The implications of cybercrime for national security

Ioan Dumitru Apachiței[1*], *Codrin Sîrcu* Ichim[2]

[1]Faculty of Law, Alexandru Ioan Cuza University of Iași, Romania
[2]Faculty of Law, Alexandru Ioan Cuza University of Iași, Romania

Abstract. This study aims to identify the general aspects concerning the elements of correspondence between the notion of cybercrime and the field of national security by analysing the regulatory and institutional framework. Electronic information concerning national security requires concrete measures for its identification and control, as its alteration, theft, or modification may constitute a source of vulnerability for the security of the State and its citizens. In this respect, the architecture of the regulatory framework we are considering concerns national security provisions and the protection of classified information.

1 Introductory consideration

The significant implications of information systems concerning social relations have led to the emergence of legal mechanisms to prevent and punish criminal phenomena that take advantage of the vulnerabilities of information systems. A first step in this direction was the adoption in 2001 of the Convention on Cybercrime, Ratified by Law no. 64/2004, published in O.J. no. 343 of 20 April 2004. The preamble to the Convention states that the term "computer-related crime" refers to those actions "*against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct*".

As the applicability of computer data has expanded, it has also become applicable in the field of national security, creating a source of vulnerability. Thus, digitising information relevant to national security requires appropriate measures to prevent and remove the consequences of cybercrime.

The *National Strategy for National Defence for 2020-2024,* approved by Parliament Decision no. 22/2020, published in O.J. no. 574 of 1 July 2020, indicates the threats that may directly or indirectly target national security, including cyber-attacks and cybercrime. Regarding cyber-attacks, reference is made to the risk of damage to "*critical information and communication infrastructures*". The Strategy's drafters also understand cybercrime to refer to the actions of criminal groups, which can consist of unauthorised access to or infection of information systems, unauthorised interception of computer data, or illicit transactions with virtual currencies [1].

* Corresponding author: ioan.apachitei@uaic.ro

Similarly, the new *Cyber Security Strategy for 2022-2027,* approved by Government Decision no. 1321/2021, published in O.J. no. 2 of 3 January 2022, identifies cyber threats from state actors as one of the essential sources of threats to national cyber security, which also affects national security. Such threats target information systems operating in the diplomatic, economic, military, and social sectors, all of which are critical to national security. Similarly, the *Strategy* unequivocally states that cyber security is "an integral part of wider national security".

The management of computer data requires the existence of a computer system, *i.e.*, a computer program that processes the data. These concepts are defined in Article 35 of Law no. 161/2003, which regulates the legal mechanisms through which computer crime is prevented and combated: "*a) computer system means any device or set of devices which are interconnected or in a functional relationship, one or more of which provides for the automatic processing of data by means of a computer program; b) automatic data processing means the process by which data in a computer system are processed by means of a computer program; c) computer program means a set of instructions which can be executed by a computer system in order to obtain a given result; d) computer data means any representation of facts, information or concepts in a form which can be processed by a computer system. This category also includes any computer program that can cause a computer system to perform a function."* (Translated from the original version in Romanian: "*a) prin sistem informatic se înțelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic; b) prin prelucrare automată a datelor se înțelege procesul prin care datele dintr-un sistem informatic sunt prelucrate prin intermediul unui program informatic; c) prin program informatic se înțelege un ansamblu de instrucțiuni care pot fi executate de un sistem informatic în vederea obținerii unui rezultat determinat; d) prin date informatice se înțelege orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic. În această categorie se include și orice program informatic care poate determina realizarea unei funcții de către un sistem informatic*").

At the same time, the law mentioned above also enshrines several provisions on the institutional framework with powers in the field of national security, thus Articles 39 and 40 stipulate that the Ministry of Justice, the Ministry of Internal Affairs, and the intelligence services must set up and update databases on cybercrime, as well as to carry out "*special training programmes for personnel responsible for preventing and combating cybercrime*".

2 Protection of state secret information

2.1 General framework for the protection of state secret information

The reference regulatory framework, applicable to the protection of classified information at the level of national legislation, is represented by Law no. 182/2002, Published in O.J. no. 248 of 12 April 2002. The first article of this law states that the protection of classified information is carried out by the *national information protection system*. The link between this category of information and the sphere of relations within the field of national security can be seen from the content of Article 4 of the same law; thus, classified information is protected against acts of espionage, compromise, and unauthorised access, alteration, or modification. The integrity of the systems responsible for storing and transmitting classified information is also ensured.

The notion of protection of classified information is within the legal, physical protection of persons who, by law, may have access to such information and of the sources generating classified information.

In Article 15 (b) and (d) of Law no. 182/2002, the Romanian legislator defines the terms "classified information" and "state secret information". The first term refers to "*information, data, documents of interest for national security, which, due to their levels of importance and the consequences that would occur as a result of unauthorised disclosure or dissemination, must be protected*", while the second refers to "*information concerning national security, the disclosure of which may prejudice national security and the defence of the country*". The distinction between the two terms is from general to special, in the same sense para. (1) of Article 178 of the Criminal Code indicates that "*state secret information is information classified as such*".

According to Article 236 of the *National Standards for the Protection of Classified Information,* approved by Government Decision no. 585/2002, published in O.J. 485 of 5 July 2002, the measures for protecting classified information in physical format are similar to information in electronic form. Annex 10/C of the document mentioned above indicates the primary sources of danger that may affect computer systems storing, processing, or transmitting classified information. Regarding the subject under consideration, threats of unauthorised alteration or destruction of data, programmes, or equipment, unauthorised access, interception of transmissions, and unauthorised copying of data are relevant. In this respect, the provisions of Article 288 of the *National Standards* stipulate that the media on which information is stored shall be kept in such a way as to correspond to the highest level of classification of the information, with protection always ensured.

All public authorities and institutions dealing with state secret information must take the necessary measures to protect it. In this respect, the provisions of Articles 24 and 25 of Law no. 51/1991, republished in O.J. 190 of 18 March 2014 establish that these bodies are obliged both to draw up their programmes to prevent the leakage of information, which is a state secret, and to request the support of the bodies responsible for national security.

2.2 General considerations regarding the correlation between cybercrime and national security from the perspective of existing incriminations in the Romanian Criminal Code

Law no. 161/2003 regulated in Chapter III of the Third Title a series of incriminations regarding cybercrime that was subsequently adopted with amendments in Chapter VI of Title VII of the Special Part of the current Romanian Criminal Code.

Cybercrime may affect national security, for example, when the purpose of the crime is to procure or transmit or disclose state secret information. In other words, cybercrime is the means of committing a national security offence. At the same time, if we consider the broad meaning of the concept of national security, we can also consider that the commission of some of the offences against the integrity of information systems and data can lead to the impairment of national security, for example, the severe disruption of the functioning of an information system (Article 363 of the Criminal Code) used within the critical national infrastructure. According to art. 3 letter a) of the Government Emergency Ordinance no. 98/2010 with subsequent amendments and additions (published in O.J. 757 of 12 November 2010), the notion of critical national infrastructure (CNI) is defined as "an element, system or component thereof, located on national territory, which is essential for the maintenance of vital functions of society, health, safety, security, the social or economic well-being of persons and whose disruption or destruction would have a significant impact at the national level as a result of the inability to maintain those functions, as well as the project of a strategic

objective of national interest whose construction is imperative to safeguard the national interest".

The correlation between the security of information systems and acts that may harm national security can be seen through the role of classified information. For example, Article 4 of Law 182/2002 states that the protection of classified information aims to prevent espionage and the security of information systems and their transmission. The same perspective is also apparent from the content of the Explanatory Memorandum to Law no. 182/2002, in which the legislator expressly indicated that one of the objectives of the draft law was to "*protect classified information against espionage, compromise or unauthorized access*". It remains to be established whether the commission of both the crimes as means and crimes as purpose will be held to be concurrent or whether they will be absorbed. For example, the offence of unlawfully intercepting a transmission of computer data (Article 361 of the Criminal Code), by means of which confidential information is communicated, will be absorbed into the crime of treason by transmitting information (Article 395 of the Criminal Code) or espionage (Article 400 of the Criminal Code) in the form of procuring "*documents or data constituting state secret information*", provided that the other conditions of the criminal law are met. The perpetrator's action could represent a similar hypothesis in seriously disrupting the functioning of computer systems (Article 363 of the Criminal Code), an act which, in time of war, is "*likely to favour the activity of the enemy or weaken the fighting power of the Romanian or allied armed forces*" (Article 396(d) of the Criminal Code).

3 Bodies with duties in fighting cybercrime that concerns national security

At the national level, other bodies have responsibilities in the cyber security and cybercrime field, but they are separate from the institutional framework for national security. One such example is the National Cyber Security Directorate (established by Government Emergency Ordinance no. 104/2021, published in the O.J. 918 of 24 September 2021), a body under the Government and coordinated by the Prime Minister. According to Article 5 point c) point 9 and Article 20 para. (1) of Government Emergency Ordinance no. 104/2021, the provisions of the Ordinance do not apply in the area reserved for national security, but the Directorate may cooperate with "institutions of the national defence, public order, and national security system".

3.1 Supreme Council of National Defence

The regulatory framework governing the organisation and functioning of the SCND (C.S.A.T. in Romanian) is represented by Law no. 415/2002, published in O.J. 494 of 10 July 2002. According to Article 119 of the Fundamental Law, the central role in coordinating and organising activities in the field of national security lies with the SCND [2], defined as an autonomous administrative authority whose activity is verified by employing parliamentary control.

Regarding the protection of national security data, we refer to the provisions of Article 14 of Law no. 182/2002, which stipulates that the SCND is also responsible for coordinating programmes for the protection of classified information throughout the country; however, this responsibility is expressly stated in Article 4 of Law no. 415/2002, which lists the primary responsibilities of the Council. However, the leading role in the general coordination and control of measures for protecting state secret information falls to the Romanian Intelligence Service (RIS), according to Art. 25 para. (1) of Law 182/2002. Para. (2) of the

same Article also requires the intelligence services, the Ministry of Internal Affairs, the Ministry of Justice, and the Ministry of National Defence to establish concrete measures for coordinating and controlling activities to protect classified information. The fact that governing bodies of these institutions are members of the SCND, according to para. (3) of Article 5 of Law no. 415/2002 explains how the Council coordinates measures for the protection of classified information.

An analysis of the SCND 's reports reveals several measures that directly concern the Council's role in combating cybercrime. For example, the SCND report on the activities carried out in 2009 [3] mentions the approval of the organisation of the Anti-Fraud Task Force, which had both operational powers and the power to promote legislative projects targeting the threats posed by cybercrime. The report also refers to the role of RIS in the fight against cybercrime, mainly through the National CYBERINT Centre set up in 2008 [4].

3.2 Intelligence Services

Intelligence services are state bodies that carry out intelligence activities to protect national security and are under parliamentary control [5]. Per the provisions of para. (1) of art. 8 of Law no. 51/1991, the Romanian Intelligence Service is responsible for obtaining internal information, while the Foreign Intelligence Service (S.I.E.) is responsible for obtaining data concerning national security from abroad. At the same time, the Protection and Guard Service (S.P.P.) ensures the protection of Romanian dignitaries and foreigners on the country's territory, namely the guarding of their work premises and residences.

The legal framework regulating the activity of the RIS is represented by Law no. 14/1992, published in O.J. 33 of 3 March 1992, the first article of which defines the RIS as being specialised in the field of national security information, and the activity of the service is organised and coordinated by the SCND and under parliamentary control. According to Article 2 of Law no. 14/1992, RIS "*organises and executes activities for the collection, verification and exploitation of information necessary to know, prevent and counteract any actions which, according to the law, constitute threats to the national security of Romania*".

Regarding the protection of classified information, the role of RIS is to protect state secrecy and prevent the leakage of such information. In this respect, the provisions of para. (1) of Article 3 of Law no. 14/1992, corroborated with art. 34 of Law no. 182/2002 provides for the following tasks of the RIS. with regard to the protection of classified information: "*shall draw up, in cooperation with the public authorities, national standards for classified information and the objectives for their implementation; shall supervise the actions taken by the public authorities for the application of the provisions of this law; shall give expert opinion on the programmes for the prevention of leaks of classified information, drawn up by public authorities and institutions, autonomous regions and companies holding such information; verify how the legal rules on the protection of classified information are respected and applied by public authorities and institutions; carry out on-the-spot checks and reviews of programmes for the protection of classified information; cooperate with the Office of the National Register of State Secret Information and the National Security Authority in all matters relating to the application of this Law; assists in the determination of targets and locations of particular importance for the protection of classified information, at the request of the heads of public authorities and institutions, economic agents and private legal entities, and submits for the Government's approval a centralised record of them; organises and is responsible, in accordance with legal provisions, for the collection, transport and distribution in the country of State secret correspondence and official correspondence of a secret nature; analyses and determines the measures to be taken in relation to complaints or suggestions concerning the way in which the programmes for the protection of classified information are applied; detects non-compliance with the rules on*

the protection of classified information and applies the contravention penalties provided for by law, and, when the facts constitute offences, refers the matter to the criminal prosecution authorities".

The *National Centre Cyberint (Centru Național Cyberint)* operates within the RIS. Its role is to use information capabilities to protect technical systems concerning defence to provide relevant information to prevent, limit, and stop the effects of aggression against information systems.

Regarding the powers of the S.I.E. in the field of protection of state secret information, the existing regulations are brief; Law no. 1/1998 itself, which provides for the organisation and functioning of this public authority, deliberately omits to set out the general framework of the powers of the Service [6]. In this regard, we note that the provisions of Article 26 of Law no. 182/2002 establish that the S.I.E. is obliged to coordinate the activities and control the measures concerning the protection of state secret information with which Romania's representatives abroad operate.

All persons authorised to handle or come into possession of state-secret information are obliged to ensure its protection. At the same time, the protection of classified information, according to Article 9 (d) of Law no. 182/2002, also implies the protection of the persons who have access to this information. In this regard, by the decision of the SCND, the persons and objectives whose protection and guarding are ensured by the Guard and Protection Service are established. The S.P.P. is also obliged to organise its own activities to protect state secrecy to prevent any leakage of data or information that is not intended for the public. To achieve this aim, the S.P.P. is part of the national defence system and has a military structure, according to para. (2) of Article 1 of Law no. 191/1998, published in O.J. 402 of 22 October 1998.

3.3 Public Ministry – Public Prosecutors Office

The role of the Public Ministry is to protect the general interests, *i.e.,* the fundamental rights and freedoms of citizens. The *Directorate for the Investigation of Organised Crime and Terrorism,* established by the provisions of Government Emergency Ordinance no. 78/2916, published in O.J. 938 of 22 November 2016 (abbreviated to DIICOT) is also part of the Public Ministry – Prosecutor's Office next to the High Court of Cassation and Justice structure.

Per Article 2 para. (1) point f) and art. 11 para. (1) point 2 of the Government Emergency Ordinance no. 78/2016, DIICOT is responsible for prosecuting cases involving the commission of cybercrime offences and those directed against national security. In this regard, the institution's organisational chart provides for the functioning the *Section for Combating Terrorist and Cybercrime Offences*, which includes the *Service for Combating Terrorist and National Security Offences* and the *Service for Combating Cybercrime* [7].

The reports on the activities of DIICOT for 2020 [8] and 2021 [9] provide relevant information on the national development of cybercrime [7].

Thus, during 2020, 1675 new cases were registered, more compared to 1484 the previous year. Thus, the total number of cases to be solved in 2020 was 4874. A total of 267 cases were settled following an indictment or the conclusion of a guilty plea agreement, resulting in a charge of 387 defendants out of the 1335 cases settled.

In 2021, the number of new cases registered increased (by 6.03%) compared to the previous year, reaching 1776 out of a total of 5052 cases in progress. Also, the number of cases solved following the issuance of indictment or the conclusion of the plea agreement was up (by 1.12%) compared to the previous year, consisting of 270 cases and 402 defendants, out of 1623 cases solved. It is also indicated in the report for 2021 that most of the offences concern the e-commerce regime, child pornography, computer fraud and fraudulent financial transactions.

4 Conclusion

The digitisation of information contributes to the speed of information transmission and processing. It is a source of strategic and financial interest, which is why cybercrime is rising.

As classified information and critical national infrastructure exploit the means of storing and transmitting information, there is a means-to-an-end link between the acts that compromise information systems and the actions that may compromise national security. This link is usually achieved by absorbing the offence of means into the constitutive content of the violation of national security.

As for the institutional framework, we have shown that the national security authorities also have powers to combat cybercrime. In this respect, the acts that fall within the concept of cybercrime can potentially constitute a source of threat to national security.

References

1. Presidential Administration, National Strategy for National Defence for the period 2020-2024, Bucharest, URL: https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_ Tarii_ 2020_2024.pdf, accessed: 15.10.2022 (2020)
2. T. Toader, M. Safta, Constituția României, [The Romanian Constitution], (Hamangiu, Bucharest, 2019)
3. Supreme Defence Council, Activity Report, 2009, URL: https://csat.presidency.ro/files/documente/Raport_CSAT_2009_5727ro.pdf, accessed: 15.10.2022 (2009)
4. D. Panc, Securitatea cibernetică la nivel național și international, [National and international cyber security], (Hamangiu, Bucharest, 2017)
5. D.C. Mâță, Dreptul, **9,** 76-79, (2015)
6. D.C. Mâță, Securitatea națională. Concept. Reglementare. Mijloace de ocrotire, [National security. Concept. Regulation. Means of protection], (Hamangiu, Bucharest, 2016)
7. Directorate for the Investigation of Organised Crime and Terrorism: Structure, URL: https://www.diicot.ro/prezentare/organigrama, accessed: 15.10.2022 (2022)
8. Directorate for the Investigation of Organised Crime and Terrorism, Activity Report 2020, URL: https://www.diicot.ro/images/documents/rapoarte_activitate/ raport2020.pdf, accessed: 15.10.2022 (2020)
9. Directorate for the Investigation of Organised Crime and Terrorism, Activity Report 2021, URL: https://www.diicot.ro/images/documents/rapoarte_activitate/ raport2021.pdf, l accessed: 15.10.2022 (2022)