CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

National Cybersecurity Organisation: ROMANIA

National Cybersecurity Governance Series

Tallinn 2020

About this study

This publication is part of a series of country reports offering a comprehensive overview of national cybersecurity governance by nation. The aim is to improve awareness of cybersecurity management in the varied national settings, support nations in enhancing their own cybersecurity governance, encourage the spread of best practice and contribute to the development of interagency and international cooperation.

Primarily focusing on NATO nations that are sponsoring nations to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), each country report outlines the division of cybersecurity roles and responsibilities between agencies, describes their mandates, tasks, and competences and the coordination between them. In particular, it covers the mandates of political and strategic management; operational cybersecurity capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and management. It offers an introduction to the broader digital ecosystem of the country and outlines national cybersecurity strategy objectives in order to clarify the context for the organisational approach in a particular nation.

CCDCOE

The CCDCOE is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 29 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the *Tallinn Manual*, the most comprehensive guide on how international law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise, Locked Shields. Every spring in Tallinn the Centre hosts the International Conference on Cyber Conflict, CyCon, a unique event bringing together key experts and decision-makers of the global cyber defence community. The Centre is also responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by its member nations, currently Austria, Belgium, Bulgaria, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. NATO-accredited centres of excellence are not part of the NATO command structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

Reports in this series

National Cyber Security Organisation in Czechia

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in France

National Cyber Security Organisation in Germany

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Italy

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in Poland

National Cyber Security Organisation in Romania

National Cyber Security Organisation in Spain

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in Turkey

National Cyber Security Organisation in the United Kingdom

National Cyber Security Organisation in the United States

China and Cyber: Attitudes, Strategies, Organisation

National Cyber Security Organisation in Israel

About the authors: this publication has been prepared by experts from the Romanian Intelligence Service and the Ministry of National Defence.

Series editor: Kadri Kaska (CCDCOE)

Information in this document has been checked for accuracy as of August 2020.

Table of Contents

1. Digital society and cybersecurity assessment

Country indicators

Population:[1] 19,414,458

Internet users:[2] 89.4%

Area:[3] 238,397 km^2

GDP per capita:[4] 11,500 EUR

International rankings*

ICT Development Index (ITU 2017):[5] 6.48

E-Government Development Index (UN 2018):[6] 67

Digital Economy and Society Index (EU 2020):[7] 40

Global Cybersecurity Index (ITU 2018):[8] 0.568

National Cyber Security Index (eGA 2019):[9] 71.43

1.1 Digital infrastructure availability and take-up

Around 76% of Romanian households had access to data communications networks in 2019; however, there was a notable discrepancy between service take-up in urban (62%) and rural areas (38%)[10] due to differences in infrastructure availability and financial means of households.

To increase access to internet networks and develop the internet infrastructure in uncovered areas, in 2011 the **Ministry of Transport, Infrastructure and Communications** (MTIC) started the RoNET

[1] Population on 1 January by age and sex, Eurostat (last update 3 July 2020), https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=demo_pjan&lang=en.

[2] Of population between 16–74 years old, according to the National Institute of Statistics. Accesul populației la tehnologia informațiilor și comunicațiilor în anul 2019. România Institutul național de statistică, 2019. https://insse.ro/cms/sites/default/files/field/publicatii/accesul_populatiei_la_tehnologia_informatiei_si_comunicatiilor_romania_2019_0.pdf.

[3] România în cifre. Institutul național de statistică, 2018. https://insse.ro/cms/files/publicatii/Romania_in_cifre_breviar_statistic_2018.pdf.

[4] Gross domestic product at market prices. Eurostat (last update 19 August 2020), https://ec.europa.eu/eurostat/databrowser/view/tec00001/default/table?lang=en.

[5] ICT Development Index 2017: Romania. ITU, 2017. https://www.itu.int/net4/ITU-D/idi/2017/#idi2017economycard-tab&ROU.

[6] Annexes 2018. UN Division for Public Institutions and Digital Government, [2018]. https://drive.google.com/file/d/1FZT5zDfTa-ejvPh9c1Zu1w51DoMOefw1/view.

[7] Romania: Digital Economy and Society Index (DESI). European Commission, 2020. https://ec.europa.eu/digital-single-market/en/scoreboard/romania.

[8] Global Cybersecurity Index (GCI) 2018. ITU Publications, 2019. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

[9] Romania, National Cyber Security Index (NCSI), version 2 April 2019. eGovernance Academy, 2019. https://ncsi.ega.ee/country/ro/.

[10] Population access to information and communication technology — Romania 2019. National Institute of Statistics, 2019. insse.ro/cms/en/content/population-access-information-and-communication-technology-%E2%80%94-romania-2019.

project. This is a major project aiming to cover the areas that lack internet broadband infrastructure. The project is ongoing, with two regions (Moldova and Oltenia) completed and the other five still developing.[11]

The **Romanian Authority for Digitalisation** (ADR), under the direct coordination of the Prime Minister, is responsible for developing strategies and implementing policies in digitalisation and the information society. It coordinates the digital transformation of the Romanian society and economy, the implementation of e-government projects[12] and of **European Union** (EU) objectives and standards in the field.[13]

1.2 Digital public services

In 2019, around 15% of Romania's internet users interacted with public authorities and services for personal interest. Among them, around 75% visited public authorities' websites for information, around 56% requested official forms and around 48% submitted official forms.[14]

A 2019 study by the **National Institute of Statistics** (INS) on population access to information and communication technology revealed the profile of the Romanian citizen who uses the internet to access or provide information to public authorities as being a young or middle-aged person, employed, with skills and knowledge in accessing websites and with a high level of education and training.[15]

As efficient public services have a significant effect on the economic and social state of the country, the main objective of e-government projects is to modernise central and local institutions to provide services to citizens and businesses in an integrated, transparent and secure way. The Romanian government aims to create a modern public administration by becoming more pro-active, increasing internal efficiency, achieving greater transparency, reducing operational costs, interacting with people and developing new sources of growth.[16]

Romania continues efforts to implement the Europe 2020 Digital Agenda through several major projects including a digital public procurement system and corresponding *e-licitatie.ro* platform; the national digital tax system available via the *ghiseul.ro* website; and the "eRomânia 2" project aimed at developing a portal which will provide information on all Romanian administrative institutions. There is also an initiative for developing cloud infrastructure for Romanian public institutions.[17]

According to *National Strategy of Romania's Digital Agenda 2020*, the country must focus on three key aspects of governance in the technology field, which will allow a total transformation of the way citizens interact with public services:

---

[11] Proiectul RO-NET. Ministerul comunicațiilor și societății informaționale. comunicatii.gov.ro/proiecte-in-implementare/proiectul-ro-net; 'Ministerul Comunicațiilor și Societății Informaționale a finalizat Proiectul RoNET, Lot 5', Ministerul Comunicațiilor și Societății Informaționale, 10 octombrie 2019. https://www.comunicatii.gov.ro/ministerul-comunicatiilor-si-societatii-informationale-a-finalizat-proiectul-ronet-lot-5/.

[12] Examples of projects are provided in section 1.2.

[13] Hotărârea nr. 89/2020 privind organizarea și funcționarea Autorității pentru Digitalizarea României (*Government Decision no. 89/2020 regarding the organisation and functioning of the Romanian Authority for Digitalisation*) Guvernul României, 13 februarie 2020. https://lege5.ro/Gratuit/gm3dcmrxgi2q/hotararea-nr-89-2020-privind-organizarea-si-functionarea-autoritatii-pentru-digitalizarea-romaniei.

[14] Supra, note 2.

[15] *Ibid*.

[16] Hotărâre pentru aprobarea Strategiei naționale privind Agenda Digitală pentru România 2020 *(Government Decision no. 245/ 2015 regarding the National Strategy of Romania's Digital Agenda 2020).* Guvernul României 19.V.2015. https://www.ancom.ro/uploads/links_files/Strategia_nationala_privind_Agenda_Digitala_pentru_Romania_2020.pdf.

[17] Supra, note 16.

- Romania should provide new or improved public services with a coherent model to ensure greater effect on the social-economic sector.
- Public institutions should promote take-up of e-government. Without effective promotion of the need to use electronic public services, the effect of the project on Romania will be reduced.
- Public institutions should optimise information technology and communications (IT&C) to streamline governance. Since technology is an enabler to reduce financial and administrative costs, Romania must find ways to reduce these costs.

1.3 Digitalisation in business

Online services play an increasingly important role in Romanian citizens' everyday lives, contributing, among other things, to minimising the time spent using traditional services.

The e-commerce market is still developing, having increased potential. By both the quantity and quality of provided services, the past years have seen significant evolution. Expectations are high, considering factors like the increasing number of internet users and the growing role of mobile devices.[18]

Electronic commerce in Romania has steadily increased – in 2017, over 35% of Romanian internet users made online purchases and the percentage rose to 42-44% in 2018 and 2019,[19] but compared to other EU countries, e-commerce in Romania is underdeveloped.[20]

National authorities are concerned with regulating e-commerce operations given the potential of e-commerce to make a significant contribution to the state budget, requiring an increased taxation level for online transactions.[21] Romania intends to develop a legal framework to regulate a digital single market, acting on the following matters:[22]

- Eliminate gaps, overlapping and excessive regulation in e-commerce legislation;
- Transparency of online service operators;
- Protect Internet users;
- Suitable payment and delivery services (purchasing a product using the Internet should be a flexible process, facilitated through e-commerce);
- Reduce abuses and disputes; and
- The implementation of high-speed communication networks and advanced technological solutions.

[18] Supra, note 7.
[19] Supra, note 2.
[20] Digital Economy and Society Index (DESI) 2020 Romania. European Commission, 2020. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66928.
[21] Mentioned in Romania's DESI country profile, supra, note 7.
[22] Supra, note 17.

2. National cybersecurity strategy and legal framework

Over the last few years, the cyber threat in Romania has been one of the most dynamic threats to national security, cybersecurity becoming an important matter of national security.[23] At the national level, steps have been taken to create and adapt national policies and strategies in regard to cybersecurity, given the rapid evolution of cyber risks and threats.

The applicable National Cybersecurity Strategy of Romania was approved by **Supreme Council for National Defence** (CSAT) Decision no. 13/2013 and Government Decision no. 271/2013. The strategy sets the necessary conceptual and organisational framework for ensuring cybersecurity. It addresses cyber infrastructure protection according to new concepts and policies in the field of cyber defence elaborated and adapted to the NATO and EU.

The Romanian cybersecurity strategy has both short and long-term objectives, stating the principle that the state relies on the availability and functioning of IT&C networks that structure the lives and economy of its citizens. The goal is to develop a dynamic information environment based on interoperability and on the provision of IT services, while protecting citizens' fundamental rights and liberties and national security interests.

The main objectives included in the strategy are:[24]

- Adjusting the legal and institutional framework to the dynamics of cyber threats;
- Establishing and implementing security profiles and minimum requirements for national cyber infrastructures, relevant in terms of the proper functionality of the critical infrastructures;
- Ensuring the resilience of cyber infrastructures;
- Ensuring security by identifying, preventing and countering vulnerabilities, risks and threats to Romania's cybersecurity;
- Drawing on the opportunities provided by cyberspace;
- Developing the cooperation between public and private sectors at national and international level in the field of cybersecurity;
- Developing a security culture by raising awareness of the population concerning the vulnerabilities, risks and threats originating from cyberspace; and
- Active participation in the initiatives promoted by the international organisations of which Romania is a part to establish a set of international confidence-building measures concerning cyberspace use.

[23] A more detailed description is provided in chapter 2 of the Cyber Security Strategy of Romania. Guvernul României Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf.

[24] Ibid, Chapter 1

3. National cybersecurity governance

3.1 Strategic leadership and policy coordination

The general cooperation framework that brings together public authorities and institutions with responsibilities and capabilities to ensure coordination of actions at the national level for cyberspace security is the National Cybersecurity System (SNSC). Its mission, as stated in the *Cybersecurity Strategy of Romania*, is to provide elements of knowledge, prevention and countering of threats, vulnerabilities and risks that may affect the national cybersecurity infrastructure.[25]

The SNSC acts in the following components:

- The knowledge component – by providing information support to develop proactive and reactive actions to ensure cybersecurity;
- The prevention component – ensuring cybersecurity through creation and development of capabilities for the analysis and prognosis regarding its status;
- The cooperation and coordination component – ensuring common and effective networking mechanism in the SNSC; and
- The countering component – ensuring effective reaction to threats or cyber-attacks by identifying and blocking their manifestation.

The **CSAT** is the authority that coordinates the strategic level of SNSC activity. The CSAT approves the *Cybersecurity Strategy of Romania* and the legal framework regarding the organisation and functioning of the **Cybersecurity Operative Council** (COSC), which is responsible mechanism of implementing the Cybersecurity Strategy of Romania.

The permanent members of COSC are the Ministry of National Defence (MApN), Ministry of Internal Affairs (MAI), Ministry of Foreign Affairs (MAE), MTIC, Romanian Intelligence Service (SRI), Special Telecommunications Service (STS), Foreign Intelligence Service (SIE), Protection and Guard Service (SPP), National Registry Office for Classified Information (ORNISS) and the Secretary of the Supreme Council of National Defence. All the institutions that are part of COSC cooperate with international bodies, such as EU, NATO and Organisation for Security and Co-operation in Europe (OSCE), each in its field of competence.

The **Romanian Government** ensures coordination of other public authorities which are not represented in COSC to provide consistency to government policies and implementation strategies for electronic communications, information technology, and information society services.

3.2 Cybersecurity authority and cyber incident response

Under Law no. 362/2018, the **Romanian National Computer Security Incident Response Team** (CERT-RO)[26] is the national authority in securing national networks and IT&C systems.[27] The institution

[25] Ibid, Chapter 4.

[26] Centrul national de raspuns la incidente de securitate cibernetica – CERT-RO. https://www.cert.ro/

[27] Hotărâre nr.494 din 11.05.2011 privind înfiinţarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO (*Government Decision no. 494/2011 regarding the establishment of Romanian National Computer Security Incident Response Team*), https://cert.ro/vezi/document/hg-494-2011-infiintare-cert.

ensures the development and dissemination of public policies for preventing and counteracting incidents involving cyber infrastructure.[28]

CERT-RO was established in 2011, is hosted in the Ministry of Communications and Information Society, and has been a member of the global Forum of Incident Response and Security Teams (FIRST) since 2012. Its constituency covers the government, private and public sectors.[29]

3.3 Cyber intelligence

Intelligence in Romania is covered under Law no. 51/1991 concerning the national security of Romania, and authorises the Romanian Intelligence Service (SRI), the Romanian Foreign Intelligence Service (SIE), and the Romanian Protection and Guard Service (SPP) to carry out intelligence duties in accordance with their legal mandate. Under the same law, the MApN, the Ministry of Internal Affairs (MAI) and the Ministry of Justice (MJ) organise intelligence structures with specific attributions to their fields of activity.[30]

In 2008, **SRI** was designated as the national authority in cyber intelligence. For this purpose, a National CYBERINT Centre (CNC) was created as a unit within SRI. Its mission comprises the identification, prevention and countering of vulnerabilities, risks and threats to the IT&C infrastructure of national interest coming from cyberspace and posed by strategically, financially and ideologically motivated actors (cyber extremism and cyber terrorism).[31]

3.4 Military cyber defence

As a NATO member state, Romania has taken steps to implement the Allied Cyber Capability Targets.[32] The MApN has been assigned responsibility for the cyber defence domain. On 1st December 2018, the **Cyber Defence Command** (CApC) was established. It operates under the command and control of the Romanian Chief of Defence as a specialised authority of the MApN in the fields of cybersecurity, cyber defence and information technology.[33]

Being one of the newest commands of the Romanian military forces, **CApC** will become fully operational in 2024. Presently, it is focused on the development and implementation of dynamic organisational policies, tactics, and procedures, designing and building a modern facility to replace work places unsuited to modern cyber operations and, most of all, the challenging tasks of recruiting, training and retaining the necessary highly specialised personnel.[34]

The CApC has a mission to plan, organise, direct and conduct operations in the cyberspace to protect military networks, provide information technology services and support the joint military operations with cyber effects. To accomplish the task of defending all Romanian Armed Forces' cyberspace, CApC oversees the cybersecurity capabilities that are assigned in each of the major commands in the Romanian Armed Forces.

---

[28] Lege Nr. 362/2018 din 28 decembrie 2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice (*Law no. 362/2018 regarding the providing of a high cybersecurity level of IT&C networks and systems*), https://cert.ro/vezi/document/legea-nr-362-din-28-decembrie-2018.

[29] CERT-RO. FIRST, https://www.first.org/members/teams/cert-ro.

[30] Lege nr. 51 din 29 iulie 1991 (*republicată*) privind securitatea naţională a României* (*Law no. 51/1991 regarding the national security of Romania*), https://www.sri.ro/assets/files/legislatie/Legea51.pdf.

[31] Serviciul Roman de informații (*Romanian Intelligence Service*). sri.ro.

[32] NATO has agreed on targets for Allies' implementation of national cyber defence capabilities through the NATO Defence Planning Process. NATO Cyber Defence, Fact Sheet. North Atlantic Treaty Organization, July 2016. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf

[33] Ministerul Apărării Naţionale (*Ministry of National Defence*), https://www.mapn.ro/.

[34] Comandamentul Apărării Cibernetice (*Cyber Defence Command*), https://www.cybercommand.ro/.

The main responsibilities of CApC are related to:

- The protection and resilience of IT infrastructures which support military defence capabilities;
- Integrating the specialised cyber operations centres into a more unified Armed Forces capability with current focus on standardising incident response and knowledge management systems, and cyber attack and security information and event management capabilities;
- The integration of cyber operations and cyber intelligence in the wider military joint operations and war/operations plans;
- The management of cybersecurity incidents in military mission and weapon system IT networks;
- The evaluation of cyber operational risks;
- The assessment and mitigation of cyber risk in the design, development, acquisition, maintenance and disposal of platforms, systems and weapons;
- The development and management of military software applications and enterprise administrative and business applications;
- The development and management of a cyber resilient MILCLOUD;
- The design and implementation of IT and cyber defence services in the military mission networks interconnected in accordance with the Federated Mission Networking (FMN) environment requirements; and
- National and international cyber military cooperation.

While not yet at formal full operation capability, the CApC is providing day-to-day cyberspace defence. Its staff operates modern security appliances and products, and the Command is creating rapid response teams for its formal initial operational capability scheduled for 2021.

CApC specialists participate on a regular basis in national and international cyber defence exercises. Romania is one of the sponsoring nations of the NATO-accredited CCDCOE and since 2018 MApN has been involved in the development of the Cyber Rapid Response Teams and Mutual Assistance in Cyber Security project within the EU's programme for Permanent Structured Cooperation (PESCO). To speed deployment of Cyberspace operations excellence, CApC is entering into a long-term partnership with the United States European Command and the Alabama National Guard (State Partner for Peace) to speed cyberspace defence excellence.

3.5 International cooperation

Regarding NATO formats, projects and activities, Romania, through **SRI** and **MApN**, takes part in:

- **Multinational Malware Information Sharing Platform** (MN MISP) which is an international community platform which shares information about malware applications;
- **Multinational Cyber Defence Capability Development** (MN CD2) that aims to develop the concept of smart defence, in which every member state will be capable of ensuring a high level of cybersecurity with low costs; and
- Cyber Coalition which is the most important **NATO** cyber defence exercise. It takes place every year and aims to develop cooperation inside **NATO**.

In June 2019, Romania became a sponsoring nation to the NATO CCDCOE. Romania participates in the **CCDCOE** activities through the **SRI** and the **MApN.**[35] Romania posted a technical officer to the **CCDCOE** in 2018 and, as a member nation, participated in the **CCDCOE** cyber defence exercises (Locked Shields and Crossed Swords). Romania also benefits from access to cyber research projects, expertise in the fields of strategy and law, and participation in conferences.

[35] Supra, note 31.

In cooperation with OSCE, Romania is represented by the MAE in working groups and meetings. In this context, SRI, through the CNC, contributes to the implementation of measures by supporting MAE, alongside with other national institutions.

In 2019, MAE and CNC cooperated to develop and implement a table-top cybersecurity exercise called "Scenario-Based Interactive Discussion (S-BID)", related to Confidence Building Measures 15 (CBM15) - security of ICS-SCADA systems.

3.6 Engagement with the private sector and academia

In developing cooperation between the public and private sectors, Romania considers ensuring cybersecurity as a priority for action in international bodies and alliances to which Romania belongs, because cyberspace brings together cyber infrastructure owned and operated by state and private entities. Romania defines its main objectives of cooperation between the public and private sectors as:[36]

- Exchanging information on threats, vulnerabilities and risks;
- Developing capabilities for early warning and response to cyber incidents and attacks;
- Conducting joint exercises on cybersecurity;
- Developing educational programs and research;
- Developing cybersecurity culture; and
- Providing a joint response in the event of major cyber-attacks.

In 2019, the CNC, in partnership with the public, private and academic sectors, supported a project to develop and consolidate cybersecurity education. The project was established in 20 universities across the country by introducing cybersecurity study programmes. With the same purpose, CNC initiated a pilot project with an informatics profile to introduce cybersecurity classes into Romanian high schools.

CNC contributed to the consolidation of the Romanian business and commercial sectors in the cybersecurity field, encouraging Romanian start-ups to support IT&C and cybersecurity domains and thereby bringing benefits to national security in the long term.

[36] Supra, note 23, Chapter 5.

References

Policy

Guvernul României Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică (*Cybersecurity Strategy of Romania*), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf.

Hotărâre pentru aprobarea Strategiei naționale privind Agenda Digitală pentru România 2020 *(Government Decision no. 245/2015 regarding the National Strategy of Romania's Digital Agenda 2020).* Guvernul României 19.V.2015. https://www.ancom.ro/uploads/links_files/Strategia_nationala_privind_Agenda_Digitala_pentru_Romania_2020.pdf.

Law

Lege nr. 51 din 29 iulie 1991 (*republicată*) privind securitatea naţională a României* (*Law no. 51/1991 regarding the national security of Romania*), https://www.sri.ro/assets/files/legislatie/Legea51.pdf.

Hotărâre nr.494 din 11.05.2011 privind înfiinţarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO (*Government Decision no. 494/2011 regarding the establishment of Romanian National Computer Security Incident Response Team*), https://cert.ro/vezi/document/hg-494-2011-infiintare-cert.

Lege Nr. 362/2018 din 28 decembrie 2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice (*Law no. 362/2018 regarding the providing of a high cybersecurity level of IT&C networks and systems*), https://cert.ro/vezi/document/legea-nr-362-din-28-decembrie-2018.

Hotărârea nr. 89/2020 privind organizarea și funcționarea Autorității pentru Digitalizarea României (*Government Decision no. 89/2020 regarding the organisation and functioning of the Romanian Authority for Digitalisation*) Guvernul României, 13 februarie 2020. https://lege5.ro/Gratuit/gm3dcmrxgi2q/hotararea-nr-89-2020-privind-organizarea-si-functionarea-autoritatii-pentru-digitalizarea-romaniei.

Other

Accesul populației la tehnologia informațiilor și comunicațiilor în anul 2019. România Institutul național de statistică, 2019. (*National Institute of Statistics, Population access to information and communication technology - Romania 2019*) https://insse.ro/cms/sites/default/files/field/publicatii/accesul_populatiei_la_tehnologia_informatiei_si_comunicatiilor_romania_2019_0.pdf.

Annexes 2018. UN Division for Public Institutions and Digital Government, [2018]. https://drive.google.com/file/d/1FZT5zDfTa-ejvPh9c1Zu1w51DoMOefw1/view.

Centrul national de raspuns la incidente de securitate cibernetica – CERT-RO. (*Romanian National Computer Security Incident Response Team*), www.cert.ro.

CERT-RO. FIRST, https://www.first.org/members/teams/cert-ro.

Comandamentul Apărării Cibernetice (*Cyber Defence Command*), www.cybercommand.ro.

Digital Economy and Society Index (DESI) 2020 Romania. European Commission, 2020. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66928

Global Cybersecurity Index (GCI) 2018. ITU Publications, 2019. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

Gross domestic product at market prices. Eurostat (last update 19 August 2020), https://ec.europa.eu/eurostat/databrowser/view/tec00001/default/table?lang=en.

ICT Development Index 2017: Romania. ITU, 2017. https://www.itu.int/net4/ITU-D/idi/2017/#idi2017economycard-tab&ROU.

Ministerul Apărării Naţionale (Ministry of National Defence), www.mapn.ro.

'Ministerul Comunicațiilor și Societății Informaționale a finalizat Proiectul RoNET, Lot 5', Ministerul Comunicațiilor și Societății Informaționale, 10 octombrie 2019. https://www.comunicatii.gov.ro/ministerul-comunicatiilor-si-societatii-informationale-a-finalizat-proiectul-ronet-lot-5.

România în cifre. Institutul național de statistică, 2018. https://insse.ro/cms/files/publicatii/Romania_in_cifre_breviar_statistic_2018.pdf

NATO Cyber Defence, Fact Sheet. North Atlantic Treaty Organization, July 2016. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf

Population access to information and communication technology — Romania 2019. National Institute of Statistics, 2019. insse.ro/cms/en/content/population-access-information-and-communication-technology-%E2%80%94-romania-2019.

Population on 1 January by age and sex, Eurostat (last update 3 July 2020), https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=demo_pjan&lang=en.

Proiectul RO-NET. Ministerul comunicațiilor și societății informaționale. comunicatii.gov.ro/proiecte-in-implementare/proiectul-ro-net

Romania, National Cyber Security Index (NCSI), version 2 April 2019. eGovernace Academy, 2019. https://ncsi.ega.ee/country/ro/.

Romania: Digital Economy and Society Index (DESI). European Commission, 2020. https://ec.europa.eu/digital-single-market/en/scoreboard/romania.

Serviciul Roman de informații (*Romanian Intelligence Service*), www.sri.ro.

Acronyms

ADR	Romanian Authority for Digitalisation
CApC	Cyber Defence Command
CBM15	Confidence Building Measures 15
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CERT-RO	Romanian National Computer Security Incident Response Team
CNC	National CYBERINT Centre
COSC	Cybersecurity Operative Council
CSAT	Supreme Council for National Defence
EU	European Union
INS	National Institute of Statistics
MAE	Ministry of Foreign Affairs
MAI	Ministry of Internal Affairs
MApN	Ministry of National Defence
MN CD2	Multinational Cyber Defence Capability Development
MN MISP	Multinational Malware Information Sharing Platform
MTIC	Ministry of Transports, Infrastructure and Communications
NATO	North Atlantic Treaty Organization
NCSC	National Cybersecurity Centre
OSCE	Organization for Security and Co-operation in Europe
PESCO	Permanent Structured Cooperation
S-BID	Scenario-Based Interactive Discussion
SIE	Romanian Foreign Intelligence Service
SNSC	National Cybersecurity System
SPP	Romanian Protection and Guard Service
SRI	Romanian Intelligence Service