

# IDR

Romanian Diplomatic Institute



# NATO'S APPROACH TO CYBERSECURITY: THE 2022 CYBERATTACKS AGAINST ALBANIA

Claudiu Codreanu

Policy Paper no. 39/2024



MINISTERUL AFACERILOR EXTERNE



# NATO'S APPROACH TO CYBERSECURITY: THE 2022 CYBERATTACKS AGAINST ALBANIA

**Claudiu Codreanu**

*Researcher*

*Romanian Diplomatic Institute*

**ABSTRACT:** Cyberspace has entered the focus of virtually all international actors, and NATO states have been the target of malicious cyber operations during the last three decades. Major cyberattacks stemmed from state actors, such as those targeting Estonia in 2007 or the cyber and information campaigns targeting Euro-Atlantic democracies in 2015-2018. The statement issued after the 2014 Wales Summit first specifically mentioned that malicious cyber operations could reach a threshold for invoking Article 5, as long as their impact on societies amounts to that of conventional attacks. In this context, the 2022 Iranian cyber campaign targeting Albania represents one of the most disruptive and notable cyberattacks targeting a NATO member, especially considering Albania's decision of cutting diplomatic ties with Iran. Thus, this article examines NATO's approach to cybersecurity and its response to the Albanian case. The first part takes into account the issue of cyberspace and cybersecurity in NATO's strategic documents after 2002, including its 2022 Strategic Concept. The second part discusses the cyberattacks against Albania in 2022, attributed to Iran by Tirana and its Allies. Finally, the third part examines NATO's response to the Iran-Albania case, highlighting its vague messaging and publicly announced support offered to Tirana.

**KEYWORDS:** NATO, cyber operations, cybersecurity, Albania, Iran, Article 5.



## INTRODUCTION

Cyberspace has entered the focus of virtually all international actors, whether for protecting their own security from threats emerging from this domain, or for exploiting these new technological means to fulfil strategic objectives. Nevertheless, as much as the Internet is global, responses to cyber threats should also be collective. In this case, NATO can represent an example of international cooperation in bolstering cybersecurity, taking into account the already-close security collaboration of its member states. For instance, NATO's Locked Shields 2024 exercise has been declared by the Alliance as "the world's most advanced live-fire cyber defence exercise" (CCDCOE, 2024).

NATO states have been the target of malicious cyber operations during the last three decades. Major cyberattacks stemmed from state actors, such as those targeting Estonia in 2007 or the cyber and information campaigns targeting Euro-Atlantic democracies in 2015-2018. NATO as an organisation and its member states have not been an exception when it comes to being targeted by malicious cyber operations. Most recently, NATO issued a statement in May 2024 condemning Russia's campaign of cyber and hybrid operations against several of its member states (NATO, 2024b). The Alliance has also been the victim of a cyberattack originating from a hacktivist group in September 2023, which led to unclassified NATO documents being posted online (Lyngaas, 2023). In addition to this, Albania was targeted in 2022 by a serious campaign of cyberattacks attributed to Iran, which led to Tirana taking the decision of deteriorating diplomatic ties with Teheran. However, despite NATO's progress in adopting clear stances and strategies on cybersecurity, its response was rather vague both in announced immediate aid and public statements. Albania even considered invoking Article 5 of the North Atlantic Treaty (Grossman, 2023). NATO recognized that malicious cyber operations can lead to invoking Article 5 (Valášek, 2020, 42).

As the Iranian cyberattacks on Albania were the first ones leading to the targeted state severing diplomatic ties with the attacker (Higgins, 2023), this article examines NATO's approach to cybersecurity and its response to the Albanian case. The first part takes into account the issue of cyberspace and cybersecurity in NATO's strategic documents after 2002, including its 2022 Strategic Concept. The second part discusses the cyberattacks against Albania in 2022, attributed to Iran by Tirana and its Allies. Finally, the third part examines NATO's response to



the Iran-Albania case, highlighting its vague messaging and publicly announced support offered to Tirana. The last section also mentions the case of EU cyber assistance offered to the Republic of Moldova, in which Romania plays a key role.

## **THE ISSUE OF CYBERSECURITY IN NATO'S STRATEGIC DOCUMENTS**

NATO's interest and concern regarding threats emerging from cyberspace and from the manipulation of cyber means gained traction after the first hacktivist cyberattacks targeting the organisation during its intervention in the Kosovo War. The 2002 Prague Summit and 2006 Riga Summit highlighted the issues of enhancing cybersecurity in the face of emergent malicious activities and exploiting technological advances for bolstering NATO's security and operations (Efthymiopoulos, 2024). Less than one year after the major cyberattacks against Estonia in 2007, NATO adopted its first Policy on Cyber Defence, as the events in Estonia showcased the strategic importance of cyberspace (NATO, 2024d; Efthymiopoulos, 2024). Moreover, the first Strategic Concept recognising that cyberattacks could amount to a threat to Allies' security and stability was adopted at the 2010 NATO Summit in Lisbon (NATO, 2024d). Another major development that led to this is Russia's use of cyberattacks combined with kinetic attacks during the Russo-Georgian war in August 2008. At the 2014 and 2016 summits, NATO emphasized the necessity of enhancing cooperation with the private sector on cybersecurity (Efthymiopoulos, 2024).

The 2011 revised NATO Cyber Policy first mentioned that the Alliance could employ a collective response to a cyber operation whilst maintaining its flexibility and strategic ambiguity (Grossman, 2023, 21). The statement issued after the 2014 Wales Summit first specifically mentioned that malicious cyber operations could reach a threshold for invoking Article 5, as long as their impact on societies amounts to that of conventional attacks (Grossman, 2023, 22). Over the following decade, cybersecurity became one of the organisation's main priorities (Efthymiopoulos, 2024). In 2016 Allies endorsed a Cyber Defence Pledge and in 2021 they adopted a Comprehensive Cyber Defence Policy (NATO, 2024d). Moreover, the NATO communique following the 2016 Warsaw Summit declared cyberspace as an operation domain, alongside air, land, and sea (Grossman, 2023, 23). Allies adopted a new concept for cyber defence at the 2023 summit in Vilnius, placing emphasis on ensuring civil-military cooperation and enhancing collaboration with the private sector



(NATO, 2024d). In addition to this, NATO has plans to enhance its partnerships with the private sector in the area of space defence (Davies, 2024). NATO adopted its Space Policy in 2019, recognising it as the fifth operational domain, beside land, air, sea, and cyberspace (Davies, 2024).

NATO's 2022 Strategic Concept sets clear the organization's position on cyber issues. The Alliance recognizes that authoritarian actors undergo efforts to undermine international norms and democratic institutions, interfering in democratic processes through cyber and information means (NATO, 2022a, 3). The document gives the example of Russia and China's cyber and disinformation tactics, but mentions Iran only regarding its nuclear programme (NATO, 2022a, 3-5). Continuing the formula set in the summit declarations and other communiqués over the years, the 2022 Strategic Concept states that "cyberspace is contested at all times" (NATO, 2022a, 5). The Alliance sets out the objective of bolstering its abilities to counter cyberspace, alongside space, threats, emphasizing that a singular or series of cyber operations could lead to invoking Article 5 (NATO, 2022a, 5-7). Russia and China are stated by NATO as examples of states pursuing malicious hybrid and cyber campaigns, highlighting the role of cyber operations in Russia's war of aggression against Ukraine, and China's cyber and disinformation campaigns (NATO, 2024d).

Regarding its institutional framework, the North Atlantic Council (NAC) offers high-level oversight of all major policies and operations, including cyber defence (Grossman, 2023, 24). Subordinated to the NAC is the Cyber Defence Committee, the main body for cyber defence policy, providing advice and oversight to member states on Allied cyber defence endeavours (Grossman, 2023, 24). Coordinated by this committee is the NATO Chief Information Officer, which manages the NATO Communications and Incident Response Capability, from where Rapid Response Teams are formed (Grossman, 2023, 25). The North Atlantic Council must approve requests for assistance, and Rapid Response Teams ought to become available for deployment within 24-hours (Grossman, 2023, 25).

In the area of cyber defence, NATO's main priorities are protecting its own networks, operating in cyberspace, and aiding member states to bolster their cyber defences whilst providing a platform for collective action and political consultation (NATO, 2024d). Most cybersecurity measures that can aid NATO's efforts depend on policies and practices implemented by its member states and on the European Union (Valášek, 2020, 42). NATO's own networks are protected by the NATO Cyber Security Centre (NCSC), based at the

Supreme Headquarters Allied Powers Europe (SHAPE). Besides NCSC, NATO's operation activity in cyberspace is ensured by the Cyberspace Operation Centre, which also provides military commanders with support on situational awareness (NATO, 2024d). Even though its member states are pursuing cyber defence activities, including striking back capabilities, and NATO is enhancing its position to defend its military networks, member states' civilian critical infrastructure remains vulnerable (Valášek, 2020, 42).

Advancing the same values and principles as the US, EU and its member states, Allies are promoting a peaceful, secure, free, and open cyberspace, stating their support for the voluntary norms of responsible state behaviour and cyberspace and international law in this domain (NATO, 2024d). Nevertheless, despite all these efforts and developments, there are still differences in cybersecurity legislations and approaches between member states and NATO, which hinder the Alliance's coordinated operations in this domain (Efthymiopoulos, 2024). Thus, NATO depends on national capabilities contributed by member states to the Alliance for most cyber operations (Grossman, 2023, 23).

## **THE 2022 IRANIAN CYBERATTACKS AGAINST ALBANIA**

The 2022 Iranian cyber campaign targeting Albania represents one of the most disruptive cyberattacks against a European NATO member since 2007 (Higgins, 2023). The incident is notable, as it was the first time a government responded by cutting diplomatic ties with the country found responsible of targeting it with cyberattacks (Grossman, 2023, 29). Albania severed diplomatic relations with Iran on September 6, 2022, expelling all diplomatic staff at the Embassy in Tirana (Grossman, 2023, 29; Higgins, 2023).

The cyberattacks against Albania have been in preparation at least since 2021, when the covert penetration of government networks began (Higgins, 2023). The first attacks targeted government services associated with the administrative domain in May 2022 (Grossman, 2023, 29). The campaign continued in July 2022 with attacks against e-albania.al, a government portal used for various services, including applying for official documents (Grossman, 2023, 29). The malicious cyber campaign seriously disrupted routine activities of citizens, as almost 95% of Albanian government services are provided online (Grossman, 2023, 29). The attackers first downloaded data from servers and then started deleting them, which hindered government services (Higgins, 2023). However, the government said that the hackers did not manage to

delete sensitive data (Miller, 2022). The cyber campaign disrupted government activities and public services alongside seeking to undermine citizens' trust in financial institutions (Higgins, 2023). In order to undermine trust in financial institutions and the government, the hackers targeted clients of several major banks with fake messages that their accounts have been withdrawn (Higgins, 2023). The cyberattacks forced the government to take offline its websites, suspending online services such as obtaining official documents or paying utilities, among others (Miller, 2022). The hacks were followed by a series of leaks of confidential information (Higgins, 2023). The campaign employed in early summer was followed by several new cyberattacks in September 2022, when Iranian hackers managed to disrupt platforms used by Albania in border and customs processing (Miller, 2022).

Highlighting the close cooperation needed with the private sector, Albania hired Microsoft to investigate the cyber operation. In a later report, the company attributed the attack to “actors sponsored by the Iranian government”, stating that Mujahedeen Khalq (M.E.K.) was the primary target (Higgins, 2023). Moreover, Microsoft assessed that the attacks might represent retaliation to cyberattacks perceived by Teheran as launched by Israel in collaboration with M.E.K. (Higgins, 2023). The most probable reason for Iran's cyber operation is Tirana's decision to offer shelter in the country to M.E.K., an Iranian dissident group once designated as a terrorist organisation by the US but backed now by several Washington political groups (Higgins, 2023).

The cyber operations were officially attributed to Iran by Albania and several Allies (Grossman, 2023, 29). The US issued a statement attributing the cyberattacks to Iran and condemning Teheran. The statement emphasizes that Iran's actions go against the norms of responsible state behaviour in cyberspace (White House, 2022). The US Justice Department issued indictments for alleged Iranian hackers involved, as the Treasury Department announced sanctions against Iran's intelligence agency and its leader (Miller, 2022). The Federal Bureau of Investigation (FBI) and the Cybersecurity Infrastructure Security Agency (CISA) issued a joint message in September 2022 highlighting the course of action through which Iranian hackers carried the cyberattacks (Miller, 2022). Prime Minister Edi Rama stated that the US provided assistance for dealing with the malicious cyber campaign, including in-person expertise (Miller, 2022).



## NATO'S RESPONSE: NO MAJOR CHANGES IN CYBERSECURITY POLITICS

Low-intensity cyber and hybrid operations are a constant, and even though they represent attempts of probing defences and capabilities, sometimes they disguise routine preparations for serious disruptions (Missiroli, 2020, 68). Moreover, hybrid campaigns involve a combination of cyber and information means, such as hack-and-leak operations (also referred to with the Russian term *kompromat*), social media influence operations, and attempts to shape voting preferences (Missiroli, 2020, 69).

NATO offered limited details regarding actions taken to aid Albania's cyber defence (Grossman, 2023, 30). Moreover, the statement issued following the cyberattacks did not mention information about NATO Cyber Rapid Reaction Teams (Grossman, 2023, 30). NATO issued a statement on September 8, 2022, condemning the cyberattack and stating that Albania and "other Allies" attributed the operation to Iran (NATO, 2022b). In its response, NATO made references to international law and the voluntary norms of responsible state behaviour in cyberspace. Moreover, it highlighted the Allies' commitment to enhance their cyber defences and protect their critical infrastructure, including by weighing potential collective responses (NATO, 2022b).

This is also reflected in the communiqués issued after summits taking place in this period. NATO's statement issued after the 2022 Madrid Summit mentions cyber alongside space and hybrid threats, and emerging and disruptive technologies (NATO, 2022c). The statement emphasized that NATO will work on aiding Ukraine in the face of the renewed Russian war of aggression, including efforts for boosting the country's cyber defence (NATO, 2022c). The statement mentions that the Alliance will enhance its resilience to cyber threats, strengthening interoperability, improving civil-military cooperation and engagement with the private sector (NATO, 2022c).

One year before, the 2021 Brussels Summit statement mentions that the organisation approved its new Comprehensive Cyber Defence Policy (NATO, 2021). The communique states that political consultation between Allies regarding cyber threats will be enhanced (NATO, 2021). The statement reaffirms that NATO will deter, defend against, and counter cyber threats through a complete set of capabilities, emphasizing that it will impose costs to cyberattackers unrestricted to the cyber domain (NATO, 2021).



One year after the cyberattacks against Albania, the 2023 Vilnius Summit's communique does not provide major changes in the Alliance's approach to cybersecurity and cyberspace, and it does not mention, even vaguely, the Albanian case. NATO reiterates that it is countering hybrid campaigns with cyber components which target its democratic processes and crucial infrastructure (NATO, 2023). The statement reiterated, as stated in the 2022 Strategic Concept, that an individual or coordinated series of cyber operations targeting NATO could lead to invoking Article 5 (NATO, 2023). In 2023, the Alliance approved a new concept for enhancing cyber defence on three levels: political, military, and technical, with an emphasis on civil-military cooperation and partnerships with the private sector (NATO, 2023).

The statement issued after the 2024 Washington Summit highlights that cyber capabilities are part of NATO's deterrence and defence posture capabilities, alongside nuclear, conventional, missile defence and space capabilities (NATO, 2024c). As stated at least since 2021, NATO reiterates that it promotes a free, open, peaceful, and secure cyberspace, highlighting the support for international law in cyberspace and the voluntary norms of responsible state behaviour in cyberspace (NATO, 2024c). Moreover, Allies agreed to establish its new NATO Integrated Cyber Defence Centre in July 2024. The Centre has the role of informing the military command of the Alliance on cyber threats and vulnerabilities, including those stemming from privately-owned civilian critical infrastructure supporting military activities (NATO, 2024a).

The 2024 communique mentions China as a state that poses "systemic challenges to Euro-Atlantic security", stemming from cyber, disinformation and hybrid campaigns (NATO, 2024c). Moreover, Russia's malicious activities against Allied members are mentioned, including malicious cyber activities and disinformation campaigns (NATO, 2024c). Conversely, the European Union is mentioned as a "unique and essential partner" for the Alliance, adding that concrete cooperation has been bolstered in the domain of cyberspace, alongside space, climate, defence, and emerging and disruptive technologies (NATO, 2024c). Moreover, NATO mentions that it is boosting its concrete cooperation for supporting Ukraine, including on cyber defence, technology, and countering disinformation campaigns (NATO, 2024c). For instance, Ukraine joined NATO's Cooperative Cyber Defence Centre of Excellence in May 2023, alongside Iceland, Ireland, and Japan (Martin, 2023). Even though the Alliance mobilized significant amounts of aid packages for Ukraine after Russia's renewed invasion, it did not offer too much detail regarding actions taken to support Ukraine's cyber



defences (Grossman, 2023, 28). Another non-NATO and non-EU country facing Russian hybrid campaigns, the Republic of Moldova, already received bilateral assistance programs in cybersecurity from Czechia and Romania since 2022, with the latter country's program set to run until 2026 (Grossman, 2023, 31). Furthermore, the EU Cyber Rapid Response Team provided support to the Republic of Moldova in November 2022 and April 2023 (Grossman, 2023, 31).

Nevertheless, none of the statements issued after 2021 mention Iran's activities in cyberspace as a threat or challenge to Euro-Atlantic security. Only the 2024 statement notes that Teheran's "destabilising actions are affecting Euro-Atlantic security", but without mentioning the cyber aspect. Albania sought NATO support during the cyber operations, Prime Minister Edi Rama stating publicly that the government even considered invoking Article 5, but it ultimately decided against it (Grossman, 2023, 29). However, Albania did not request and NATO did not provide the help of a Rapid Response Team, and nor did the EU (Grossman, 2023, 29). NATO had the tools to respond if needed, as the 2021 Cyber Defence Policy notes that Cyber Rapid Response Team would be on standby thereafter for ensuring a 24-hour response capability (Grossman, 2023, 24). To assess the effects of the cyber campaign and Allied support, NATO representatives met with then-Defence Minister of Albania, Niko Peleshi, in September 2022 (Grossman, 2023, 30). Moreover, the United States deployed a defensive hunt forward team to provide assistance for three months, the operation taking place in March 2023 according to the US Cyber Command (Grossman, 2023, 30).

## CONCLUSIONS

NATO's approach to cybersecurity has matured over the last two decades, as showcased by its Strategic Concepts, summit communiqués, and policies adopted. Major cyberattacks, such as those targeting Estonia in 2007, and major international events, such as Russia's hybrid war against Ukraine in 2014 and full-blown invasion in 2022, played a crucial role in shaping the organisation's cyber policies and practices. Even though NATO's response to Iran's cyberattacks against Albania was rather vague, it is important to notice that Albania was concretely aided by one of NATO's most prominent members, the US. However, as cybersecurity is an ever-changing domain due to both technological advances in Artificial



Intelligence, quantum computing, space technologies and so on, and international security developments, NATO's policies should also be kept in touch with the latest events.

As actively protecting the national networks of member states is out of the scope of the Alliance, a recommendation should be actively preventing cyberattacks against NATO networks and critical infrastructure, instead of only responding to malicious cyber operations and addressing vulnerabilities (Efthymiopoulos, 2024). However, this policy would need close coordination with all its member states, which have different legislations and approaches to cybersecurity practices.

Emerging and disruptive technologies constitute means for hybrid and influence campaigns that aim at undermining NATO's and its member states' institutions, democratic processes, resilience, and social cohesion (Bellasio & Silfversten, 2020, 98). In this context, NATO adopted an Emerging and Disruptive Technology Implementation Roadmap in 2019, which tends to developments in AI software, autonomous systems, quantum technologies and so on (Csernaton, 2024). Thus, enhancing cooperation with the tech industry, and more general with the private sector, will be crucial to bolstering NATO's cyber defences and exploiting technological advances in all domains (Bellasio & Silfversten, 2020, 102). In a report for ETH Zürich, Taylor Grossman (2023, 29) highlights that private tech companies and individual countries have been able to provide aid in the cyber domain to Ukraine much more quickly than NATO or the EU. Therefore, NATO should take steps to shape its policies and practices in all domains harnessing cyber innovation and countering cyber threats (Bellasio & Silfversten, 2020, 100-101).

NATO and EU can and should improve their cooperation on countering hybrid, and especially cyber, threats (Missiroli, 2020, 70). NATO already works with the EU on cyber issues, coordinating their efforts to counter cyber and hybrid threats through sharing information and exchanging best practices between their rapid response teams (NATO, 2024d). Moreover, NATO and EU have collaborated in the area of cybersecurity and countering disinformation campaigns, such as the support provided for establishing the European Centre of Excellence for Countering Hybrid Threats (Lété & Pernik, 2017, 3). Thus, NATO should enhance its collaboration with ENISA (the EU Agency for Cybersecurity) and the newly-established ECCC (European Cybersecurity Competence Centre), especially when it comes to partnerships with the private sector, academia, or civil society. As Romania not only hosts ECCC's headquarters, but is already an important player in aiding the cybersecurity of NATO



and EU partners, Bucharest could also play a key role in solidifying NATO-EU cooperation on cybersecurity.

## BIBLIOGRAPHY

- Bellasio, J. & Silfversten, E. (2020). The Impact of New and Emerging Technologies on The Cyber Threat Landscape and Their Implications for NATO. In A. Ertan, K. Floyd, P. Pernik & T. Stevens (Eds.), *Cyber Threat and NATO 2030: Horizon Scanning and Analysis* (pp. 88-109). CCDCOE. <https://ccdcoe.org/library/publications/cyber-threats-and-nato-2030-horizon-scanning-and-analysis/>
- CCDCOE (2024). *Locked Shields 2024 demonstrated the real power of cooperative defence*. <https://ccdcoe.org/news/2024/locked-shields-2024-demonstrated-the-real-power-of-cooperative-defence/>
- Csernatoni, R. (2024, July 17). *How to future-proof NATO's defence innovation and EDT strategy*. CEPS. <https://www.ceps.eu/how-to-future-proof-natos-defence-innovation-and-edt-strategy>
- Davies, P. (2024, May 11). *NATO wants to work with tech start-ups on space defence. Secrecy is proving to be a huge obstacle*. Euronews <https://www.euronews.com/next/2024/05/11/nato-wants-to-work-with-tech-start-ups-on-space-defence-secrecy-is-proving-to-be-a-huge-ob>
- Efthymiopoulos, M. P. (2024, March 9). *NATO: Time to Adopt a Pre-emptive Approach to Cyber Security in New Age Security Architecture*. Georgetown Journal of International Affairs. <https://gjia.georgetown.edu/2024/03/09/nato-time-to-adopt-a-pre-emptive-approach-to-cyber-security-in-new-age-security-architecture/>
- Grossman, T. (2023). *Cyber Rapid Response Teams: Structure, Organization, and Use Cases*. CSS ETH Zürich. <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2023-11-Cyber-Rapid-Response-Teams.pdf>
- Higgins, A. (2023, February 25). *A NATO Minnow Reels from Cyberattacks Linked to Iran*. New York Times. <https://www.nytimes.com/2023/02/25/world/europe/albania-iran-nato-cyberattacks.html>

- Lété, B. & Pernik, P. (2017). *EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions*. GMF Policy Brief, no. 38. <https://www.gmfus.org/sites/default/files/EU-NATO%2520Cybersecurity%2520and%2520Defense%2520Cooperation%2520edit.pdf>
- Lyngaas, S. (2023, October 3). *NATO says it is addressing an apparent cyberattack after strategy documents posted online*. CNN. <https://edition.cnn.com/2023/10/03/politics/nato-cyber-attack-strategy/index.html>
- Martin, A. (2023, May 17). *Ukraine, Ireland, Iceland and Japan officially join NATO's cyber defense center*. The Record Media. <https://therecord.media/nato-ccdcoe-ukraine-iceland-ireland-japan>
- Miller, M. (2022, October 5). *Albania weighed invoking NATO's Article 5 over Iranian cyberattack*. Politico. <https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347>
- Missiroli, A. (2020). From hybrid warfare to “cybrid” campaigns: the new normal?. In T. Tardy (Ed.), *NATO at 70: No Time to Retire* (pp. 65-72). NATO Defence College. <https://www.ndc.nato.int/news/news.php?icode=1414>
- NATO (2021). *Brussels Summit Communiqué*. [https://www.nato.int/cps/en/natohq/news\\_185000.htm](https://www.nato.int/cps/en/natohq/news_185000.htm)
- NATO (2022a). *NATO 2022 Strategic Concept*. [https://www.nato.int/cps/en/natohq/topics\\_210907.htm](https://www.nato.int/cps/en/natohq/topics_210907.htm)
- NATO (2022b). *Statement by the North Atlantic Council concerning the malicious cyber activities against Albania*. [https://www.nato.int/cps/en/natohq/official\\_texts\\_207156.htm](https://www.nato.int/cps/en/natohq/official_texts_207156.htm)
- NATO (2022c). *Madrid Summit Declaration*. [https://www.nato.int/cps/en/natohq/official\\_texts\\_196951.htm](https://www.nato.int/cps/en/natohq/official_texts_196951.htm)
- NATO (2023). *Vilnius Summit Communiqué*. [https://www.nato.int/cps/en/natohq/official\\_texts\\_217320.htm](https://www.nato.int/cps/en/natohq/official_texts_217320.htm)
- NATO (2024a). *Allies agree new NATO Integrated Cyber Defence Centre*. [https://www.nato.int/cps/en/natohq/news\\_227647.htm](https://www.nato.int/cps/en/natohq/news_227647.htm)
- NATO (2024b). *Statement by the North Atlantic Council on recent Russian hybrid activities*. [https://www.nato.int/cps/en/natohq/official\\_texts\\_225230.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/official_texts_225230.htm?selectedLocale=en)



NATO (2024c). *Washington Summit Declaration*.

[https://www.nato.int/cps/en/natohq/official\\_texts\\_227678.htm](https://www.nato.int/cps/en/natohq/official_texts_227678.htm)

NATO (2024d). Cyber defence. [https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm)

Valášek, T. (2020). NATO at 70: enter the technological age. In T. Tardy (Ed.), *NATO at 70: No Time to Retire* (pp. 41-48). <https://www.ndc.nato.int/news/news.php?icode=1414>

White House (2022, September 7). *Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania*. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/07/statement-by-nsc-spokesperson-adrienne-watson-on-irans-cyberattack-against-albania/>

# IDR

Institutul Diplomatic Român

**Our mission.** The Romanian Diplomatic Institute (RDI) has the mission to make a substantial contribution to increasing the quality of Romanian diplomacy through training, further education, research, the development of critical and strategic thinking and international networking. A good foreign policy serves as a beneficial domestic policy.

**Guiding principles:** human resource development, professionalism, respect and dialogue, and responsibility for the community.

Based on the founding legal attributions of the RDI, the further development of the Institute is carried out, according to the needs identified in the MFA, along the following four directions:

- Training and further education of diplomats and other trainees;
- Deepening the research and expertise dimension on regional and functional issues;
- Operating the RDI as a think-tank of the MFA;
- Integration of the RDI into an international network of similar relevant institutes.

Author: Claudiu Codreanu is a researcher at the Romanian Diplomatic Institute – Department of Expert Analysis.

RDI Policy Paper series

ISSN 2285-8938

ISSN-L 2285-8938

Cover photo: <https://unsplash.com/photos/macro-photography-of-black-circuit-board-FO7JllwjOtU>

The Romanian Diplomatic Institute

<https://www.idr.ro/en/> | [secretariat@idr.ro](mailto:secretariat@idr.ro)

Primăverii 17, sector 1, Bucharest, 011972