CYBERDEFENSE REPORT

Romania's National Cybersecurity and Defense Posture

Policy and Organizations

Zürich, October 2020

Cyberdefense Project (CDP)
Center for Security Studies (CSS), ETH Zürich

CSS ETH Zurich

ETH zürich

Available online at: css.ethz.ch/en/publications/risk-and-resilience-reports.html

Author: Alice Crelier

ETH-CSS project management: Myriam Dunn Cavelty Deputy Head for Research and Teaching; Benjamin Scharte, Head of the Risk and Resilience Team; Andreas Wenger, Director of the CSS.

Editor: Alice Crelier, Jakob Bund
Layout and graphics: Miriam Dahinden-Ganzoni

© 2020 Center for Security Studies (CSS), ETH Zurich

DOI: 10.3929/ethz-b-000445557

Table of Contents

1 Introduction

Romania, as a full member of both NATO and the EU, is playing an increasingly important role in cybersecurity and cyberdefense, both regionally and internationally. Romania promotes an open and competitive national information and communication technologies market that works hand in hand with the public cybersecurity structures. Its geopolitical position, on the frontlines of the conflicts surrounding the Black Sea, triggers a growing sense of insecurity at the national level that reflects the country's current cybersecurity and cyberdefense posture and its increasing international cooperation and engagements, especially with the EU and NATO.

1.1 Key National Trends

During the Cold War, Romania was part of the Eastern Block and was ruled by a communist dictatorship. After the fall of communism 1989, Romania sought to foster strong relations with the US, its new main ally, and aligned itself with NATO and the EU. Romania eventually joined NATO in 2004 and the EU in 2007. By doing so, Romania reaffirmed its political position along Western countries.

Geographically, Romania is situated in the middle of continental Europe, along the Eastern border of the EU and has access to the Black Sea. This geopolitical situation is directly reflected by the country's defense and foreign policy that focuses on strong cooperation with Western countries and institutions. For example, Romania increasingly welcomes and participates in large joint NATO exercises on its territory.

The conflict in Ukraine and the disputes over Transnistria increased Romania's perceptions of insecurity and reaffirmed Romania's "traditional fears of foreign aggression" (Stratfor Worldview 2019). Deteriorating security on Europe's eastern flank and the Black Sea region and the emergence or intensification of new threats – hybrid threats and cyber threats like cyber espionage and malicious cyber campaigns against government websites – pushed Romania towards an intensification of cooperation with the US (Lesser 2007; Melvin 2018). Because of its political alliances and its geographical position, Romania has increasingly been considered as a buffer state between a Western core and Russia's interests. Romania's own geographic location and its participation in international programs in countries that are at the fault line of these geopolitical forces, like Ukraine (e.g. through the NATO Trust Fund for developing Ukraine's cyberdefense), further intensified the aforementioned threats.

Romania adopted an economic model that gives large freedom to private companies. This approach has helped Romania to develop a vibrant information security sector. Information and communication technologies (ICT) have become one of the most important pillars of the country's economy, even if compared at international levels, Romania is not among the leading nations (Alexe 2019; Eremia 2019).

Romania inherited a strong and omnipresent intelligence apparatus from Cold War times, represented by the National Information Community[1] (NIC). Even though cyberdefense and cybersecurity are de jure decentralized at the operational level, the fact that the national cyber intelligence center is the designated national cybersecurity authority and the presence of intelligence offices in almost every ministry de facto centralize cybersecurity and cyberdefense under the aegis of Romania's intelligence community.

Cyberdefense

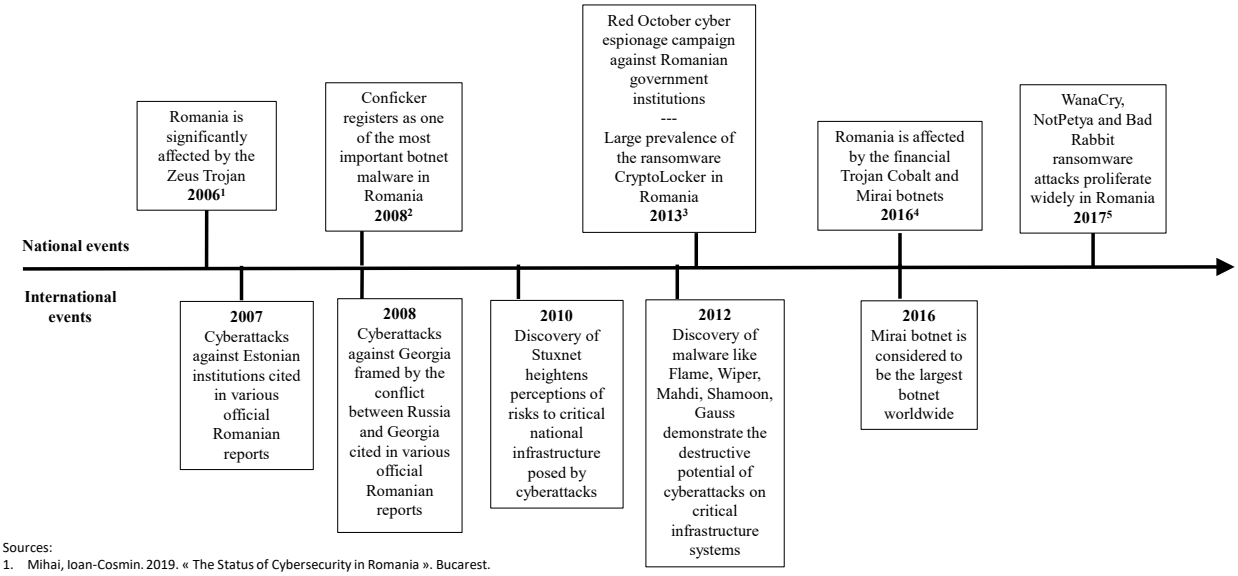
Romania organizes its cyberdefense measures through the National Defense Strategy and in accordance with its Cybersecurity Strategy. The Ministry of National Defense coordinates Romania's cyberdefense through its tight collaboration with the Romanian national cyber intelligence center called Cyberint Center (CIC).

The following diagram describes the main international and domestic cybersecurity and cyberdefense-related events that shaped Romania's policies. Several cyberattacks are mentioned in government releases and in international organizations' reports as trigger points and reasons for significant shifts in Romania's cybersecurity and cyberdefense policies[2] (Mihai 2019; Cocolan, s. d.; Vevera 2014).

[1] Comunitatea Naţională de Informaţii

[2] References to incidents and events in this diagram are limited to the main developments shaping the cybersecurity - and - defense polices analyzed in this study.

Diagram 1: Timeline of Trigger Events



Sources:
1. Mihai, Ioan-Cosmin. 2019. « The Status of Cybersecurity in Romania ». Bucarest.
2. *Idem.*
3. Ackermann, Robert K. 2016. « Romania Battles State Actors in Cyberspace ». SIGNAL Magazine, 27
4. Mihai, Ioan-Cosmin. 2019. *Ibid.*
5. *Idem.*

1.2 Fundamentals of the National Framework

Cybersecurity

Romania's cybersecurity and cyberdefense are both part of the National Cybersecurity System that helps the cooperation at both strategic and operational levels of Romania's cybersecurity institutions (in both the public and private sectors). The Supreme Council of National Defense, along with the Ministry for Communication and the Information Society, leads Romania's cybersecurity policy at the strategic level. At the operational level, Romanian cybersecurity is led by the CIC, in close cooperation with the Ministry for Communication and the Information Society and other cybersecurity-related institutions.

Cyberdefense

The Romanian Armed Forces' main cyberdefense institution is the Cybernetic Defense Command. The command structure is part of the Ministry of National Defense (MoND) and works in tight collaboration with the CIC. Military cyberdefense focuses both on defensive and offensive capabilities and is responsible for the protection of the information and communication infrastructures of the MoND and the armed forces.

1.3 Key Organizational Structures

At the strategic level, Romania's organizational structure for cybersecurity and cyberdefense is centralized. At the operational level, however, Romania's cybersecurity and cyberdefense structure is decentralized – but the decision-making is concentrated within Romania's intelligence institutions that are dispersed across the administrative apparatus. The Romanian Government leads on issues of national cybersecurity and cyberdefense through the Supreme Council of National Defense (SCND)[3], while the Ministry for Communication and Information Society[4] (MCIS) is responsible for policy development. The MCIS mainly focusses on the governmental, social, and economic aspects of cyber issues. Efforts by the MCIS in this vein highlight the importance of the development and support of a strong and competitive Romanian ICT market. The MCIS also recognizes the importance of good international cooperation with regard to the cyber domain, especially with the US, NATO, and the EU. The CIC is subordinated to the Romanian Intelligence

[3] Consiliu Suprem de Apărare a Ţării. For consistency and ease of reading, titles of policy documents and relevant agencies will be rendered in English with English abbreviations, while original titles will be provided in footnotes. For a full list of documents, abbreviations and Romanian-English equivalency, see Annex 3.

[4] Ministerul Comunicațiilor și Societății Informaționale

Service[5] (RIS) and is the responsible body, along with the Romanian National Computer Security Incident Response Team[6] (CERT-RO), for national cybersecurity (incident response, coordination and resolution, proactive mitigation measures, national and international information sharing). The Ministry of National Defense[7] (MoND) is responsible for the cyberdefense and the maintenance of its own ICT networks and cooperates with the CIC and with the CERT-RO. This collaboration includes MoND's networks-related incident response, coordination and resolution as well as information sharing).

1.4 Partnerships

Romania's key partners with regard to cybersecurity issues are its allies within the EU and NATO. On a bilateral basis, close cooperation has been established with the United States. Romania has also developed numerous public-private partnerships.

[5] Serviciul Român de Informaţii

[6] Hotărâre nr.494 din 11.05.2011 privind înfiinţarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică -CERT-RO, 2011

[7] Ministrul Apărării Naţionale

2 Cybersecurity Policy

2.1 Overview of Key Policy Documents

2.1.1 Cybersecurity Strategy of Romania, 2013[8](CSR)

The Cybersecurity Strategy of Romania adopted in 2013 is Romania's first cybersecurity strategy and details the country's cybersecurity policy. The Romanian Government issued the CSR as a response to the EU's regulatory process with regard to cybersecurity and in compliance with Romanian Government decision 489 of 2011 on the establishment of the CERT-RO. The CSR explains the contextual framework of cybersecurity in Romania –rapid development of ICT, the benefits of digitalization and the vulnerabilities linked to it. The goal of the CSR is to protect national interests with regard to cybersecurity, while being in compliance with the goals of the National Strategy for Critical Infrastructure Protection[9] and the National Defense Strategy 2020-2024[10] (NDS). The strategy states eight goals that heavily focus on creating an integrated national system called the National Cyber Security System[11] (NCSS) responsible for the implementation of all measures for preventing and responding to cyberattacks and cyber incidents. In addition, the strategy in its goals emphasizes development of cooperation and adaption of standards regarding cyberdefense in line with the EU, NATO and the US.

2.1.2 Proposal for the Cybersecurity Law, 2014[12] (PCL)

In order to align its cybersecurity policy with the EU and NATO – and without any public consultation – the Romanian Government developed the Proposal for the Cybersecurity Law. This bill was submitted to the Parliament, which accepted it in December 2014 without publicity. However, the document generated controversies and members of the Parliament and 13 non-governmental organizations strongly opposed the adoption of this law, many provisions of which they considered unconstitutional. Eventually, the Constitutional Court struck down the Cybersecurity Law in its entirety on January 2015 because it violated provisions contained in at least eight articles of Romanian constitution: " Articles 1(3) and (5), 21, 23(1), 26, 28, 53, 119, 148 concerning state sovereignty and the rule of law, access to justice, personal freedom and safety, private life, communications secrecy, limitations to the exercise of certain rights or freedoms, respecting the attributions of the Supreme Council for National Defense as well as complying with European Union treaties" (Jasmontaite et Burloiu 2017).

The sweeping scope of the PCL sought to extend regulatory powers over all legal entities in both the public and private sector that use ICT and handle personal data without indicating any data protection measures in case of misuse. This expansion would have included journalistic outlets and non-governmental organizations (NGOs).

Moreover, the governmental authorities in charge of cybersecurity – predominantly the Romanian Intelligence Service – would have been granted access to ICT systems and logs of data-hosting providers without additional prior legal authorization. Finally, the PCL elevated the RIS as the national authority on cybersecurity questions and assigned the agency the lead on Romanian cybersecurity. Since 2015, the PCL has been revised several times but is still – as of October 2020 –not yet adopted (Turcu 2016; Jasmontaite et Burloiu 2017; CYBERWISER.eu 2019).

2.1.3 National Defense Strategy 2020-2024, 2020 (NDS)

The National Defense Strategy 2020-2024, entitled "Together, for a safe and prosperous Romania in a world marked by new challenges", builds on a series of planning documents: the 1991 Law of National Security of Romania, the 1994 Law of National Defense of Romania, Romania's 2001 National Security Strategy, Romania's Military Strategy 2002-2004, the 2004 White Paper on Government Security, the National Defense, the Law on the Planning of the National Defense of Romania, the National Defense Strategy 2008-2015, and especially on the National Defense Strategy 2015-2019 of 2015.

The National Defense Strategy, published in July 2020, is the latest national defense strategy issued by the government of President Klaus Iohannis. This is the second defense strategy – following the one of 2015 – that considers a paradigm shift in national defense and security reflecting the increasing complexity, interconnection and unpredictability of the dynamics of the overall security environment as well as a potential global power reconfiguration (Parlamentul Romaniei, 2020a, p. 17). Moreover, this strategy includes pandemics and puts an emphasis on the use of cyber capabilities in the context of geopolitics and warfare.

[8] Strategia de securitate cibernetică a României şi a Planul de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, 2013

[9] Strategia Națională Privind Protecția Infrastructurilor Critice, Hotărâre 718, 2011

[10] Strategia naţională de apărare a ţării pentru perioada 2020 - 2024 - Impreună, pentru o Românie sigură şi prosperăîntr-o lume marcată de noi provocări, 2020

[11] Sistemul Naţional de Securitate Cibernetică

[12] Legea privind securitatea cibernetică, 2014

The National Defense Strategy focuses on ensuring the national security and increased resilience of Romanian society and critical infrastructures against possible crises through convergence with EU and NATO prerogatives and political lines.

Moreover, the document identifies the following major trends with potential to affect and influence the security environment: rising geostrategic tensions with a reconfiguration of international and regional balances of influence, aftermath of the Covid-19 pandemic, other pandemics, migratory fluxes, increasing influence of Russia, resurgence of nationalism and extremism as well as hybrid and cyber threats.

The National Defense Strategy 2020-2024 continues to highlight cyber-related issues such as: the rapid development of ICT and increased interconnectivity, threats related to the emerging technologies, 5G –related vulnerabilities as well as "Cryptocurrencies, blockchain technology, artificial intelligence, machine learning, the Internet of Things, big data or quantum technology or the Dark Internet [and the] perspectives for their use in terms of organized crime, cybercrime, hacktivist, terrorist or extremist activities. , as well as offensive operations coordinated by entities related to the interests of some state actors. [moreover, t]he risk of adapting hybrid offensive actions to technological developments is profiled, through a continuous diversification of the modalities of action and of the coordinated resources, in order to affect the national interests, including security"[13] (Parlamentul Romaniei, 2020a, pp. 18–19).

Such references mostly stand in the context of national security objectives, the assessment of the international security environment, and the priority actions envisioned to address the main national-level threats, risks, and vulnerabilities. Across all these categories, the emphasis is put on cyber threats emanating from hostile states and non-state actors targeting critical infrastructure systems or strategic interests in the private or public sector. The strategy recognizes that cyber threats may take asymmetrical and hybrid forms especially with regard to terrorist activity, cyber criminality, and information operations.

Finally, the National Defense Strategy 2020-2024, within its lines of action, highlights the priority measures to mitigate the aforementioned cyber-related threats and risks. The strategy does not address options for how Romania might respond to a significant cyberattack.

2.1.4 National Strategy on the Digital Agenda for Romania 2020[14] (NSDAR)

The National Strategy on the Digital Agenda for Romania 2020, approved by the Romanian Government in February 2015, is aligned with the European policy document called Digital Agenda for Europe of 2010. Romania's Digital Agenda is adapted to the overall context of Romania and aims at defining Romania's strategic vision for ICT over the timeframe 2015-2020. In particular, the NSDAR aims at ensuring the development of ICT in Romania to EU standards and Romania's further integration into the EU digital single market. The document sets out four areas of action (Administratia prezidentiala al Romaniei, 2015a):

Area 1: e-Government, Interoperability, Cyber Security, Cloud Computing and Social Media: efforts to increase efficiency and reduce costs in the public sector in Romania by modernizing the administration.

Area 2: ICT in education, culture and health: support for these technologies at the sectoral level.

Area 3: ICT in e-commerce and research, development and innovation in ICT: regional comparative advantages of Romania, and backing growth in the private sector.

Area 4: Broadband and digital infrastructure services: efforts to ensure social inclusion (Administratia prezidentiala al Romaniei 2015b).

2.1.5 Romanian National Cyberdefense: Fields, Tasks and Priorities

In Romania, cyberdefense is organized through the National Defense Strategy 2020-2024[15] and the Military Strategy of Romania 2016[16] (MSR). The latter is the main document that regulates Romania's overall defense planning at the national level, ensures the strategic framework and the coordination mechanisms within Romania's administration. Considering the country's defense as a whole, the NDS promotes an extensive and holistic national security concept that puts the emphasis on streamlining international cooperation and convergence with NATO and EU principles. The incorporation of cyberdefense considerations also takes into account Romania's geopolitical situation, on the frontlines of the conflicts surrounding the Black Sea, which has inspired a growing sense of insecurity at the national and international level. These dynamics are specially shaped by the deterioration of the relations between NATO and the Russian Federation, the conflict in Ukraine, new terrorist threats and hybrid warfare.

[13] Translated from Romanian by the author.

[14] Strategia Națională privind Agenda Digitală pentru România 2020, 2015

[15] Strategia Naţională De Apărare A Ţării Pentru Perioada 2015 - 2019: O Românie puternică în Europa şi în lume

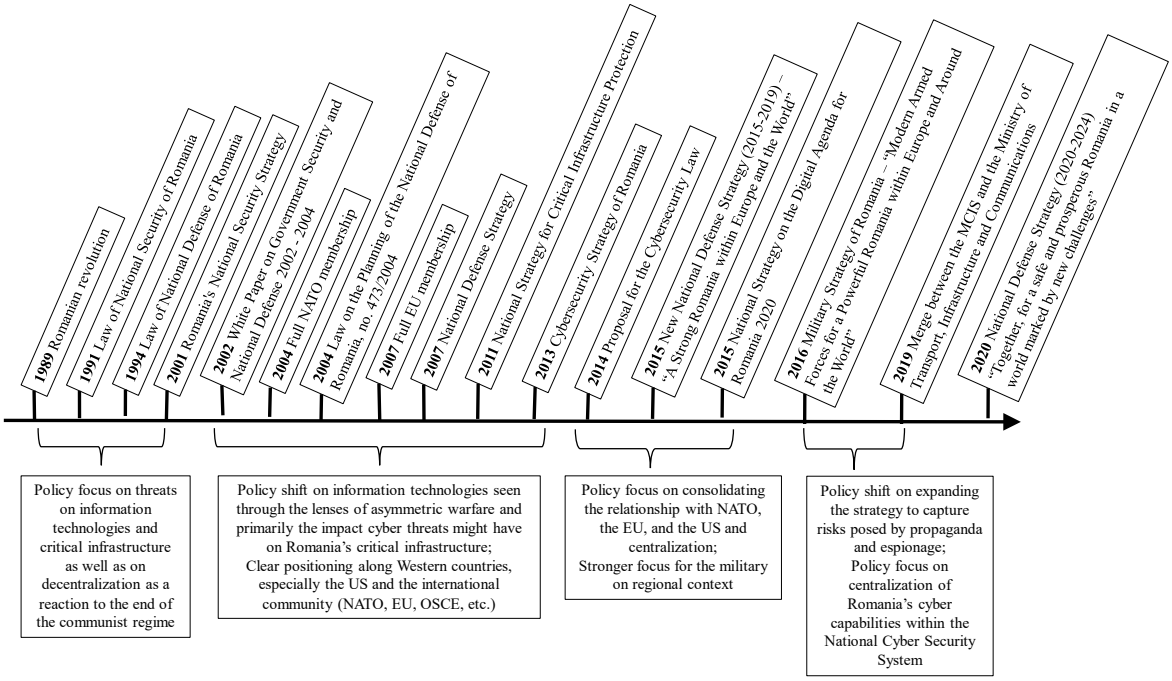
[16] Strategia Militară A României din 28 septembrie 2016: Forţe armate moderne, pentru o Românie puternică în Europa şi în lume

Cybersecurity is part of the national security objectives and measures set forth in the NDS and is usually linked to the protection of critical infrastructure, asymmetric threats or terrorism. In this document, cyberspace is seen as a means or vector to counter terrorism or asymmetric threats. Cyber threats are defined as hostile actions initiated state or non-state actors with the aim or ability to negatively affect strategically important information infrastructure systems of public institutions or companies. These cyberattacks of national significance include operations performed by cybercrime or extremist groups with the capability to materially affect Romania's national security (Parlamentul Romaniei 2015, 14-15) .

The Military Strategy of Romania 2016 gives more information about Romania's cyberdefense. Cyberattacks are defined as a "complex category of threats" characterized by "the increasing dynamic, global character, [and] difficulty in identifying the sources of attack and establishing effective countermeasures. The critical civilian infrastructure objectives, as well as defense communications systems and information technology equipment may be probable targets for such attacks" (MoND 2016, 8). According to the MSR, the Romanian Armed Forces are responsible for the cyberdefense of their own ICT infrastructure, in time of peace and war. The Romanian Armed Forces are required to develop offensive and defensive capabilities in order to fulfill their mandate. Moreover, the Romanian Armed Forces have to collaborate at both the national and international level with regard to cyberdefense. At the national level, cyberdefense is considered as part of the NCSS and is coordinated through the CIC. At the international level, the Romanian Armed Forces execute joint cyberdefense exercises and take part in various joint activities and exercises with NATO and the EU and bilaterally with other strategic partners, in particular the US.

The following diagram describes the timeline of Romanian national and international policies and the key trends that impacted Romanian cybersecurity and cyberdefense policies.

Diagram 2: Timeline of Policy Developments and Trends



Source: CSS, ETH Zürich.

2.2 Key Policy Principles

The CSR 2013, the NDS 2020, and the MSR 2013 are three complementary documents that cover both cyberdefense and cybersecurity. These strategy documents emphasize maintaining Romania's state and territorial integrity, democracy and rule of law by increasing Romania's cybersecurity and cyberdefense preparedness and resilience to cyber threats and incidents.

Moreover, these three strategic documents align in their assessment of the geopolitical situation of Romania, the risk posed by Russian threat actors, the need for a tight national cross-sectoral cooperation, and the need for strong international partnerships within the NATO and EU setting. In this context, each of the aforementioned documents considers cyber-related domains to be of national importance because of their tight links to national critical infrastructures. In all three documents, cyber capabilities are also associated with asymmetrical threats, organized crime, and terrorism. This link between cyber and terrorism and asymmetrical threat puts cyberdefense and cybersecurity in a position of great importance for Romania's national security, which is consistent with NATO and EU's defense priorities.

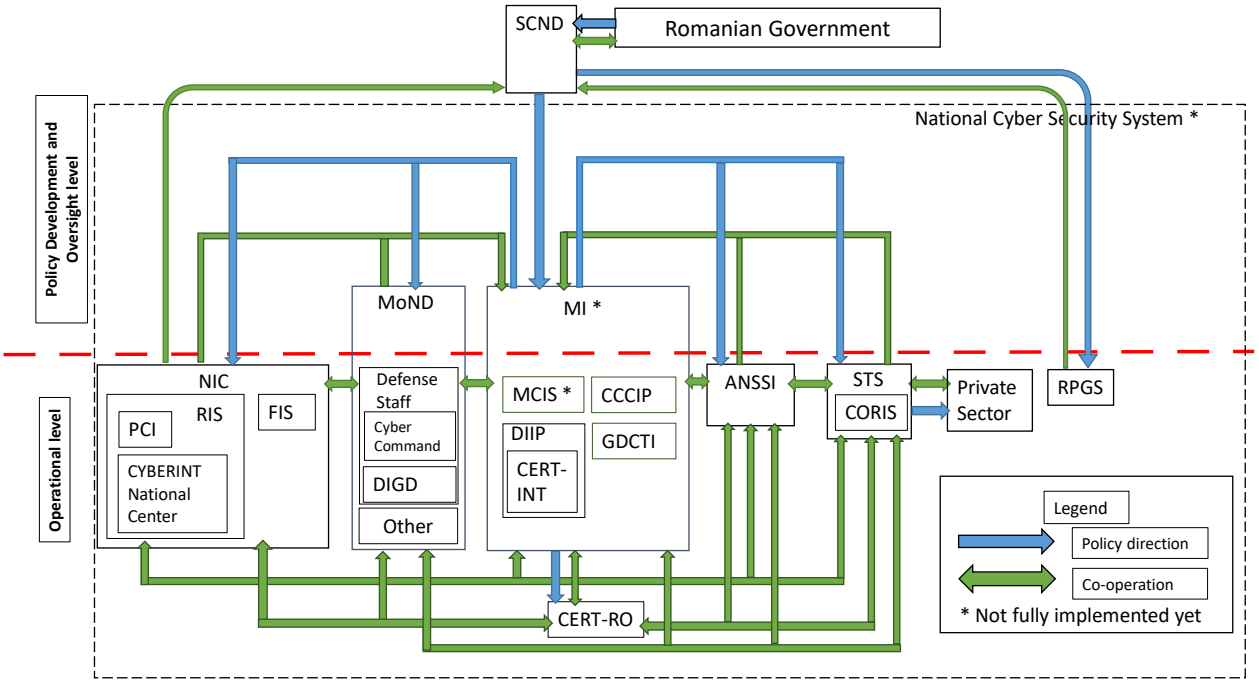
The CSR 2013 mentions the MoND and the Armed Forces only in the action plan for its implementation. This organization demonstrates the intention to formally separate cyberdefense and cybersecurity as institutional responsibilities, while promoting an open inter-institutional cooperation framework to explore and leverage synergies. To this end, these mission sets are integrated through the NCSS. At the strategic level, both are overseen by the SCND and at the operational level coordinated by the CIC.

3 Public Cybersecurity Structures and Initiatives

3.1 Overview of the National Organizational Framework

The following section describes the state of play of Romania's cyberdefense- and cybersecurity-related institutions and their cooperation. Some central institutions, like the National Cyber Security System are *de jure* already established, yet not functional. Diagram 3 shows the already implemented and functional institutions and the cooperation mechanisms between them.

Diagram 3: Oversight Organigram Structures and Cooperation Mechanisms



Source: CSS, ETH Zürich.

3.2 National Cybersecurity Structures and Initiatives: Organization, Mandates, and Operational Capabilities

As is the case with numerous national cybersecurity and cyberdefense sector policy frameworks, Romania's approach is divided into two distinct levels: policy development and oversight and the operational level, as shown in Diagram 3.

The 2013 CSR establishes the National Cybersecurity System with a list of roles and responsibilities for various authorities and institutions involved in ensuring cybersecurity, including public- and private sector cooperation and international cooperation at both strategic and operational level. The stakeholders engaged include NGOs, the intelligence community, professional associations, and academia. This complex framework shows that Romania's organizational structures charged with cybersecurity

and cyberdefense are comparatively decentralized and exhibits continuities with Romania's wider security architecture, including the prominent role of the intelligence community.

Overall, strategy development and policymaking are directed by the SCND, which receives its orders directly from the Romanian Government. The MCIS coordinates the policy and strategy implementation with the other public authorities competent in the field, namely the NIC, the MoND, the Ministry of Interior[17] (MI), the Special Telecommunication Service[18] (STS), the Ministry of Foreign Affairs[19] (MFA), and the Romanian Protection and Guard Service[20] (RPGS). At the operational level, all aforementioned ministries and services collaborate with each other.

Since 2013, a lot of work has been undertaken with regard to Romania's cybersecurity architecture. Some institutional reforms concerning the responsibilities and operation of the MCIS, the NCSS, the Cyber Security Operative Council[21] (CSOC), the Technical Support Group[22] (TSG), and the National Cyber Alert System (NCAS) are still in progress.

In accordance with the 2013 CSR, both strategic and operational responses concentrate on the following threats and actors:

- Threats: cyber-attacks against the infrastructure supporting public functions or information society services, whose disruption or damage to which could constitute a danger to national security; unauthorized access to information infrastructure; modification, deletion or deterioration of computer data or unauthorized restriction of access to such data; cyber-espionage, harassing and blackmailing individuals and businesses.
- Actors: persons or organized criminal groups that exploit vulnerabilities to obtain financial or strategic benefits; terrorists or extremists who use cyberspace to conduct and coordinate terrorist attacks, communication activities, propaganda, recruitment and training, fundraising for terrorist purposes; state or non-state actors which initiate operations in cyberspace, with the purpose of gathering intelligence in the governmental, military, and economic fields or otherwise pose a threat to national security through the use of offensive cyber capabilities (MCIS 2013).

3.2.1 Supreme Council of National Defense (SCND)

The SCND is an autonomous administrative body at the strategic level of policy development and oversight. The SCND exercises these same authorities in the area of cybersecurity and cyberdefense. It is mandated by the constitution and controlled by the parliament and is responsible for the organization and coordination of Romania's cybersecurity.

3.2.2 Ministry for Communication and Information Society (MCIS)

According to both the 2013 CSR and the 2017 law on the MCIS, the MCIS is the main institution responsible for meeting the objectives and activities set out by the CSR within the central administration.[23] With regard to cybersecurity, it has the responsibility of carrying out Romanian Government's policy in the fields of electronic communication, information technology and information society.[24] The MCIS publishes relevant governmental policy documents on cybersecurity and is responsible for both intergovernmental and international coordination in the field of cybersecurity. At the operational level, the MCIS receives administrative assistance and feedback from several subordinate and non-subordinate agencies.

In other words, the MCIS is the main state actor responsible for cybersecurity entrusted with the following tasks:

- ensuring the development of strategies in the field of electronic communications, postal services, information technology and information society, including cybersecurity;
- defining strategic objectives in the field of electronic communications, postal services, information technology and information society;
- defining, implementing, monitoring, evaluating, and coordinating policies in its field of competence, in collaboration with the

[17] Ministerul Afacerilor Interne

[18] Serviciul de Telecomunicaţii Speciale

[19] Ministerul Afacerilor Externe

[20] Serviciul de Protecţie şi Pază

[21] Consiliul Operativ de Securitate Cibernetică

[22] Grupul de suport Tehnic

[23] According to the 2013 CSR, the MCIS is undergoing a restructuring after which it will be called MSI. In practice, many official sources, including the CSR and government websites, continue to use the appellation "MCIS". For reasons of clarity and consistency, this study reflects this practice and uses the more common denomination "MCIS" in referring to the MSI.

[24] On 6 November 2019, the Romanian Government adopted an emergency order instructing a merger of the MCIS with the Ministry of Transport, Infrastructure and Communications (Petrescu 2019).

General Secretariat of the Government in accordance with the law;
- defining a normative-methodological, functional, operational and financial framework necessary for the implementation of policies, including by transposing European norms in the field of electronic communications, postal services, cybersecurity, information technology, information society, and the national interoperability framework in harmonization of national legislation with EU regulations;
- ensuring the coordination of the activities of other public authorities in order to achieve coherent policies and implementation of governmental strategies in the field of electronic communications, postal services and the information society, and for information technology in collaboration with the General Secretariat of the Government according to the law;
- ensuring communication with other organizations within the public administration, the private sector and civil society, in order to give consistency to policies and strategies;
- ensuring the administration, efficient management, and allocation of the public property of the state in its field of activity, according to the law;
- developing, financing, implementing, monitoring, evaluating, promoting, and administering government programs and projects in order to achieve the objectives defined in the strategic documents;
- stimulating regional, local, and private sector development and promoting public-private partnerships in its field of activity;
- stimulating the development of international partnerships (MCIS 2019).

3.2.3 National Information Community (NIC)

The NIC and its services report directly to the SCND. The NIC is composed of the following services: the Romanian Intelligence Service, the Foreign Intelligence Service[25] (FIS), the Department of Intelligence and Internal Protection (DIIP)[26] and the General Directorate for Defense Intelligence (DIGD).[27]

At the level of the NIC, Romania's cybersecurity is ensured by the RIS, FIS, DIIP and the DIGD. The latter is responsible for Romania's cyberdefense and will therefore be addressed in Section 3.3.2

The operative level is led by the operative council, which is made up of the representative of all four intelligence services and one representative of the government.

3.2.3.1 Romanian Intelligence Service

The RIS is Romania's main domestic intelligence service. Its role is to gather relevant information to national security through signal intelligence (SIGINT), electronic intelligence (ELINT), technical intelligence (TECHINT), cyber intelligence (CYBINT), human intelligence (HUMINT), open source intelligence (OSINT) and imagery intelligence (IMINT) in tight collaboration with the FIS. The RIS, according to the 2013 CSR, is also responsible for national cybersecurity through the CIC. The CIC, along with the CERT-RO (see section 4.2.7), is the designated overall national cyber intelligence authority.

The CIC is responsible for preventing, analyzing, identifying, and responding to cyber incidents. Moreover, the CIC elaborates and distributes public policies for preventing and counteracting incidents occurring within national cyber infrastructure.

The CIC focuses on counter-espionage, economic security, transnational threats, and the protection of classified information.

3.2.4 Ministry of Interior (MI)

The MI, with regard to cybersecurity, is subordinated to the SCND and coordinates with the other ministries and services. The following bodies assume various cybersecurity responsibilities within the MI:

3.2.4.1 Centre for Coordination of Critical Infrastructure Protection (CCCIP)[28]

The CCCIP is the specialized body of the Ministry of Interior responsible for coordinating and functioning as the point of contact in the field of critical infrastructure protection with the European Commission, EU member states, NATO, other international and national organizations, and the private sector. In this capacity, the CCCIP provides regular monitoring and risk assessments for critical infrastructure in Romania and implications of wider dependencies that exist across Europe (this includes close collaboration with the STS [see section 4.2.6] when it comes to ICT) (MAI, 2019a).

[25] Serviciul de Informații Externe

[26] Departamentul de Informații și Protecție Internă

[27] Direcţia Generală de Informaţii a Apărării

[28] Centrul de Coordonare a Protecţiei Infrastructurilor Critice

3.2.4.2 General Directorate for Communication and Information Technology (GDCIT) [29]

The GDCIT is a specialized unit responsible for the coordination and implementation of public policies within the MI and controls the way in which they are carried out. It also coordinates the elaboration and supervises the implementation of ICT-related norms, standards, methodologies, instructions, projects, and orders within the MI or for other ministries and agencies. The GDCIT produces evaluations, forecasts, feasibility studies and strategic plans on ICT matters involving the MI. It also leads on the modernization and implementation of ICT systems within the ministry and ensures, together with the Ministry of National Defense, the interoperability of interdepartmental ICT infrastructure (MAI, 2019b).

3.2.5 Department of Intelligence and Internal Protection (DIIP)

The DIIP is part of the NIC and is subordinated to the MI. This intelligence service is responsible for preventing and countering threats to the MI and, in collaboration with the other Romanian intelligence services, is tasked with collecting overall information to ensure national security. This also includes cybersecurity. The CERT-INT response center is a specialized structure established by the DIIP that aims at improving the security of Romanian IT infrastructure and preventing and counteracting IT security incidents and cyber-attacks.

According to the DIIP, CERT-INT's mandate includes the detection of vulnerabilities and intrusions in cyber infrastructure; the timely response to the occurrence of IT security incidents; providing technical support to system and network administrators and security administrators for applying best security practices; and the prevention of external attacks on national IT infrastructure.

In order to meet these objectives, CERT-INT is organized into a defensive component that identifies, analyses, investigates, and monitors cybersecurity incidents and an offensive component that prevents IT security incidents by using specific proactive measures (DGPI 2019).

3.2.6 Special Telecommunication Service

Special telecommunications are directly involved in national security and are characterized by a high level of protection and confidentiality.

To ensure this level of protection, the STS organizes, conducts, and coordinates the activities in the field of special telecommunication for Romania's public sector and for the accredited users from the private sector on the operational level. The STS responds directly to the SCND. As part of its main activities, the STS

- "designs, implements, administrates, operates, maintains and optimizes telecommunication networks, infrastructures, ICT services and systems;
- provides security services associated to special telecommunications, guaranteeing their confidentiality;
- provides Data Centers and IT systems specific services;
- provides encrypted communication services and management of cyber security incidents
- administrates the Single National Emergency Call System 112 (SNUAU);
- ensures the continuity of communications and information networks for the National Emergency Management System (SNMSU);
- is the public authority in charge with the critical infrastructure under its administration, related to ICT and National Security sectors" (STS, 2019a).
- is the designated security authority for the protection of classified information.

CORIS-STS is the Romanian CERT responsible for preventing and responding to the penetration, disruption and destruction of special telecommunication networks as well as the interception of the communications on these networks. CORIS-STS cooperates with all Romanian public and private CERT-like entities.

CORIS-STS, according to its missions and architecture, can deploy both defensive and offensive means. Its main services are proactive services, reactive services and security quality management services (STS, 2019b).

3.2.7 Romanian National Computer Security Incident Response Team (CERT-RO)

[29] Direcţia Generală pentru Comunicaţii şi Tehnologia Informaţiei

The Romanian National Computer Security Incident Response Team was established in November 2011, according to EU legislation. CERT-RO is a Romanian governmental institution that reports directly to the MCIS. CERT-RO focuses on research, development, and knowledge sharing in cybersecurity and is responsible for preventing, analyzing, identifying, and responding to cyber incidents (including through incident triage, incident coordination, incident resolution, proactive activities). Moreover, CERT-RO conducts awareness campaigns to increase overall knowledge by distributing public politics for prevention and counteracting within national infrastructures (including critical infrastructures). According to its missions and architecture, CERT-RO can deploy both defensive and offensive means even if its main services are proactive services. Finally, CERT-RO is the Romanian point of contact for international cooperation with the incident response community (CERT-RO 2019; CYBERWISER.eu 2019; UNIDIR 2018; European Commission 2016).

3.2.8 Romanian Protection and Guard Service (RPGS)[30]

The RPGS, according the 2013 CSR, together with the other competent ministries and services, is responsible for Romania's cybersecurity. The service is a state institution that reports to the SCND and on special occasions directly to the Romanian Government. The RPGS is specialized in providing, within the Romanian legal boundaries, Romanian and international dignitaries and their families with protection, including cybersecurity (SPP 2019).

3.2.9 National Association for Information Systems Security (ANSSI)[31]

Established in 2012, ANSSI is a collaborative platform connecting Romania's public and private sectors and, more broadly speaking, bringing together Romania's information security sectors.

ANSSI is a private, independent, and non-profit organization that has a network of 50 corporate members. According to ANSSI, its members represent 25 per cent of the total number of employees in the ICT sector. Through its wide network and the events it organizes, ANSSI promotes the transfer and adoption of internationally recognized best practices in Romania and sets up partnerships with similar agencies from other countries.

ANSSI's offers expertise across a number of issue areas, such as:

- Romania's national security strategy;
- legislative frameworks for cybersecurity;
- the development framework of the Information Society;
- the Strategy for the Digital Agenda of Romania;
- the Development framework of the Government Cloud;
- the national energy strategy; and
- the legal framework for public procurement.

Additionally, ANSSI has prepared operational resources, including:

- a good practice guide for public procurement; and
- application guides for EU funding schemes (ANSSI 2019).

[30] Serviciul de Protecţie şi Pază

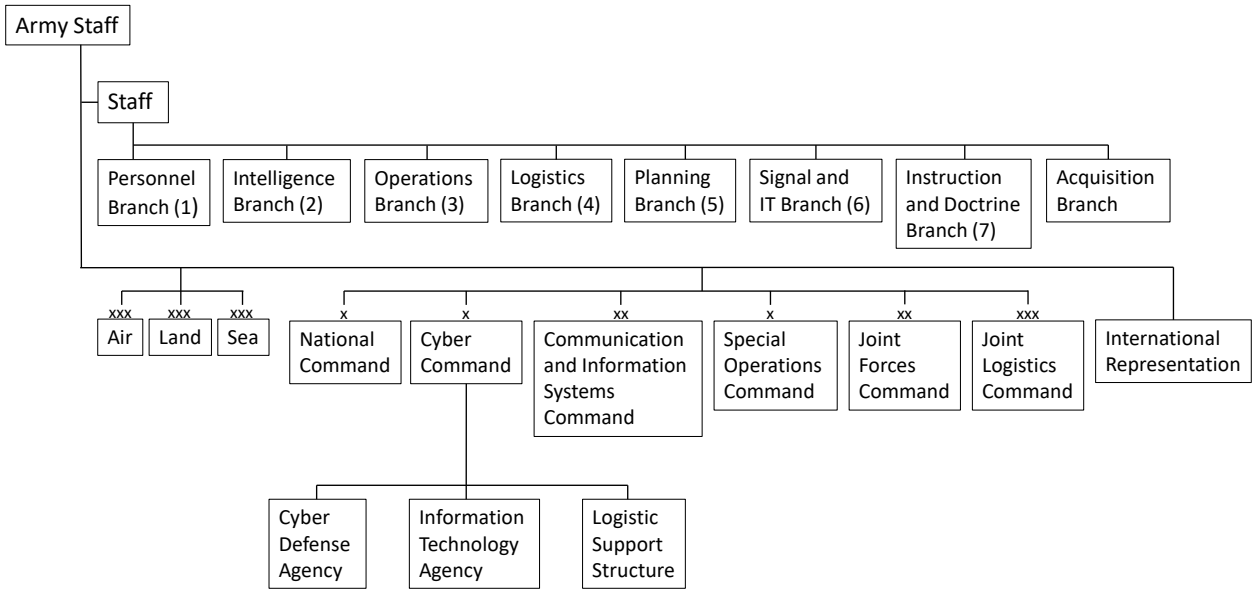
[31] Asociația Națională pentru Securitatea Sistemelor Informatice

3.3 National Cyberdefense Structures and Initiatives: Organization, Mandates, and Operational Capabilities

According to the NDS 2020-2024 and the 2017 Romanian White Paper on Defense, the MoND is responsible for the country's cyberdefense, policy development, and oversight of the military against cyber threats and reports directly to Romanian government and the SCND. The MoND, with regard to cyberdefense, coordinates with the MCIS and the SCND at a strategical level and facilitates, as foreseen in the 2013 CSR, inter-institutional cooperation at the operational and tactical level with the other dedicated agencies and departments (most importantly NIC, the MCIS, MI, ANSSI, the STS, CERT-RO).

The main bodies responsible for cyberdefense at the MoND are subordinated to the Armed Force's Staff, which operates at both the strategic and operational level. Diagram 4 below provides a graphical representation of the organization of the Defense Staff:

Diagram 4: Staff Structure of the Romanian Armed Force



Source: CSS, ETH Zürich.

3.3.1 Directorate of Communications and Information Technology,[32] Branch 6

Directly subordinated to the Defense Staff, the Directorate of Communications and Information Technology is the structure responsible for planning, organizing, and coordinating the development of communication, information technology and cyberdefense systems and services to ensure the strategic command, control, communication, computing, surveillance, and reconnaissance (C4ISR) capabilities of the Romanian Armed Forces. It also ensures the interoperability with the EU and NATO regarding Branch 6 responsibilities (MoND, 2019a).

3.3.2 Defense Intelligence General Directorate , Branch 2

Founded in July 1999, the DIGD is the military intelligence agency of the Romanian Armed Forces that operates under the auspices of the MoND and is directly subordinated to the ministry and to the SCND. The DIGD is organized into two directorates: the Directorate for Military Intelligence[33] (foreign intelligence) and Directorate for Military Security[34] (counterintelligence).

According to the 2016 Military Strategy of Romania, the DIGD carries "out specific land, sea, and air special reconnaissance, direct action, and military assistance missions, on the territory of Romania or abroad, independently or in cooperation with other national forces and/or allied forces, according to the law" (MoND 2016, 15). As it is part of NIC, the DIGD cooperates with the other information services and agencies, including on the topic of cyberdefense. The DIGD is responsible for preventing and countering threats to the Romanian Armed Forces and the national defense. Based on its mandate, the DIGD "ensures the collection, processing, verification, storage and use of information and data on internal and external, military and non-military risk factors and threats to national security in the military field, coordinates the application of counter-information measures and cooperates both with national departmental and intelligence services as well as those of the member states of the alliances, coalitions and international organizations to which Romania belongs and which ensure the security of national classified information" namely NATO and the EU (MoND, 2019b).[35] Even though not explicitly specified on the DIGD's website or in the Military Strategy, the aforementioned description of its role indicates that the DIGD, when it comes to cyberdefense, has both offensive and defensive capabilities.

3.3.3 Cybernetic Defense Command[36] and CERTMIL-MTC

Established in October 2018 as a part of the Romanian Armed Forces and directly subordinated to the Defense Staff, the Cybernetic Defense Command (Cyber Command) is a command structure that has three subordinate agencies: the Cyber Defense Agency, the Information and Technology Agency and the Logistic Support Structure.

Romania's Cyber Command is responsible for:

- the development, implementation and management of the ICT infrastructures of the Romanian Armed Forces;
- the protection and resilience of military ICT infrastructure against cyber threats;
- the early warning and reaction to malicious cyber activities directed against the Romanian Armed Forces;
- the training of specialized personnel; and
- the standardization and interoperability in the field of cyber defense (MoND, 2018, 2019c).

Cyber Command can deploy both defensive and offensive means.

CERTMIL-MTC stands for Main Technical Center for cybersecurity incidents response. According to CERTMIL-MTC' website, this entity is subordinated to the MoND and is responsible for evaluating risks, providing specialized assistance in forensics analysis, ensuring centralized management for cyber incidents and providing IT investigations and recovery services for the MoND after cyber incidents (MoND 2017). The CERTMIL-MTC is not directly mentioned in Romanian cyberdefense planning documents (specifically the 2016 Military Strategy of Romania and the 2015-2019 Defense White Paper). However, considering its official purview, it is highly probable that the CERTMIL-MTC works very closely with or is directly subordinated to the Cybernetic Defense Command.

3.3.4 Communications and Informatics Command[37]

The Communications and Informatics Command is subordinate to the Defense Staff. It manages the subordinate units responsible for planning and conducting operations in the CIS infrastructure. The

[32] Direcția comunicații și tehnologia informației

[33] Direcția Informații Militare

[34] Direcţia Siguranță Militară

[35] Translated from Romanian by the author.

[36] Comandamentul Apărării Cibernetice

[37] Comandamentul Comunicațiilor și Informaticii

Communications and Informatics Command also provides the communication services and information technology necessary for the Romanian Armed Forces at the strategic level. Moreover, this command is responsible for supporting the operational and tactical levels through communication systems and services, and information technology, to ensure cybersecurity and the integrity of the infrastructure used by the Romanian Armed Forces (MoND, 2019d).

3.4 Fundamentals of the Public Organizational Framework

Even though at the strategic level, the policy- and decision-making for cybersecurity and cyberdefense matters are centralized at the SCND, decentralization is observed at the operational level. A broad range of cybersecurity-related institutions is spread out across the public sector. Almost every ministry has its own organizational unit that is responsible for cybersecurity or cyberdefense.

However, plans for the restructuring of policy and institutional frameworks indicate a direction towards further centralization of Romania's cybersecurity and cyberdefense architecture, both at the strategic and operational level.

First, this restructuring includes the changes already foreseen under the 2013 CSR, implementation of which is still in progress. Organizations concerned include the:

- **NCSS**: Because it encompasses all the cybersecurity and cyberdefense structures of Romania, and because some of these are still developing or would be transformed, the above-mentioned NCSS is still work in progress. This integrated cybersecurity and cyberdefense system is directly subordinated to the SCND. It can be described as the "general framework of cooperation which brings together public authorities and institutions with responsibilities and capabilities in the field in order to ensure coordination of actions at national level for cyberspace security, including through cooperation with academia and business, professional associations and organizations NGOs" (UNIDIR 2018; Turcu 2016).
- **CSOC**: According to the 2013 CSR, the CSOC is the main body that coordinates the NCSS at the strategic level. Technical coordination of the CSOC should be provided by the CIC by informing on the relevant cyber incidents.
- **TSG**: within the CSOC, the TSG is responsible for the operational and tactical level of coordination of the NCSS. This organ will be made up of expert-level representatives of the national security system represented in the CSOC and reports annually to Romanian Supreme Council of National Defense (Turcu 2016; UNIDIR 2018; MAE 2019).

Second, on 6 November 2019, the Romanian Government adopted an emergency order aimed at restructuring the ministries, reducing their number to 16 in an attempt to reduce costs. Consequently, the Romanian Government decided to merge the MCIS within the Ministry of Transport, Infrastructure and Communications (Petrescu 2019). On 28 January 2020, the Romanian Government adopted Decision 90 on the Organization and Functioning of the Ministry of Transport, Infrastructure and Communications that encompasses the regulation of electronic communications in Romania (Parlamentul Romaniei, 2020b). The Romanian Government's official websites, however, offer no information on whether the merge has begun. Moreover, the official webpage of the MCIS is still active and relays information on Romania ICT-related current status.

Once carried out, this merger could have at least the two following consequences: first, it could lead to representativeness issues with regard to the wider ICT development and infrastructure digitalization efforts, and cyber field in Romania. Over the past years, this sector developed exponentially in Romania, in both the private and public sectors, making it one of the most important contributors of Romania's GDP. Within a national administrative apparatus contending with inertia, the MCIS, as an independent ministry has been comparatively resilient and fast-working. The additional administrative stratification and complexity to which this merger with a particularly big ministry could lead, would probably slow down its operations with reverberating effects for the wider sector and reduce its representativeness. Second, if not well managed, the merger between these two ministries could lead both structures to poor performance and again, hinder the ICT and cyber sector.

These changes would however not hinder the role of the CIC that will remain the first responder when it comes to cybersecurity and to a certain extent, also to cyberdefense. This leads to the following finding: the MoND and the CIC are two separate structures that have their own priorities, goals, and capabilities. The CIC focuses mostly on civilian issues, including cybercrime, and to a lesser extent on military issues. Within the MoND, on the other hand, Cyber Command defends the MoND's ICT infrastructure, systems, and networks. Both Cyber Command and the CIC have offensive capabilities. Moreover, the Romanian Intelligence Service is a

militarized institution, although it is not part of the Romanian Armed Forces and a civilian institution. This, of course, also applies to the CIC. Consequently, even if there is *de jure* a clear separation between civilian cybersecurity and military cyberdefense, this line becomes *de facto* very blurry. Here lies a risk of rivalries developing between the NIC and the MoND structures over resources and incidents responses. However, this risk is reduced because in practice, those fields lead seamlessly into one another, forming a unitary cluster of interactions and processes led by the intelligence community.

The overall presence of both offensive and defensive capabilities with regard to cyberdefense and cybersecurity shows that even though Romania's overall posture is defensive, it could have the means to adopt an offensive posture if needed.

4 Cyberdefense and Cybersecurity Partnership Structures and Initiatives

The 2013 CSR addresses the importance of "conducting joint exercises on cyberspace security", the "development of educational programs and research" and the "Development of safety culture" (MCIS 2013, 8). The CSR, however, does not precisely explain which bodies are responsible for which activity.

4.1 Public-Private Partnerships for Cyberdefense

The 2013 CSR and the 2011 National Strategy for Critical Infrastructure Protection widely promote cooperation between the public and the private sector and NGOs when it comes to cybersecurity and cyberdefense. Moreover, the 2013 CSR considers that both the public and the private sector must be protected against cyber threats, cyberespionage, and related reputational harm. Over the past ten years, Romania massively invested into the ICT private sector. The market for software and ICT services is estimated to account for some 5 billion EUR and estimations predict a growth by about 15 per cent until 2021. Moreover, Romania has the highest rate of ICT workers per capita in Europe. According to the National Strategy on Digital Agenda for Romania 2020, Romania will continue to invest in the ICT sector, especially in e-Government, interoperability, security cybernetics, cloud computing, and social media (Administratia prezidentiala al Romaniei, 2015b; Eremia, 2019). Both the CSR and the National Strategy for Critical Infrastructure Protection implicitly suggest that the public and private sectors together are responsible for the protection of critical ICT infrastructure and that public-private cooperation is necessary in order to achieve this objective.

As stated above, most of the strategic coordination of Romania's public- private partnership is directed through ANSSI. However, at the operational level, CERT-RO also contributes to this engagement between public private entities that *inter alia* is sponsored by Bitdefender, Romania's largest cybersecurity company. To this effect, CERT-RO has signed a Memorandum of Understanding (MoU) and Protocols with more than 20 private entities, ranging from antivirus companies to CERT teams from the banking sector (ITU 2013; UNIDIR 2018).

4.2 International Cyberdefense Partnerships

Chapter one above analyzed the importance that Romania attaches to international partnerships. This includes Romania's traditional multilateral cooperation with allies like the EU and NATO. Romania works with ENISA, and it is part of two of the EU's main projects on cybersecurity: the first is a cyber-threat and incident response information sharing platform; the second, concerns the buildup of cyber rapid response teams and mutual assistance in cybersecurity. Romania is also a member of PESCO and cooperates, together with the other member states, on the development of various cyberdefense projects. The latest was launched on 12 November 2019 and focuses on cyberdefense cooperation capabilities among the member states (FINABEL 2019). As a member of NATO, Romania cooperates with other member states through NATO's Cooperative Cyber Defense Centre of Excellence and has signed a MoU with NATO's Cyber Defense Management Board. Moreover, since 2014, Romania is the lead-nation in the NATO Trust Fund for developing Ukraine's cyberdefense (Cocolan, s. d.; Mihai 2019). Romania also participates in various ITU cybersecurity drills and shares best practices, expertise and guidance on capacity building with the international community through the Global Forum on Cyber Expertise. Romania is a member of the OSCE and participates in the organization's confidence building measures designed to reduce the risk for conflict related to the use of ICT.

In addition to the aforementioned partners, Romania cooperates bilaterally through its CERT-RO, the MoND, or the NIS. The CERT-RO is affiliated with international organizations like FIRST and signed several MoUs with other countries, including Slovakia, Hungary, the Republic of Moldova, Kazakhstan, Uzbekistan, China, South Korea, and Japan. Moreover, the MoND signed MoUs with Serbia and Ukraine, as stated above.

This list of countries highlights Romania's interests and the influence of geopolitics with regard to cybersecurity and cyberdefense. Indeed, its partnerships with the EU and NATO indicates that Romania is seeking to maintain and even reinforce its positioning within the Western cybersecurity hemisphere. At the same time, Romania's interest in countries like Serbia, the Republic of Moldova, Kazakhstan, Uzbekistan, and Ukraine also testify to efforts to closely follow Russian activity in Romania's neighborhood. This is not surprising considering that Romania is one of the front countries on NATO's eastern border. Both the interest to reinforce its position among Western countries and the interest in Russia as a geopolitical actor, are anchored in the 2020-2024 NDS and the 2013 CSR.

Finally, Romania's international cooperation with the public and private sector entities indicates that

there is no clear preference for military over economic alliances. Since Romania seems to need both money and geopolitical stability, it would certainly build alliance with actors that can bring both economic advantages and strategic influence to the Black Sea region.

4.3 Cyberdefense Awareness Programs

CERT-RO is the main body responsible for promoting cybersecurity awareness programs, including the following activities:

- "CERT-RO maintains an active presence in social media and is constantly publishing alerts and relevant information to the public.
- CERT-RO is also involved in ECSM [European Cyber Security Month] in an effort to bring together the existing efforts of public institutions, academia and private actors to ensure a greater impact of the awareness campaigns in correlation with the larger effort at EU level.
- CERT-RO organizes an annual cybersecurity training for journalists – as a realization of the importance mass-media has in correctly and thoroughly informing the public on cybersecurity topic" (ENISA n. d.).

Romania, in collaboration with its private sector and NGOs, has also participated in and organized several cyber-awareness-related events like the 2019 Bucharest Symposium on Global Cybersecurity Awareness or the 2019 Cyber Hygiene Day in Bucharest.

4.4 Cyberdefense Education and Training Programs

Romania's public and private sector, in cooperation with international entities like ENISA or NATO, organizes various cybersecurity and cyberdefense training formats, ranging from courses, Master programs to exercises and conferences.

Romanian universities run four different Master programs: a Master in Information Security at the Military Technical Academy in Bucharest, a Master in Information Systems Protection and Security at the University of Iasi, and two different Cybersecurity Master Programs organized by the University of Economic Studies in Bucharest.

The CIC organizes its own annual cyberdefense exercise called CyDEx comprising various simulations. CERT-RO also organizes a series of cybersecurity courses and training sessions on an annual basis.

In parallel, the private sector, along with public institutions, also invests in cyberdefense education and training. Companies like INFOSIS or Bitdefender have organized training programs and various challenges with NGO's like the Swiss Webacademy.

Finally, Romania co-organizes and takes part in cybersecurity exercises and challenges like the European Cybersecurity Challenge and NATO's Locked Shield.

4.5 Cyberdefense Research Programs

In 2013, Romania established the Cyber Security Research Centre in order to promote, support, consolidate, and coordinate research in the field of cybersecurity in Romania. The Centre is an NGO that engages in various activities, including:

- engagement "with expertise in the information security field, development of new technologies and integration of new information security systems;
- research in the information security domain;
- developing partnerships with key international structures, with the purpose of neutralizing threats within the information security field;
- investigat[ing] and expos[ing] vulnerable areas of information systems with the purpose of improving the quality of information security
- mass-media campaigns and hosting security conferences;
- initiat[ing] and develop[ing] projects for local and regional IT development" (CSSIR 2019).

On 13 March 2019, the Romanian Presidency of the Council of the European Union, in the digital field, obtained the mandate to start talks with the European Parliament on establishing the European Cybersecurity Industrial, Technology and Research Centre. The European-level Cybersecurity Industrial, Technology and Research Centre is supported by a Cybersecurity Competence Network, aimed at coordinating a cluster of National Cybersecurity Centers designated by the member states (romania2019.eu 2019).

5 Conclusion

In analyzing Romania's current cybersecurity and cyberdefense policy and institutional landscape as well as its historical background, this study has sought to highlight a number of points:

First, Romania's cybersecurity and cyberdefense policies clearly reflect the country's wider concerns about national security, emphasizing the need to position itself among Western countries, with a strong bilateral alliance with the US, full membership within the EU and NATO, and active participation in joint exercises and operations organized within the framework of NATO.

Second, Romania's policy and institutional landscape is undergoing transformation with regard to cybersecurity and defense. Since 2013, new directives and legislation have been enacted but not fully implemented. For example, the 2013 CSR, among other aspects, initiated the creation of the NCSS, the CSOC, and the TNG. These institutions exist *de jure* but *de facto* they have not yet become fully operational. This raises questions about the legitimacy of actions taken by certain institutions and the effectiveness of certain acts of law.

Third, Romania promotes an open inter-institutional cooperation framework with regard to cybersecurity and cyberdefense policy. These elements provide some measure of decentralization. However, since the NIC has a dominant role in Romania's overall cybersecurity and cyberdefense picture , actions within this framework effectively remain centrally coordinated under the NIC's control.

This dynamic leads to the fourth point. With regard to the links between the NIC and the cybersecurity and cyberdefense architecture and policies, Romania still has a very strong intelligence culture, elements of which have been inherited from the former communist apparatus.

Finally, Romania is a country that should not be underestimated with regard to cybersecurity and cyberdefense. Romanian cooperation both nationally and internationally shows that the government has chosen strong allies. Moreover, the intelligence culture and the central role of the NIC can lead to the acquisition of valuable information with regard to cyber-related topics. It remains to observe that Romania has developed both defensive and offensive capabilities throughout its cybersecurity and cyberdefense apparatus. These are important assets that can make Romania an unexpectedly strong actor.

6 Abbreviations

ANSSI	National Association for Information Systems Security (Asociația Națională pentru Securitatea Sistemelor Informatice)
CCCIP	Centre for Coordination of Critical Infrastructure Protection (Centrul de Coordonare a Protecţiei Infrastructurilor Critice)
CERT-MIL	Military Computer Emergency Response Team
CERT-RO	Romanian Computer Emergency Response Team
CI	Critical Infrastructure
CIS	Communication and Information Systems
CORIS-STS	The Operational Response Centre for Security Incidents (Centrul Operațional de Răspuns la Incidente de Securitate)
CIC	Cyberint Centre (Centrul Naţional Cyberint)
CSOC	Cyber Security Operative Council (Consiliul Operativ de Securitate Cibernetică)
CSR	Cybersecurity Strategy of Romania
CYBINT	Cyber Network Intelligence
DIGD	Defense Intelligence General Directorate (Direcţia Generală de Informaţii a Apărării)
DIGINT	Digital Network Intelligence
DIIP	Department of Intelligence and Internal Protection (Departamentul de Informații și Protecție Internă)
FIS	Foreign Intelligence Service (Serviciul de Informații Externe
GDCIT	General Directorate for Communication and Information Technology (Direcţia Generală pentru Comunicaţii şi Tehnologia Informaţiei)
ICT	Information and Communication Technologies
IMINT	Imagery Intelligence
ITU	International Telecommunication Union
MCIS	Ministry for Communication and Information Society (Ministerul Comunicațiilor și Societății Informaționale)
MFA	Ministry of Foreign Affairs (Ministrul afacerilor externe)
MI	Ministry of Interior (Ministerul Afacerilor Interne)
MoND	Ministry of National Defense (Ministerul Apărării Naționale)
MoU	Memorandum of Understanding
MSR	Military Strategy of Romania
NCAS	National Cyber Alert System
NCSS	National Cyber Security System (Sistemul Naţional de Securitate Cibernetică)
NDS	National Defense Strategy
NIC	National Information Community (Comunitatea Naţională de Informaţii)
NGO	Non-Governmental Organization
NSDAR	National Strategy on the Digital Agenda for Romania 2020
OSCE	Organization for Security and Co-operation in Europe
OSINT	Open Source Intelligence
PCI	Protection of Classified Information (Protecţia informaţiilor clasificate)
PCL	Proposal for the Cybersecurity Law
POC	Point of Contact
RIS	Romanian Intelligence Service (Serviciul Român de Informaţii)
RPGS	Romanian Protection and Guard Service (Serviciul de Protecţie şi Pază)
SCND	Supreme Council of National Defense (Consiliu Suprem de Apărare a Ţării)
SIGINT	Signals Intelligence
STS	Special Telecommunication Service (Serviciul de Telecomunicaţii Speciale)
TSG	Technical Support Group (Grupul de Suport Tehnic)
TECHINT	Technical Intelligence

7 Bibliography

Administratia prezidentiala al Romaniei, 2015a. National Strategy on the Digital Agenda for Romania 2020.

Administratia prezidentiala al Romaniei, 2015b. Strategia Națională privind Agenda Digitală pentru România 2020.

Alexe, A., 2019. Five counties in Romania generate 90 pct of IT industry revenues, study finds. Bus. Rev. URL http://business-review.eu/tech/it/five-counties-in-romania-generate-90-pct-of-it-industry-revenues-study-finds-204989 (accessed 12.18.19).

ANSSI, 2019. Asociația Națională pentru Securitatea Sistemelor Informatice [WWW Document]. URL http://anssi.ro/anssi-despre-noi/ (accessed 11.7.19).

CERT-RO, 2019. CERT.RO [WWW Document]. https://cert.ro. URL https://cert.ro/ (accessed 11.12.19).

Cocolan, M.-M., n.d. International cooperation for Critical Information Infrastructure Protection: NATO-UKRAINE Trust Fund on Cyber Defence. RASIROM 8.

CSSIR, 2019. About us – Cyber Security Research Center from Romania. URL https://ccsir.org/about-us/ (accessed 12.5.19).

CYBERWISER.eu, 2019. Romania (RO) [WWW Document]. URL https://www.cyberwiser.eu/romania-ro (accessed 10.18.19).

DGPI, 2019. Despre CERT-INT [WWW Document]. https://dgpi.ro. URL https://webcache.googleusercontent.com/search?q=cache:0VCHAsEL9V0J:https://dgpi.ro/despre-cert-int+&cd=1&hl=fr&ct=clnk&gl=ch&client=firefox-b-d (accessed 11.5.19).

ENISA, n.d. National Cyber Security Strategies (NCSSs) Map — ROU [WWW Document]. ENISA. URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map (accessed 2.21.19).

Eremia, M., 2019. Romania - Information Technology/Cybersecurity s Fields URL https://www.export.gov/article?id=Romania-Information-Technology-Cybersecurity (accessed 12.5.19).

European Commission, 2016. The Directive on security of network and information systems (NIS Directive). Digit. Single Mark. URL https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (accessed 8.17.17).

FINABEL, 2019. 13 new projects of PESCO. URL https://finabel.org/news-flash-13-new-projects-of-pesco/ (accessed 12.5.19).

ITU, 2013. Cyberwellness Profile Romania.

Jasmontaite, L., Burloiu, V.P., 2017. Lithuania and Romania to Introduce Cybersecurity Laws, in: Schünemann, W.J., Baumann, M.-O. (Eds.), Privacy, Data Protection and Cybersecurity in Europe. Springer International Publishing, Cham, pp. 131–145. https://doi.org/10.1007/978-3-319-53634-7_9

Lesser, I.O., 2007. Global trends, regional consequences wider strategic influences on the Black Sea. ICBSS, Athens.

MAE, 2019. Reglementarea domeniului securității cibernetice la nivel național [WWW Document]. mae.ro. URL https://www.mae.ro/node/28367 (accessed 12.3.19).

MAI, 2019a. Centrul de Coordonare a Protecţiei Infrastructurilor Critice [WWW Document]. Minist. Afac. Interne. URL https://www.mai.gov.ro/despre-noi/organizare/aparat-central/centrul-de-coordonare-a-protectiei-infrastructurilor-critice/ (accessed 11.5.19).

MAI, 2019b. Regulament de organizare și funcționare [WWW Document]. Minist. Afac. Interne. URL https://www.mai.gov.ro/despre-noi/organizare/regulament-de-organizare-si-functionare/ (accessed 11.5.19).

MCSI, 2019. MCSI [WWW Document]. MCSI. URL https://www.comunicatii.gov.ro/ (accessed 10.31.19).

MCSI, 2013. Cyber security strategy of Romania.

Melvin, N., 2018. Rebuilding collective security in the Black Sea region, SIPRI policy paper. sipri, Stockholm.

Mihai, I.-C., 2019. The Status of Cybersecurity in Romania.

MoND, 2019a. Direcția comunicații și tehnologia informației [WWW Document]. defense.ro. URL https://www.defense.ro/directii/dcti (accessed 12.5.19).

MoND, 2019b. Directia generala de informatii a apararii [WWW Document]. Minist. Apararii Natl. URL https://www.mapn.ro/organizare/dgia/index.php (accessed 11.29.19).

MoND, 2019c. Comandamentul Apărării Cibernetice [WWW Document]. www.defense.ro. URL https://www.defense.ro/comandamente/capc (accessed 11.26.19).

MoND, 2019d. Istoric - Comandamentul Comunicațiilor și Informaticii [WWW Document]. mapn.ro.

URL http://cci.mapn.ro/pages/view/121 (accessed 12.5.19).

MoND, 2018. The Romanian Armed Forces Response Capability to Cybernetic Security incidents. Romanian Def. 2018 60.

MoND, 2017. CERTMIL [WWW Document]. Certmil.ro. URL https://www.certmil.ro/index.php (accessed 12.3.19).

MoND, 2016. THE MILITARY STRATEGY OF ROMANIA.

Parlamentul Romaniei, 2020a. Strategia Nationala de Aparare a Tarii 2020-2024.pdf.

Parlamentul Romaniei, 2020b. HOTĂRÂRE nr. 90 din 28 ianuarie 2020 privind organizarea și funcționarea Ministerului Transporturilor, Infrastructurii și Comunicațiilor.

Parlamentul Romaniei, 2015. National Defense Strategy 2015 -2019, a Strong Romania within Europe and the World.

Petrescu, A., 2019. Comasarea MCSI și MT conduce la un randament subperformant al ambelor structuri cu un impact dezastruos. Financ. Intell. URL https://financialintelligence.ro/comasarea-mcsi-si-mt-conduce-la-un-randament-subperformant-al-ambelor-structuri-cu-un-impact-dezastruos/ (accessed 12.5.19).

romania2019.eu, 2019. Consensus on Cybersecurity Centres for Romanian Presidency of the Council of the European Union. Romanian Pres. Counc. Eur. Union. URL https://www.romania2019.eu/2019/03/13/consensus-on-cybersecurity-centres-for-romanian-presidency-of-the-council-of-the-european-union/ (accessed 12.5.19).

SPP, 2019. Serviciul de Protecție și Pază [WWW Document]. spp.ro. URL http://www.spp.ro/#/index (accessed 11.26.19).

Stratfor Worldview, 2019. Romania - Geopolitics, Analysis and News [WWW Document]. Stratfor. URL https://www.stratfor.com/region/europe/romania (accessed 12.16.19).

STS, 2019a. STS - Mission, Vision and Values [WWW Document]. www.sts.ro. URL https://www.sts.ro/en/mission-vision-and-values (accessed 11.7.19).

STS, 2019b. CORIS-STS [WWW Document]. www.sts.ro. URL https://www.sts.ro/en/coris-sts (accessed 11.8.19).

Turcu, D., 2016. Considerations on cyber security legislation and regulations in Romania 173–180.

UNIDIR, 2018. Romania | UNIDIR [WWW Document]. cyberpolicyportal.org. URL https://cyberpolicyportal.org/en/states/romania (accessed 10.24.19).

Vevera, A.-V., 2014. AMENINŢĂRI CIBERNETICE GLOBALE ŞI NAŢIONALE. Rev. Romana Inform. Si Autom. 24, 6.

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.