, partially resumed in 2008.	De facto Russian control; limited international recognition.
South Ossetia	Georgia vs. South Ossetian separatist authorities (supported by Russia).	Armed conflict 1991–1992, escalated in 2008.	De facto Russian control; ongoing 'borderization'.
Nagorno-Karabakh	Azerbaijan vs. Armenia (ethnic Armenian majority in the enclave).	Armed conflict 1991-1994, renewed in 2020 and 2023.	Full Azerbaijani control since 2023; exodus of Armenian population.
Crimea	Ukraine vs. Russian Federation.	Annexation by the Russian Federation in 2014.	Russian military control; heavy militarization; part of the active war theatre since 2022.

In the extended Black Sea Region, the following risks to regional and international security are evident:

- *Military and hard security risks* (active war in Ukraine, militarization of Crimea, air raids by planes and drones into NATO airspace, possible sabotage of underwater infrastructure, arms trafficking);
- *Cyber and informational risks* targeting critical infrastructures (seaports, energy systems, ICT equipment), Russian campaigns of disinformation, manipulation, and

propaganda aimed at destabilizing public perception in hostile states;

- *Economic and energy risks* (logistical blockages of maritime and land corridors, vulnerability of the Baku–Tbilisi–Ceyhan pipeline, South Caucasus Pipeline, Turkish Stream, undermining the competitiveness of the ports of Constanța, Varna, Batumi);
- *Political and governance risks* (resurgence of extremist and populist movements promoting hate speech, mass protests, political instability of riparian states, rise of pro-Russian political forces with anti-democratic and anti-Western rhetoric).

Figure 1. Map of the extended Black Sea Region (EBSR) with "frozen conflicts"

Source: *International Conflict Resolution Center (https://icrcenter.org)*

All these categories of risks are constantly amplified by factors such as the unpredictability of Kremlin decisions, the failure of U.S.–Russia negotiations to end the war in Ukraine, the exclusion of Ukraine from negotiation formats, Turkey's ambiguous role as a NATO member involved in Russian-Ukrainian talks, China's latent interests projected onto harbour infrastructure (e.g., investments in the ports of Piraeus and Constanța via intermediary companies), and the European Union's difficulty in becoming an active part of the

negotiations regarding the war in Ukraine and European security

To counter these risks and neutralize the amplifying factors of insecurity in the extended Black Sea Region, Romania considers it essential to consolidate NATO's presence in the Black Sea (air and maritime patrols, joint exercises, integrated radar systems), empower regional security alliances (*Three Seas Initiative*[3], intensified Romanian-Bulgarian-Turkish cooperation in securing the Black Sea[4], bilateral regional partnerships such as Romania–Azerbaijan), encourage more active Turkish diplomatic involvement[5], strengthen NATO's Eastern flank, secure critical infrastructures, diversify energy and trade routes protected from Russian interference, and promote preventive diplomacy and multilateral cooperation in the field of cybersecurity.

Cyber Diplomacy in the Extended Black Sea Region

Cyber diplomacy represents a relatively recent branch of diplomacy and foreign policy, emerging alongside the expansion of the internet and the widespread adoption of information and communication technologies (ICT), particularly after the 2000s. It focuses on regulating international relations in cyberspace. Cyber diplomacy encompasses not only issues specific to the virtual environment, but also the adaptation of traditional diplomatic practices through the use of digital technologies. To clarify and operationalize the concept of "cyber diplomacy," this analysis employs the related notions of "classical diplomacy," "digital diplomacy," and "cybersecurity."

Classical diplomacy refers to the management of relations between countries through discussions and negotiations conducted through diplomatic representatives, with the aim of cooperation between countries, avoiding conflicts, and maintaining peace and international order. Digital diplomacy concerns the technical tools (digital technologies and online platforms) that contemporary diplomacy benefits from for communication between countries, managing foreign affairs and promoting the image of state actors in the international environment.

According to Marcus Holmes, digital diplomacy has been conceptualized "as a strategy of managing change through digital tools and virtual collaboration". Cyber diplomacy, in turn, can be defined as the set of diplomatic practices through which states, international organizations (such as the UN, OSCE, and OECD), and other state or non-state actors negotiate, cooperate, and regulate activities in cyberspace. Its primary objectives are to prevent and resolve conflicts and to ensure an online environment that is as resilient as possible to cybercrime. Cyber diplomacy cannot be reduced to bilateral negotiations or ad hoc treaties; it must be conceived as a systemic governance process that integrates the technological, political and social levels of the digital space. Cyberspace is seen as a

complex, interdependent ecosystem, where actors (states, international organizations, corporations, civil society) must cooperate to ensure global stability and resilience[6]. The governance of cyberspace requires a set of norms, rules and institutions that are accepted by most states, within a framework of cooperation comparable to that of classical international law[7] Cyber diplomacy represents an emerging frontier in international relations and a key area for building trust between states[8].

The security vulnerabilities of web platforms can undermine diplomatic credibility, for example, through attacks on official websites or the falsification of institutional communications. Addressing such risks requires cyber diplomacy to be grounded in close cooperation between diplomats and technical experts. Equally important is the rapid adoption of international standards designed to secure the digital infrastructures that underpin diplomatic activity. Mutual trust among states cannot rest solely on formal agreements and treaties, but also on the proven capacity for technological resilience[9].

Table 2. Comparison between Classical, Digital, and Cyber Diplomacy

Criterion	Classical Diplomacy	Digital Diplomacy	Cyber Diplomacy
Definition	Management of international relations through negotiations and official representation between states.	Use of digital technologies and online platforms for diplomatic communication, promotion of interests, and dialogue with the global public.	Negotiation and international cooperation to establish rules, norms, and security measures in cyberspace.
Main objective	Maintaining peace, cooperation, and international order.	Modernizing and streamlining the diplomatic process through ICT.	Ensuring security, stability, and responsible governance of cyberspace.
Actors involved	States, international organizations, diplomatic corps.	States, diplomats, global public, mass media, NGOs.	States, international organizations (UN, EU, OSCE), private sector, technical community, NGOs.
Instruments	Bilateral/multilateral treaties, summits, diplomatic notes,	Social media, online platforms, virtual conferences, digital	Multilateral negotiations on cybersecurity,

Criterion	Classical Diplomacy	Digital Diplomacy	Cyber Diplomacy
	mediation.	campaigns.	cooperation agreements, confidence-building measures (CBMs), public–private partnerships.
Fields of Application	Foreign policy, security, economy, culture.	National image, public communication, public diplomacy.	Cybersecurity, protection of critical infrastructure, norms for online behavior, attribution of attacks, Internet governance.
Examples	Treaty of Versailles (1919), Treaty of Trianon (1920), UN Charter (1945).	Diplomatic campaigns on Twitter/Facebook, international online conferences.	UN resolutions on responsible state behavior in cyberspace, EU–NATO agreements on cybersecurity, RO–AZ cooperation for the Cyber Diplomacy Twinning Center.

An important moment in the development of cyber diplomacy was the *Budapest Convention on Cybercrime* (2001), the first international treaty on this subject that refers to combating cybercrime committed by natural or legal persons through the use of information and communications technology[10]. In 2004, in the context of the increase in the number of cross-border cybercrime, the United Nations (UN) established a group of governmental experts in the field of cybersecurity to develop tools and working procedures against cyber threats[11]. A massive cyberattack occurred in 2007 on Estonia, one of the most advanced countries in the world in terms of digitalization of public services. According to the Romanian Intelligence Service (SRI), a similar cyberattack also took place on the websites of some public and financial-banking institutions in Romania. The cyberattack was claimed by the pro-Russian group KILLNET, specialized in DDoS (*Distributed Denial of Service*) attacks, and has also attacked websites of institutions in the USA, Poland, the Czech Republic, but also on NATO websites[12].

Ever since the historic NATO Summit in Prague (2002), when Romania joined this political-military alliance, the member states have discussed the need to protect critical in-

frastructures from cyber threats[13]. After 2004, we can talk about the institutionalization of cyber diplomacy at the international level. In 2008, a year after the cyber-attack on Estonia, NATO developed the first document (*NATO Policy on Cyber Defence*) that describes the framework of the cyber defence for the member countries. However, the first NATO document directly related to cyber diplomacy can be considered the revised edition of the *NATO Policy on Cyber Defence 2011*, which introduces the idea of international political cooperation in cyber matters[14].

The European Union adopted the *Cyber Diplomacy Toolbox* in 2017, considered the first formal framework of diplomatic measures for cyber incidents, which allows member countries to use all Common Foreign and Security Policy[15] (CFSP) measures to prevent, deter and respond to cyberattacks targeting the integrity and security of the EU[16]. Currently, we are witnessing a multiplication of bilateral and multilateral agreements in the field of cyber diplomacy, public-private initiatives involving technology companies, public institutions and non-governmental organizations, which propose policies to regulate the online environment, the use of digital technologies, and combat cyber threats.

The following table summarizes the conceptual relationship between "cyber diplomacy" and "cybersecurity," considering their scope of activity, the tools and procedures employed, the levels of action (international, national, operational), and the categories of cyber threats addressed. The purpose is to highlight both areas of correspondence and potential divergence.

Table 3. The conceptual relationship between cyber diplomacy and cybersecurity

Element	**Cybersecurity**	**Cyber Diplomacy**	**Connections**
Purpose	Protecting digital infrastructures and information.	Creating norms and agreements for a safe and stable cyberspace.	Cyber diplomacy establishes the political and legal framework in which security measures are applied.
Instruments	Technical measures (firewalls, encryption, monitoring), incident response, domestic legislation.	International negotiations, treaties, confidence-building mechanisms, diplomatic sanctions.	Cyber diplomacy supports the adoption of international standards that cybersecurity implements.
Level of action	National / operational.	International / political-strategic.	The outcomes of diplomatic negotiations influence national

Element	Cybersecurity	Cyber Diplomacy	Connections
			cybersecurity policies.
Threats addressed	Cyberattacks, espionage, cybercrime.	Instability in cyberspace, lack of common norms, conflict escalation.	Cybersecurity combats the effects; cyber diplomacy prevents and manages the causes through cooperation.

The analysis of the table indicates a complementary relationship between the concepts of "cyber diplomacy" and "cybersecurity." Cyber diplomacy defines the modalities of cooperation and negotiation at the international level for the protection of infrastructures and databases in areas of shared security interest, while cybersecurity provides the institutional frameworks, technical tools, and operational procedures required to prevent and counter cyber threats. In short, cyber diplomacy establishes the rules of international cooperation in the digital domain, whereas cybersecurity ensures their practical implementation.

Cybersecurity in Romania and Azerbaijan: institutions, policies, correspondences

In accordance with the *Cybersecurity Strategy 2022-2027*, Romania is actively involved in international and regional organizations concerned with cybersecurity. In this regard, through international dialogue and cooperation with relevant partners and organizations, our country aims to promote an open, free, stable and secure global cyberspace, where human rights, fundamental freedoms and the rule of law are fully respected.

Romania treats cybersecurity as an integral component of national security. The country has developed a legislative framework aligned with international standards, facilitating bilateral cooperation and the rapid exchange of information among authorities, with the aim of promoting a free, open, secure, and human rights–respecting internet. The national legal framework regulating diplomacy and cybersecurity includes the *Cybersecurity Strategy of Romania 2022-2027, the National Defence Strategy 2020-2024, Law No. 362/2018 on ensuring a high common level of security of network and information systems, and Government Emergency Ordinance No. 104/2021 on the establishment of the National Cybersecurity Directorate.*

According to Law no. 58/2023, which supplements art. 3 of Law no. 51/1991 on the national security of Romania, republished, with subsequent additions, three new threats to national security are introduced:

- cyber threats or cyber-attacks against information and communi-

cations infrastructures of national interest;

- actions with consequences at national, regional and global levels, which affect the resilience of the state in relation to hybrid risks and threats;
- active measures carried out by a state or non-state entity, through online propaganda or disinformation campaigns, likely to affect the constitutional order.

As a member state of the EU, OSCE and NATO, Romania supports the implementation of the *European Union Cyber Security Strategy*[17] and promotes the increased integration of cybersecurity within the *Common Foreign and Security Policy*, including through the use of the *EU Cyber Diplomacy Toolbox*. At the same time, Romania supports the implementation of CBMs (*Confidence-Building Measures*) within the OSCE, as well as the development of *NATO's Cyber Defence Policy*, aiming to strengthen the resilience of the Alliance and its members, as well as to strengthen deterrence and defence capabilities in cyberspace.

Currently, cyber diplomacy has become an essential component of the foreign policy of countries, international organizations and transnational companies. In Romania, the Ministry of Foreign Affairs (MAE) is the national authority responsible for cyber diplomacy, which ensures the representation of Romania in international relations on cybersecurity issues. Even though the Ministry of Foreign Affairs is the first-ranking public authority with responsibilities in the field of cyber diplomacy, we note that the first initiative in the field of cyber diplomacy belongs to the National Institute for Research and Development in Informatics – ICI Bucharest[18], which operates under the coordination of the General Secretariat of the Government (SGG), which established a Cyber Diplomacy Center in 2019.

The Cyber Diplomacy Center within ICI Bucharest is engaged in developing strategies, initiatives, and actions aimed at enhancing cybersecurity and promoting peace and stability at both regional and international levels, including the involvement of relevant stakeholders from the cyber domain in research and development activities. At the same time, the Center provides expertise in cybersecurity—such as tools for responding to cyber threats—and conducts information, education, and awareness campaigns for the general public on safe navigation in cyberspace[19].

ICI Bucharest collaborates with all relevant national (Ministry of Internal Affairs, Ministry of National Defence, Foreign Intelligence Service, Romanian Intelligence Service, National Cyber Security Directorate) and international (UN, EU, NATO, OSCE) structures involved in the field of diplomacy and cyber security.

The National Cyber Security Directorate operates under the Government of Romania, created by Emergency Ordinance no. 104/2021, which took over the tasks, infrastructure and staff of the former CERT-RO (*Na-*

tional Cyber Security Incident Response Center), transformed into FIRST (*Forum of Incident Response and Security Teams*), as a response structure to cyber incidents in Romania.

Another institution with a key role in cybersecurity management is the National Cyberint Center, operating within the Romanian Intelligence Service (SRI), which is responsible for preventing, detecting, investigating, and countering cyber threats affecting Romania's national security. At the national level, Cyberint safeguards strategic ICT infrastructures. According to official documents published on the SRI website, the National Cyberint Center holds the status of a national authority in the protection of ICT infrastructures relevant to Romania's national security and exercises extensive competences in the prevention and mitigation of cyber threats[20].

The Romanian Intelligence Service (SRI) employs technical and informational capabilities to fulfil its legal responsibilities and to inform designated authorities with the aim of preventing, limiting, and mitigating the consequences of cyber threats to national security. Since July 2020, the National Cyberint Center has also performed the role of CERT within the SRI. The main manifestations of cyber threats to Romania's national security are associated with cyber operations conducted by three categories of actors: state-sponsored groups, organized cybercrime groups, and ideologically motivated entities.

Table 4. Institutional architecture in Romania with responsibilities in cyber diplomacy and cybersecurity

Institution	**Level of authority**	**Relevant fields of activity**	**Responsibilities**
Supreme Council of National Defence (CSAT)	Supreme decision-making body in national security.	Coordination of national security policies.	Sets the strategic directions for national security, including in the cyber domain.
Ministry of Foreign Affairs (MFA)	Ministerial level.	Cyber diplomacy, international representation.	Coordinating and representing Romania in international dialogues on cybersecurity; formulating the national diplomatic position.
Ministry of Research, Innovation and Digitalization	Ministerial level.	Public policies on digitalization and cybersecurity.	Drafting national legislation and strategies on cybersecurity and

Institution	Level of authority	Relevant fields of activity	Responsibilities
(MCID)			digitalization.
Ministry of National Defence (MoND)	Ministerial level.	Military cyber defence.	Protection and defence of military infrastructures and networks; developing cyber defence capabilities.
Ministry of Internal Affairs (MoIA)	Ministerial level.	Internal security, applied cybersecurity.	Preventing, detecting and countering cyber threats within its areas of competence.
Romanian Intelligence Service (SRI)	Intelligence service, national cyber intelligence authority.	National security, cyber intelligence.	Information gathering and analysis, prevention and counteraction of cyber threats affecting national security.
Foreign Intelligence Service (SIE)	Foreign intelligence service.	External intelligence, including the cyber security component.	Protecting Romania's interests abroad, including through cyber intelligence actions.
Special Telecommunications Service (STS)	Special state service.	Secure communications infrastructure.	Providing critical communications infrastructure for state institutions.
National Cyber Security Directorate (DNSC)	National civil authority.	Civil cybersecurity.	Coordination, analysis, prevention and response to cyber incidents; public awareness and training
Directorate for Investigating Organized Crime and Terrorism (DIICOT)	Specialized structure of the Public Ministry.	Investigation of cybercrime.	Combating cybercrime and cyberattacks.
'Carol I' National Defence University	Military higher education institution.	Training and research in security and cyber defence.	Training specialists and conducting applied research.
National Institute for Research and Development in	National research institute in ICT, cybersecurity,	Research and innovation in ICT, cybersecurity and	Developing technological solutions, international part-

Institution	Level of authority	Relevant fields of activity	Responsibilities
Informatics (ICI Bucharest)	cyber diplomacy, critical infrastructures protection.	cyber diplomacy.	nerships and know-how transfer; hosting the Cyber Diplomacy Center

On the Azerbaijani side, the State Service for Special Communications and Information Security (SSSCIS) plays a central role in cybersecurity. This reflects Azerbaijan's broader strategy of anchoring cybersecurity within its national security apparatus, with CERT-AZ as the operational body for cyber incident response. The emphasis is on protecting government ICT systems, critical infrastructure, and ensuring a strong connection between cyber defence and state security institutions.

In August 2023, Azerbaijan adopted its first comprehensive strategy dedicated exclusively to information and cybersecurity for the period 2023–2027, as reported by the Digital Watch Observatory. The strategy sets out several core objectives: safeguarding critical infrastructure, reducing dependence on foreign technologies, fostering domestic innovation, strengthening public awareness and education, and reinforcing international cooperation. Its strategic priorities include the development of advanced threat detection systems (notably those based on artificial intelligence), the enhancement of response mechanisms such as CERT operations, cryptography, and monitoring capacities, the protection of vital infrastructure, the refinement of both legal and cultural frameworks, and the expansion of cross-sectoral and cross-border partnerships[21]. The following table summarizes the responsibilities of the main institutions in Azerbaijan in the field of cybersecurity and cyber diplomacy, considering the hierarchy between them.

Table 5. Public Institutions in Azerbaijan with Responsibilities in Diplomacy and Cybersecurity

Institution	Level of Authority	Areas of Action	Responsibilities
President of the Republic of Azerbaijan	Head of State	Supreme authority over national security and foreign policy	Defines strategic directions in diplomacy, defence, and cybersecurity; appoints heads of relevant bodies.
Ministry of Foreign Affairs (MFA)	Ministerial level	Diplomacy, international representation	Manages foreign relations, represents Azerbaijan in inter-

Institution	Level of Authority	Areas of Action	Responsibilities
			national organizations, formulates foreign policy.
Ministry of Digital Development and Transportation	Ministerial level	Digital policy, ICT, cybersecurity development	Oversees ICT policies, digital transformation projects, and established the Azerbaijan Cybersecurity Center for training specialists.
Special State Protection Service (SSPS)	Special state service reporting to the President	Protection of state communications and officials	Oversees security of state communication systems and coordination of special communication services.
Special Communication & Information Security State Service	Agency under SSPS	Cybersecurity infrastructure, cryptography, training	Secures state communication networks, develops cryptographic systems, coordinates CERT-AZ, trains cybersecurity personnel.
CERT-AZ (Government Computer Emergency Response Team)	National-level operational team	Incident response, cyber awareness	Coordinates national cybersecurity incidents, conducts analysis, issues alerts, provides recommendations to public and private sectors.
State Security Service (DTX)	National intelligence and security agency	Internal security, counterintelligence, cyber intelligence	Protects internal security, counteracts espionage and terrorism, likely addresses cyber threats.
Foreign Intelligence Service	National foreign intelligence agency	External intelligence, including cyber components	Gathers intelligence abroad to protect Azerbaijan's interests, including in cyberspace.

Institution	Level of Authority	Areas of Action	Responsibilities
State Border Service	Security agency	Border protection, infrastructure security	Protects Azerbaijan's borders and critical infrastructure, including pipelines, with possible cybersecurity elements.
Topchubashov Center	Independent policy think tank (non-governmental)	International relations research	Produces studies and organizes conferences contributing to foreign policy and security discourse.

According to the United Nations Office for Disarmament Affairs Documents Library, in 2023, Azerbaijan implemented a set of rules for securing critical infrastructures and created a special registry for them. At the same time, it improved its position in the National Cyber Security Index ranking, moving up from 86th to 50th place[22].

In September 2024, Baku hosted the first international conference dedicated to Cyber Diplomacy. The event brought together diplomats, "cyber ambassadors" and global actors in intelligence, and security studies[23]. In April 2025, Azerbaijani State Service for Special Communication and Information Security (SSSCIS) officials highlighted, at the Digital Summit in Bucharest organized by ICI Bucharest, the essential role of cyber diplomacy in managing technological dependencies, supply chain risks and cyberattacks, emphasizing the need for international cooperation.

Romanian-Azerbaijani cooperation in the field of cyber diplomacy

Recent geopolitical developments, the intensification of global cyberattacks, and the growing interdependence of digital infrastructures have made cybersecurity a strategic priority for states worldwide. The Wider Black Sea Region is increasingly exposed to sophisticated cyber risks that target both critical infrastructures and democratic processes. Countries in this area face significant strategic and technological challenges, which require enhanced cooperation through diplomatic dialogue, the exchange of best practices, and the strengthening of common capabilities.

Since gaining independence after the dissolution of the Soviet Union, Azerbaijan, as an OSCE member, has developed an independent diplomatic service aimed at advancing national interests. This process has entailed the expansion of embassies and diplomatic missions abroad, together with

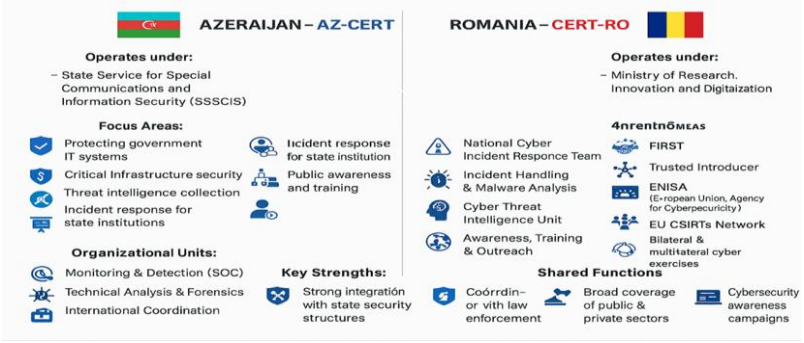
the adoption of modern approaches such as cultural, digital, multilateral, and energy diplomacy[24].

Both Romania, a member of the European Union and NATO, and Azerbaijan, a relevant regional actor in the Caucasus, face similar threats: attacks on critical infrastructures, disinformation campaigns and ransomware-type actions. Bilateral cooperation may encompass areas such as the exchange of data on cyberattacks, the development of joint response capabilities, the training of ICT specialists, and the harmonization of legal frameworks on data protection and cyber incidents. The convergence between Romania and Azerbaijan is rooted in the adoption of public policies on cybersecurity, with a focus on protecting critical infrastructures, strengthening response capabilities to cyber incidents, and reinforcing international cooperation.

Both countries have national structures (CERT) with responsibilities for managing cybersecurity incidents. A CERT has a specialized team responsible for preventing, detecting, analysing, and responding to cybersecurity incidents. It acts as a central hub for coordination when digital infrastructures are threatened, ensuring that both government institutions and private stakeholders can respond effectively to cyberattacks.

AZ-CERT (Azerbaijan) operates under the authority of the State Service for Special Communications and Information Security (SSSCIS), an institution directly linked to national security structures and responsible for the control and protection of governmental ICT systems. In Romania, CERT-RO has been integrated into the National Cybersecurity Directorate (DNSC), evolving from an independent national CERT into a component of a broader authority under the Ministry of Research, Innovation, and Digitalization. The DNSC exercises both strategic and operational responsibilities, coordinating cybersecurity across the public and private sectors in alignment with EU frameworks. The following figure illustrates the structure of AZ-CERT in Azerbaijan compared with that of CERT-RO within the DNSC in Romania.

Figure 2. Comparative structure AZ-CERT vs. CERT-RO



Romanian–Azerbaijani cooperation in the field of cybersecurity represents an emerging dimension of bilateral relations. In recent years, official visits —including dialogues at the level of foreign ministers and senior officials responsible for digital affairs— have incorporated a cyber cooperation component. Discussions have also explored the prospect of signing a memorandum of understanding on the exchange of best practices, training, and technical support. Romania, through the National Cybersecurity Directorate (DNSC) and the European Cybersecurity Competence Centre (ECCC), has the potential to become a key partner for Azerbaijan by providing expertise and support for the establishment of similar centers in the region.

Both countries actively participate in regional and multilateral initiatives. Romania, as an EU and NATO member state, promotes Euro-Atlantic standards in the cyber field. Azerbaijan is involved in the *EU Eastern Partnership* and collaborates with the OSCE and other organizations to promote adherence to international norms in cyberspace. Participation in joint exercises, such as Cyber Europe or events organized by the *European Union Agency for Cybersecurity*[25] and OSCE generate opportunities for mutual dialogue and cooperation based on common values, regulations and procedures.

Cyber diplomacy has become an essential instrument of contemporary security architecture, particularly in regions marked by geopolitical tensions such as Eastern Europe and the South Caucasus. The cooperation between the National Institute for Research and Development in Informatics (ICI Bucharest), the Azerbaijan Diplomatic Academy (ADA University), and the Special Communications and Information Security Service of the Republic of Azerbaijan (SCISSA) represents an innovative initiative through the establishment of the Cyber Diplomacy Twinning Center. On September 24, 2024, a Memorandum of Understanding was signed between ICI Bucharest, ADA University, and SCISSA. The document provides for the creation of the Cyber Diplomacy Twinning Center in Azerbaijan, with the objective of promoting education, research, and cooperation in the fields of cyber diplomacy, critical infrastructure protection, and information technologies. The main signatories were Dr. Carmen-Elena Cîrnu (ICI Bucharest), Dr. Fariz Ismailzade (ADA University), and Major General Allahveran Ismayilov (SCISSA).

The Cyber Diplomacy Twinning Center was formally inaugurated during the inaugural *International Conference on Cyber Diplomacy* held in Baku September, 2024. This joint Romanian-Azerbaijani initiative in the sphere of cyber diplomacy seeks to foster the development of educational programs on cybersecurity and digital diplomacy, advance research on safeguarding critical infrastructures, organize conferences, workshops, and international forums, promote the exchange of best practices in com-

bating cyber threats, and support the advancement of a multilateral diplomatic agenda in the digital domain.

The Romanian-Azerbaijani initiative offers a functional model of cooperation in an emerging and complex field. Through cyber diplomacy, communication channels are built in a digital space characterized by uncertainty, polarization and conflict. The expansion of this initiative at the regional and international level can transform Romania into a reference hub in the field of digital diplomacy and cyber governance. Although cooperation in the field of cyber diplomacy between Romania and Azerbaijan is at an early stage, there are premises for its development, especially in the research-development and information-education-awareness components of the general public.

In exploring the prospects of Romanian–Azerbaijani cooperation in the field of cyber diplomacy, an interview was conducted with Dr. Fariz Ismailzade, Vice-Rector of ADA University and Coordinator of the Cyber Diplomacy Center in Azerbaijan. The Romanian–Azerbaijani partnership in this area has been primarily driven by Azerbaijan's need to strengthen its cybersecurity expertise and defence capabilities. Despite growing global attention to cybersecurity, many states—including Azerbaijan—continue to face shortages of qualified specialists and limited international experience in this domain. Romania, with its accumulated expertise in both the technical and policy dimensions of cybersecurity, has been regarded as a suitable partner.

The Memorandum of Understanding (MoU) was initiated by the Azerbaijan State Agency for Cybersecurity Protection, which proposed a trilateral format involving governmental institutions, universities, and research centers. This model was intended to integrate training, policy dialogue, and research activities, in line with international trends of multi-stakeholder cooperation in cyber diplomacy. The Center pursues three strategic objectives: (1) developing capacity-building programs and training for cybersecurity specialists; (2) facilitating policy dialogues and conferences aimed at improving national legislation and regulatory frameworks; and (3) strengthening both individual expertise and overall national cybersecurity capacity through knowledge transfer from Romanian experts. To date, cooperation has materialized in joint workshops and training programs involving Azerbaijani governmental representatives. Although private sector participation remains limited, plans are underway to extend the partnership to companies and industry actors. The initial phase has therefore been primarily educational and institutional, laying the foundations for long-term sustainability.

Given Azerbaijan's geopolitical position—bordering Russia, Iran, and Türkiye—and its role as a major energy producer, the protection of critical communication, energy, and information infrastructures constitutes a

national priority. The interview underscores past cyberattacks attributed to both state and non-state actors, highlighting the strategic importance of the partnership with Romania. Through expertise transfer and training, the initiative contributes directly to strengthening the resilience of Azerbaijan's critical infrastructures. The main cooperation mechanisms include knowledge-transfer workshops, academic exchanges, and joint training activities, through which Romanian experts have already shared practical insights with Azerbaijani specialists. A key best practice emphasized by Dr. Ismailzade is the initiative's low level of bureaucracy and rapid implementation, which enabled the swift mobilization of resources and effective coordination. Furthermore, the involvement of embassies and diplomatic instruments has been identified as a future avenue for deepening cooperation and supporting institutional dialogue.

Dr. Ismailzade did not identify major barriers such as bureaucratic or cultural differences; instead, he emphasized the efficiency and speed of the project's launch as a distinctive strength. An important lesson learned is that international cyber diplomacy initiatives benefit from streamlined decision-making and could be replicated in other fields, including education and scientific research. In the medium term (3–5 years), the project seeks to expand training activities, placing greater emphasis on technical specialists—ICT experts, programmers, and engineers—while also engaging students in research and educational programs. Beyond the bilateral dimension, Romania and Azerbaijan have the potential to position themselves as regional leaders in cyber diplomacy, setting a precedent for countries in the South Caucasus and Central Asia. Replicating this model in other geopolitical contexts could further strengthen regional resilience and cooperation.

The interview concludes with a clear recommendation: similar bilateral projects should be promoted swiftly and with minimal bureaucracy, given the rapidly evolving technological and security environment. The Romanian–Azerbaijani partnership demonstrates that efficiency, multi-stakeholder engagement, and knowledge transfer are essential ingredients for building sustainable international cooperation in cybersecurity. There are strong foundations for developing a strategic partnership based on shared interests and geopolitical complementarity. Strengthening this cooperation can contribute to regional stability, the alignment of digital protection standards, and enhanced cyber resilience in an increasingly complex digital environment shaped by the technological revolution brought about by Artificial Intelligence across all areas of human activity.

Conclusions and recommendations

The analysis of Romanian-Azerbaijani cooperation in cyber diplomacy confirms the growing im-

portance of digital security in international relations, particularly in the extended Black Sea Region, which is an area where conventional conflicts and frozen disputes are compounded by cyber threats, hybrid warfare, and disinformation campaigns. In this context, cyber diplomacy is no longer a peripheral dimension of foreign policy but a central tool for enhancing resilience and ensuring stability.

Despite different geopolitical alignments, Romania and Azerbaijan converge around shared interests: the protection of critical infrastructures, the management of cyberattacks, and the safeguarding of digital sovereignty. The creation of the Cyber Diplomacy Twinning Center—through the partnership of ICI Bucharest, ADA University, and Azerbaijan's State Service for Special Communications and Information Security—represents an innovative and practical response to these challenges. By bringing together governmental institutions, academic expertise, and technical know-how, the initiative establishes a foundation for education, policy dialogue, and joint research in the field of cyber diplomacy. To consolidate and expand this cooperation, several recommendations can be outlined:

- Deepen Bilateral Engagement by strengthening the Cyber Diplomacy Twinning Center and expanding its scope to include training, academic exchanges, and technical cooperation.
- Broaden Multistakeholder Involvement by incorporating the private sector, civil society, and international partners, thereby creating a more inclusive cyber diplomacy ecosystem.
- Regionalize the Model by extending the Romanian–Azerbaijani partnership to other Black Sea and South Caucasus states, fostering a regional platform for digital security and cyber governance.
- Advance Legal Harmonization by aligning legislation on data protection and cybersecurity with Euro-Atlantic and international norms, ensuring trust and interoperability.
- Incorporate Strategic Foresight by addressing emerging challenges such as artificial intelligence, quantum computing, and 5G/6G, and embedding them into bilateral policy agendas.
- Strengthen Confidence-Building Measures through joint exercises, simulations, and information-sharing mechanisms designed to build trust and reduce risks of escalation.

The Romanian–Azerbaijani partnership offers valuable lessons for international practice. It demonstrates that bilateral cyber diplomacy can be launched with minimal bureaucracy, rapid mobilization, and strong institutional synergy – qualities often missing in larger multilateral frameworks. By linking Euro-Atlantic experience with the strategic priorities of the South Caucasus, the initiative has the potential to act as a policy laboratory for the wider region. In a world increasingly shaped by technological interdependence, the Romanian–

Azerbaijani model provides a forward-looking blueprint for states seeking to enhance cyber resilience, foster trust, and promote cooperative security in contested geopolitical environments.

Notes

- Acknowledgments: This article was prepared with the support of Dr. Ing. Adrian-Victor Vevera, First-Degree Scientific Researcher (CS I) and General Director of the National Institute for Research and Development in Informatics – ICI Bucharest, who also facilitated the author's interview with Dr. Fariz Ismailzade, Vice-Rector of ADA University and Coordinator of the Cyber Diplomacy Center in Azerbaijan. The author also wishes to express gratitude to Dr. Fariz Ismailzade for kindly agreeing to participate in the structured interview.

[1] Ciprian Iftimoaei, *Despre democrație, securitate și bună guvernare. România în context regional*, Editura Lumen, Iași, 2015, pp. 11-41.

[2] Steve Holland, Andrew Osborn and Darya Korsunskaya, *'No deal until there's a deal': Trump-Putin talks yield no breakthrough on Ukraine*, https://www.reuters.com, (accessed August 2025).

[3] Ministerul Afacerilor Externe (RO), *Inițiativa celor Trei Mări (I3M)*, https://www.mae.ro/node/49437, (accesed August 2025).

[4] AP News, *Turkey, Bulgaria and Romania sign a deal to tackle Black Sea mines*, https://apnews.com/article/turkey-bulgaria-romania-mines-black-sea-guler-149e33a227512ad043de191781c0ecff, (accessed August 2025).

[5] Yevgeniya Gaber, *To help bring lasting peace to Ukraine, Turkey should enhance its cooperation on Black Sea security*, https://www.atlanticcouncil.org/blogs/turkeysource/to-help-bring-lasting-peace-to-ukraine-turkey-should-enhance-its-cooperation-on-black-sea-security/?utm_source=chatgpt.com, (accessed August 2025).

[6] Alexandru Georgescu, Adrian-Victor Vevera, Carmen-Elena Cîrnu, *The Diplomacy of Systemic Governance in Cyberspace*, International Journal of Cyber Diplomacy, Vol. 1, Nr. 1, 2020, https://ijcd.ici.ro, (accessed August 2025).

[7] André Barrinha & Thomas Renard, *Cyber-Diplomacy: the making of an international society in the digital age*, Global Affaires, 2017, https://www.egmontinstitute.be, (accessed August 2025).

[8] Ioana-Cristina Vasiloiu, *A New Frontier for Global Cooperation in the Digital Age*, *Informatica Economică*, Vol. 27, Nr. 4, 2023, https://revistaie.ase.ro, (accessed August 2025).

[9] Carmen-Elena Cîrnu, Ioana-Cristina Vasiloiu, Bridging the gap: an analysis of Cybersecurity in web technologies for Cyber diplomacy, International Journal of Cyber Diplomacy, Vol. 5, 2024, https://ijcd.ici.ro, (accessed August 2025).

[10] Uniunea Europeană, *Convenția privind criminalitatea informatică*, https://eur-lex.europa.eu/RO/legal-content/summary/convention-on-cybercrime.html, (accesed August 2025).

[11] CyberPeace Institute, *United Nations Cybersecurity Processes Explained*, https://cyberpeaceinstitute.org/united-nations-cybersecurity-process-explained, (accessed August 2025).

[12] Serviciul Român de Informații (SRI), *Atacuri cibernetice asupra site-urilor unor instituții publice și financiar-bancare*, https://www.sri.ro/articole/atacuri-cibernetice-asupra-site-urilor-unor-institutii-publice-si-financiar-bancare.html, (accessed August 2025).

[13] NATO, *Prague Summit 2002. Selected Documents and Statements*, p. 53 (Strengthen our capabilities to defend against cyber attacks) https://www.nato.int/docu/0211prague/speeches-e.pdf, (accessed August 2025).

[14] NATO, *Cyber Defence*, https://www.nato.int/cps/en/natohq/topics_78170.htm, (accessed August 2025).

[15] European Commission, *Common Foreign and Security Policy*, https://commission.europa.eu, (accessed August 2025).

[16] Yuliya Miadzvetskaya & Ramses Wessel, The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox*, European Papers*, Vol. 7, No 1, 2022, pp. 413-438.

[17] Uniunea Europeană, *Strategia de securitate cibernetică a UE*, https://digital-strategy.ec.europa.eu/ro/policies/cybersecurity-strategy, (accessed August 2025).

[18] National Institute for Research & Development in Informatics - *ICI Bucharest, Short History*, https://ici.ro/en/short-history, (accessed August 2025).

[19] National Institute for Research & Development in Informatics - ICI Bucharest, *Cyber Diplomacy Center*, https://www.ici.ro/ro/centre-de-competenta/centrul-de-cyber-diplomacy, (accessed August 2025).

[20] Romanian Intelligence Service, *Cyber intelligence*, https://www.sri.ro/ cyber-intelligence, (accessed August 2025).

[21] Digital Watch Observatory, *The Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027*, https://dig.watch, (accessed August 2025).

[22] United Nations Office for Disarmament Affairs Documents Library, *View of the Republic of Azerbaijan on Resolution 78/237 "Developments in the field of information and telecommunications in the context of international security"*, https://docs-library.unoda.org, (accessed August 2025).

[23] Nazrin Abdul, Azerbaijan advances cybersecurity initiatives through strategic developments, 2024, https://www.azernews.az, last accessed August 2025.

[24] Fariz Ismailzade, *Digital Diplomacy in Azerbaijan: Lessons Learned and Future Opportunities*, in Bjola, C., Holmes, M. (Eds.), Digital Diplomacy in the OSCE Region, Contributions to International Relations, Springer, Cham, 2024, https://doi.org/10.1007/978-3-031-50966-7_2, (accessed August 2025).

[25] ENISA a fost creată în 2004, din 2019 funcționează pe baza Regulamentului UE 2019/881 (*Cybersecurity Act*), și are sediul principal la Atena (Grecia) și un sediu secundar în Heraklion – Creta. Această agenție europeană sprijină statele membre și instituțiile UE în dezvoltarea și implementarea politicilor de securitate cibernetică, gestionarea incidentelor cibernetice majore, îmbunătățirea rezilienței infrastructurilor critice, dezvoltarea certificării europene pentru securitatea cibernetică.

Bibliography

Books

BJOLA, C. & HOLMES, M. (Eds.), *Digital Diplomacy: Theory and Practice*, Routledge, London–New York, 2015.

IFTIMOAEI, C., *Despre democrație, securitate și bună guvernare. România în context regional*, Editura Lumen, Iași, 2015.

Articles and studies

ABDUL, N., *Azerbaijan advances cybersecurity initiatives through strategic developments*, Azernews, 2024, https://www.azernews.az.

BARRINHA, A. & RENARD, T., *Cyber-Diplomacy: the making of an international society in the digital age*, Global Affaires, 2017, https://www.egmontinstitute.be.

CÎRNU, C.-E., VASILOIU, I.-C, Bridging the gap: an analysis of Cybersecurity in web technologies for Cyber diplomacy, *International Journal of Cyber Diplomacy*, Vol. 5, 2024, https://ijcd.ici.ro.

GABER, Y., *To help bring lasting peace to Ukraine, Turkey should enhance its cooperation on Black Sea security*, Atlantic Council, https://www.atlanticcouncil.org.

GEORGESCU, A. VEVERA, A.-V., CÎRNU, C.-E., *The Diplomacy of Systemic Governance in Cyberspace*, International Journal of Cyber Diplomacy, Vol. 1, Nr. 1, 2020, https://ijcd.ici.ro.

HOLLAND, S, OSBORN, A., and KORSUNSKAYA, D., *'No deal until there's a deal': Trump-Putin talks yield no breakthrough on Ukraine*, Reuters, https://www.reuters.com.

ISMAILZADE, F., *Digital Diplomacy in Azerbaijan: Lessons Learned and Future Opportunities*, in Bjola, C., Holmes, M. (Eds.), Digital Diplomacy in the OSCE Region, Contributions to International Relations, Springer, Cham, 2024, https://doi.org/10.1007/978-3-031-50966-7_2.

LEVITAN, J., *What Europe's Frozen Conflicts Mean for Black Sea Security*, International Conflict Resolution Center, https://icrcenter.org.

MIADZVETSKAYA, Y., & WESSEL, R., *The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox*, European Papers, Vol. 7, No. 1, 2022, pp. 413-438.

VASILOIU, I.-C., *A New Frontier for Global Cooperation in the Digital Age*, Informatica Economică, Vol. 27, Nr. 4, 2023, https://revistaie.ase.ro.

Websites and online platforms

AP NEWS, *Turkey, Bulgaria and Romania sign a deal to tackle Black Sea mines*, https://apnews.com.

CERT.GOV.AZ – Computer Emergency Response Team al State Service for Special Communication and Information Security (SCISSS), *Public bulletins and reports on confirmed incidents and associated categories (malicious links, fake domains, email problems)*, https://cert.gov.az/en/statistics.

CYBERPEACE INSTITUTE, *United Nations Cybersecurity Processes Explained*, https://cyberpeaceinstitute.org/united-nations-cybersecurity-process-explained.

DIGITAL WATCH OBSERVATORY, *The Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027*, https://dig.watch.

DNSC – Directoratul Național de Securitate Cibernetică, *Raport Anual*

2024, în secțiunea „Rapoarte și studii" (Documente), https://www.dnsc.ro.
ENISA – European Union Agency for Cybersecurity, *Cybersecurity Act (Regulation EU 2019/881)*, Athens–Heraklion, 2019, https://certification.enisa.europa.eu.
EUROPEAN COMMISSION, *Common Foreign and Security Policy*, https://commission.europa.eu.
EUROPEAN COMMISSION, *EU External Cyber Capacity Building Guidelines*, 2023, https://digital-strategy.ec.europa.eu.
MAE – Ministerul Afacerilor Externe (RO), *Inițiativa celor Trei Mări (I3M)*, https://www.mae.ro.
MAE – Ministerul Afacerilor Externe (RO), *Diplomație cibernetică și securitate cibernetică*, https://www.mae.ro.
MAE – Ministerul Afacerilor Externe (RO), *Comunicate privind cooperarea bilaterală cu Azerbaidjanul*, https://www.mae.ro.
NATO, *Prague Summit 2002. Selected Documents and Statements*, https://www.nato.int.
NATO, *Cyber Defence*, https://www.nato.int.
ICI Bucharest –National Institute For Research & Development In Informatics, *Short History*, https://ici.ro/en/short-history.
ICI București –Institutul Național de Cercetare-Dezvoltare În Informatică, *Cyber Diplomacy Center*, https://www.ici.ro/ro/centre-de-competenta/centrul-de-cyber-diplomacy.
SRI –Serviciul Român de Informații, *Cyber intelligence*, https://www.sri.ro/cyberintelligence.
IDEM, *Atacuri cibernetice asupra site-urilor unor instituții publice și financiar-bancare*, https://www.sri.ro/articole/atacuri-cibernetice-asupra-site-urilor-unor-institutii-publice-si-financiar-bancare.html.
UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS, *View of the Republic of Azerbaijan on Resolution 78/237 "Developments in the field of information and telecommunications in the context of international security"*, https://docs-library.unoda.org.
UNIUNEA EUROPEANĂ, *Convenția privind criminalitatea informatică*, https://eur-lex.europa.eu/RO/legal-content/summary/convention-on-cybercrime.html.
UNIUNEA EUROPEANĂ, *Strategia de securitate cibernetică a UE*, https://digital-strategy.ec.europa.eu/ro/policies/cybersecurity-strategy.

APPENDIX

Interview on the topic of Romanian-Azerbaijani Cooperation
in the field of Cyber Diplomacy

Introductory information

Interviewee Name: Dr. Fariz Ismailzade
Institution: ADA University, Azerbaijan, https://www.ada.edu.az
Position: Vice-Rector of ADA University, fismailzade@ada.edu.az
Role in the Cyber Diplomacy Twinning Center project: Coordinator

Section 1 – Motivation and context of cooperation

1. **What were the main motivations behind initiating the Romanian-Azerbaijani cooperation in the field of cybersecurity?**

Cybersecurity is becoming a very important part of everyday security, and all countries are paying more and more attention to it. Unfortunately, in many cases countries lack specialists and international experience on this issue so therefore, Azerbaijan has been cooperating with Romania on cybersecurity topic and getting the experience of Romanian experts, Romanian specialist, technology specialists, policy specialists, to increase their capabilities on the country, to increase the defense and protection capabilities so this was the main motivations behind initiating Romania and Azerbaijan cooperation.

2. **How did the signing of the Memorandum of Understanding (MoU) come about? Who were the key stakeholders?**

The signing of the MoU was suggested to us by the Azerbaijan State Agency, which is responsible for cybersecurity protection. They have decided that it's a good idea to organize trilateral cooperation, not only involving state bodies but also universities. Because a lot of training, discussions, conferences, and research take place at universities. Therefore, the initiative came from them, but it was a trilateral partnership, and I think this is the most important and most effective way of going forward with the cooperation to involve researchers, IT specialists, and faculty students. So that is a very efficient platform for cooperation.

3. **To what extent do you consider this collaboration to reflect global trends in cyber diplomacy?**

Well, I believe that this collaboration kind of reflects the global trends because all countries are moving in that direction, involving not only international partnerships but also multi-stakeholder partnerships, involving government agencies, the private sector, universities, and research centers. So, in our case, we haven't evolved any private companies yet, but among some of the participants, there might be some representatives of the private companies, so in the future, we might involve them as well. But overall, I think this is pretty much reflecting the global trend.

Section 2 – Objectives and expected Outcomes

4. What are the main strategic objectives of the Cyber Diplomacy Twinning Center?

Overall strategic objectives of this center is to do a lot of capacity building programs, training programs, also to do policy discussions, policy conferences to identify best ways to improve the legislation, to improve the rules, and regulations. Here we will discuss the training center, not only the capabilities of the personalities and individuals, but also the overall country's capabilities. And, I think that here we will be using a lot of experience coming from Romanian policy and research experience.

5. What concrete results (e.g., research projects, educational programs, workshops) have already been achieved or are currently being implemented?

So far, we have only implemented workshops, training programs with the involvement of various government agencies but in the future we are planning to do more conferences and workshops with the involvement of the private sector as well.

6. In what ways does this partnership contribute to the protection of critical information and communication infrastructures?

Azerbaijan is located at a very important strategic area, where bordered by Russia, Iran, Türkiye, and also in addition to nations, there are also some non-state actors involved in our region, including some criminal groups and international terrorist organizations. So, of course, protecting our communication infrastructure, critical information infrastructure as well as energy infrastructure, because Azerbaijan is an energy producer, it is very important for Azerbaijan, so protecting these infrastructure networks and improving the capabilities of the country is very important. There have been cases in the past where various countries or non-state actors have attacked Azerbaijan's infrastructure. So protecting it and making sure that it is at a good level is very important for the country.

Section 3 – Cooperation mechanisms and best practices

7. **What types of joint activities are carried out within the Center (e.g., expert exchanges, research, training)?**

As I mentioned in the previous question, № 5, so far, only a joint workshop has been done.

8. Have any best practices been identified and transferred between the partner organizations?

During that workshop, Romanian experts transformed their knowledge, skills, and information to Azerbaijani partners.

9. What diplomatic or institutional tools are being used to support transnational dialogue and collaboration?

I think that in the future we can involve diplomatic tools as well, because embassies are supporting such kind of cooperation and dialogue. We can involve and utilize the help of embassies and other governmental institutions.

Section 4 – Challenges and lessons learned

10. What lessons can be drawn from this initiative for other similar international cooperation projects in the digital domain?

Well, this is a very useful partnership. I think this can be multiplied and copied in other areas as well, in other areas of education and science. You know, Romania and Azerbaijani partnership is good for the region, wider Black Sea region, so I think that this partnership has been developed without many bureaucratic barriers, it was just a quick decision, quick implementation so therefore we should try to copy this in other areas as well.

11. How do you see this partnership evolving over the next 3–5 years?

I would be interested to see the next 3-5 years more training for technical specialists like IT specialists, programmers, and engineers.

12. Do you consider that Romania and Azerbaijan can become relevant regional actors in promoting cyber diplomacy?

Yes, I believe that if this partnership becomes successful, we can replicate it with other relevant regional actors involved in Central Asian countries or South Caucasus countries. This way, we can be a role model on this issue.

Final Questions

13. What recommendations do you have for other countries wishing to launch similar bilateral projects in the field of cyber diplomacy?

I would recommend that this kind of partnership should be fast promoted. Because technology, circumstances, and environment are changing. So, without too many bureaucratic approval processes, this can be approved quite fast.

14. Are there any aspects you would like to add that were not covered during this interview?

I would also be interested in discussing how we can involve students and use in such projects.