Cybersecurity – Dimensions of national security

Lecturer. Dan Constantin MÂȚÂ, PhD.
Alexandru Ioan Cuza University of Iasi, Faculty of Law
danmata@uaic.ro

Abstract
In the present view on the concept of security there are a number of constituents that act interdependently. These build-up a pluridimensional morphology of security that features: the political dimension, the military dimension, the economic dimension, the social dimension, the ecological dimension. Alongside these traditional dimensions of the concept of national security a number of authors also theorized the informational dimension. In the light of the gravity of risks and threats, cybersecurity is deemed to be an important component of national security. This is why at European level there is an intense process of attunement and adaptation of the legislation regarding states' cybersecurity for the purpose of ensuring a safe, free and democratic cyberspace.
Keywords: *national security, cybersecurity, legislative framework, strategy*

1. Introduction

The phrase „national security" is unanimously used in all specialist works being deemed the expression most representative for the concept of defending a state's fundamental national interests against any aggressions, dangers, threats or risks [1]. Specialists in international relations theory, political sciences, public politics or law proposed numerous definitions and analysis schemes.

Some authors define national security as a concept that „concentrates on the preservation of state sovereignty and its protection against any external or internal, conventional or unconventional threats" [2]. In a slightly different perspective, it is insisted upon the fact that national security is "a state of affairs, the one where a nation is protected against the dangers that threaten the unity of the state where it develops, its territorial integrity, independence and sovereignty, its constitutional order and own system of values" .[3]

We note that these definitions are constructed around the notion of threat to common or individual values. There is, however, a modality of analysis that potentiates precisely these values in the definitional effort. Thus national security is regarded as being "the essential category that refers to the state of the nation, of social communities, of the citizens and of the state, based on economic prosperity, legality, socio-political balance and stability, expressed in the rule of law and guaranteed through economic,

political, social, legal, military, informational and other actions, for the unrestricted exercise of rights and freedoms, full manifestation of state's freedom to decide and action, of its fundamental attributes and of its status as an international law subject" [4].

Other authors hesitate to assume the pattern of a standard definition and consider that the most effective manner to define security is represented by this concept dimensions' social relevance [5]. In this context, the issue was raised on the error in assuming there is a similitude between the state and society regarding security. The state can be both a point of reference and an agent of security, but, in principle, the society is the one defining its identity, while the state identifies and follows its interests [6].

2. The Dimensions of National Security

The traditional approach to the dimensions of the security concept identifies 3 analysis levels: individual, state and international. In the present view on the concept of security there are a number of constituents that act interdependently. These build-up a pluridimensional morphology of security that features: the political dimension, the military dimension, the economic dimension, the social dimension, the ecological dimension. Shaped for the first time during the Copenhagen School these dimensions have experienced a different evolution determined by the emergence of new types of threats to national security. Thus, although the political and military dimensions maintain their privileged place in the content of security, lately the accent was on the non-military aspects of security.

The political security focuses on the role of the state in international relations and possible threats to its security. Traditionally the political security was related exclusively to states survival and was defined in terms of sovereignty. Defending state's fundamental interests is its ultimate goal and this can be achieved mainly by increasing [7]. In the current political context, threats to a state's security can come from another state actor, but can also come from non-state actors .[8]

Military security refers to state's military capacity to confront internal or external aggressions [9]. Redefining the concept of security did not lead to a significant decrease in the role of armed forces and international military organisations. In the current geopolitical context, there was even noticed an increase in the competencies of

professionalised military bodies capable to assume specific missions [10]. Moreover, the discrepancy between the military capabilities of the states with advanced technologies and the military power of the states that have weapon systems from previous generations [11].

Economic security implies counteracting all the dangers, threats and risks to economic resources. Economic blockades and economic boycotts, as well as any limitations on the development of economic exchanges, fall in these categories [12]. The objective of economic security is to maintain a certain level of citizen welfare and cohesion of power through access to resources, finances and markets [13]. It is unanimously accepted that underdevelopment, famine and poverty constitute risks to security, regardless of its level (national, regional, continental or global) [14].

Ecological security presupposes protecting humans from the damage produced by environment deterioration. At the same time, this means protecting the environment from damage caused by man, because these can be a source of threats to the environment as a result of abusive behaviour that can lead to ecological disasters[15] . Deforestations, water pollution, natural and industrial gas emissions in the ozone layer, massive resource exploitation etc., all fall in this category.

Some authors criticize this multidimensional model of security finding the excessive expansion of the concept of security inefficient and dangerous. The main arguments are that the theoretical development of new dimensions can cause the dilution of the concept of security. Furthermore, the issue was raised on the danger of the “militarisation” of responses to problems deemed to threaten security by including in the same category very different threats that can generate a repressive approach to the detriment of political or social solutions [16].

Along with these dimensions of national security a number of authors theorized the informational dimension. This notion is based on the concept of informational security defined as “the state of protecting individual’s, society’s and state’s informational needs, that would allow guaranteeing their fulfilment and progressive evolution, irrespective of the presence of internal and external informational threats” [17]. Several types of informational security have been identified: physical security, document security, personnel security, communications security and computer security

[18]. On a theoretical level, it was proposed that a national informational security system be designed within the national security system, and that it had the following objectives: revealing and forecasting destabilising factors and informational threats to national interests; drafting a set of measures to prevent and remove these factors and threats; creating and maintaining a state of readiness of the forces and means of ensuring informational security [19].

By its characteristics (the absence of frontiers, dynamism and anonymity) the cyberspace ensures free access to information and communications, but it also represents a favourable environment for threats, vulnerabilities or incidents for the security of people and goods. In the light of the gravity of risks and threats, cybersecurity is deemed to be an important component of national security. This is why at European level there is an intense process of attunement and adaptation of the legislation regarding states' cybersecurity for the purpose of ensuring a safe, free and democratic cyberspace. The main directions of this process consist of elaborating a number of national strategies and adopting the legislative framework regarding the creation, administration and functioning of a cybersecurity integrated system is functioning.

3. Current Cybersecurity Regulations

In Romania, the relevant legislation in the field of cybersecurity is deficient in terms of systematisation and terminology. It is, mainly, the result of the process of transposition into the Romanian legislation of a number of directives from the Council of the European Union without the organic vision of the Romanian law maker for this essential field. From this viewpoint, we can see that cybersecurity regulation presents the same shortcomings that can be seen in Romania's national security general regulation.

The first regulatory act that affects this matter is Government emergency ordinance no 98/2010 on the identification, designation and protection of critical infrastructures [20], that represents the transposition into Romanian legislature of the Council's Directive 2008/114/CE of 8 December 2008 on the identification and designation of critical European infrastructures and evaluation of the necessity to improve their protection. By its provisions this ordinance established the legal

framework on the identification, designation of critical national/European infrastructures and evaluation of the necessity to improve their protection, with the aim of increasing the capability to ensure the stability, security and safety of the economic-social systems and the protection of individuals. In accordance with Article 3 (a) the critical national infrastructure represents “one of its elements, systems or components, on national territory, that is essential for the preservation of society’s vital functions, health, security, social or economic welfare of individuals, the perturbation or destruction of which would have a significant impact at national level as a result of the incapacity to preserve those functions”. For the purposes of the emergency ordinance, the protection of these critical infrastructures presupposes any activity that is intended to ensure infrastructure’s functionality, continuity and integrity in order to deter, diminish and neutralize a threat, a risk or a weakness.

Coordination, at national level, of the activities regarding the identification, designation and protection of critical infrastructures is carried out by the prime-minister through the appointed counsellor, and the designation of the critical infrastructure is carried out by Government Decision. Article 9 of Government Emergency Ordinance no 98/2010 mentions 3 cross-sectoral criteria underlying the identification of a critical infrastructure: the criterion on victims; the criterion on the economic effects; the criterion on the effect on population. In Annex 1 there are listed 10 sectors of the critical national infrastructure (energy; information technology and communications; water supply; nutrition; health; national security; administration; transportation; chemical and nuclear industry; space and research) each including more subsectors.

Government Decision no 1110/2010 on the competence, attributions and organisation of the Interinstitutional Working Group for the Protection of Critical infrastructures [21] establishes that this group is composed of experts/specialists appointed by competent public authorities (ministries, the Special Telecommunications Service, the Foreign Intelligence Service, the Romanian Intelligence Service, the Romanian Space Agency, etc.) and that it is coordinated by a state counsellor appointed by the prime-minister.

By Government Decision no 494/2011 for the Establishment of the Romanian National Computer Security Incident Response Team – CERT-RO [22] the attributions

of this public institution with legal personality as an independent expertise and research-development structure in the field of cyber infrastructure protection were established. In accordance with the provisions of Article 3 for cyber infrastructures administered by institutions in the field of defence, public policy and national security, CERT-RO carries out only the cooperation tasks, based on agreements concluded with their CERT structures.

This regulatory act also defines a set of notions and expressions, including "cybersecurity" and "cyber incidents". In accordance with Article 2 (e) by cyber security it is understood "the state of normality following the implementation of a set of proactive and reactive measures ensuring the confidentiality, integrity, availability, authenticity and non-repudiation of the information in electronic format, of public or private resources and services in the cyberspace. The proactive and reactive measures can include: policies, concepts, security standards and guides, risk management, instruction and awareness-raising, implementation of technical solutions to protect cyber infrastructures, identity management, consequences management". The cyber incident is any event that occurred in cyberspace and could affect cybersecurity.

The Cyber Incidents Real Time Early Warning and Information National System is constituted under CERT-RO. The data received in the system will be centralized and processed for the purpose of real time warning and issuing of reports regarding the distribution and nature of incidents, as well as for the collaboration with national authorities responsible for ensuring cybersecurity.

By Government Decision no 718/2011 on the approval of the National Strategy on Critical Infrastructure Protection [23] it was stated that this framework document is "intended for the adoption and implementation of specific measures and actions for the purpose of reducing the negative effects induced by specific risk factors on critical infrastructures, at national and regional level". The weaknesses, risk factors and threats in the field of critical infrastructure protection are defined in its body, and the main goals, strategic objectives and principles underlying the protection of critical infrastructures are identified.

A significant moment in building the cybersecurity concept was the adoption of Government Decision no 271/2013 for the approval of Romania's Cybersecurity

Strategy and the National Action Plan on the implementation of the National Cybersecurity System [24]. The scope of this strategy is to "define and maintain a safe virtual environment, with a high degree of resilience and trust, based on national cyber infrastructures that would constitute a significant support for national security and good governance, for maximising the benefits of the citizens, business environment, and Romanian society, as a whole". The concepts and definitions from previously adopted regulatory acts are included in its contents and new ones, like cyber threats, cyber terrorism, cyber espionage, security risks in cyberspace, cyber infrastructure resilience etc., are added.

Cyberspace threats are defined as circumstances or events that constitute a potential danger to cybersecurity. They take one of the following forms: cyber-attacks on infrastructures that carry public utility functions or informational society services the disruption/ affecting of which could be a threat to national security; unauthorized access of cyber infrastructures; unauthorized change, deletion or damage of informational data or illegal restriction of the access to this data; cyber espionage; material damage, harassment and blackmailing natural or legal persons, of public and private law.

Romania's Cybersecurity Strategy also establishes the foundations of the national cybersecurity system (SNSC). This represents the general cooperation framework that brings together public authorities and institutions for the purpose of coordinating actions nationally to ensure cyberspace security, including by cooperation with the academic and business environment, professional associations and non-governmental organisations. At national level, SNSC's activity is coordinated by the Supreme Council for Defence of the Country. In particular, SNSC's uniform coordination is carried out through the Cybersecurity Task Force Council (COSC) headed by the presidential counsellor for national security issues and composed of ministries and state bodies' representatives with attributions in the field of national security.

One of Romania's Cybersecurity Strategy objectives is to adapt the regulatory and institutional framework to the dynamics of threats specific to cyberspace. I this respect, it is stated that "the Romanian government will elaborate the draft law on cybersecurity, that will be submitted to Parliament for its approval, accordingly with the law".

In this context, on 30 April 2014, the Govern agreed the submission to the Chamber of Deputies, of the draft on Romanian cybersecurity. This regulatory draft was presented in the Statement of Reasons as a "national priority" the adoption of which aims: establishing the general framework for the regulation of cybersecurity activities; defining the obligations of the public or private law legal persons for the purpose of protecting cyber infrastructures; ensuring the general cooperation framework for cyber security, by establishing the National Cyber Security System [25]. On 16 September 2014 the draft law was adopted by the Chamber of Deputies, and on 19 December 2014 by the Senate, in its capacity as Decisional Chamber.

By Decision No 17 of 21 January 2015 on the objection of unconstitutionality of the provisions set out by the Law on Romanian Cybersecurity [26] the Constitutional Court assumed that this law's purpose "is to supplement the legal framework in the field of national security" and that this framework already includes "a set of regulations, primary or secondary regulatory acts". Consequently, beyond the 10 aspects of unconstitutionality, the Court found that "the whole regulatory act has deficiencies in terms of respecting the legislative technique norms, coherence, clarity, predictability, which could determine the violation of the principle of legality enshrined in Article 1 (5) of the Constitution".

4. Aspects of comparative law

In line with other regulatory models of cyber security we consider that a short analysis of the solutions adopted in France and the Republic of Moldova would be helpful. Both states recently had a broad debate on the recast of legislation regarding national security, including cybersecurity aspects. The French model is positively singularized also through an Internal Security Code, adopted on 12 March 2012, which enshrined security as a fundamental right and as one of the conditions for the exercise of individual and collective freedoms [27].

In France, the National Association for Information Systems Security (ANSSI) was established in July 2009 in order to ensure the technical aspect of these systems' security. In terms of national security, this body has prevention, audit and inspection tasks. In particular, it writes reports and recommendations and authorises the use of a number of cyber devices. Under it there is an Operational Centre for Informational

Systems Security (COSSIL) which, upon referral from another internal body, from a foreign partner or ex officio identifies the origin of a threat or a cyber-attack and takes appropriate technical measures [28]. The White Paper of Defence of 29 April 2013 defined the concept of cyber threat and put it on the third place in the risk list, after classic war and terrorist attacks. Based on this document, the Information Systems National Security Agency becomes National Authority and has new attributions in the field of control of the electronic communications operators [29].

In the Republic of Moldova, by Decision of the Supreme Security Council of 7 October 2014, it was recommended to the Parliament the examination, as a priority, of the regulatory acts drafts concerning the fields of informational security, prevention and counteraction of cybercrimes and telecommunications. Through the same decision, the Government was recommended more actions concerning cybersecurity as for example: the implementation of the Action Plan regarding the implementation of the "Digital Moldova" 2020 National Strategy for the Development of the Information Society; the creation of the national CERT (security incident response team); the elaboration and promotion of regulatory acts drafts in the field of information security; elaboration, approbation and implementation of a set of proactive and reactive measures to reduce possible information weaknesses, risks and dangers, to decrease the impact of threats, attacks and incidents from cyberspace etc. Last but not least, the Intelligence and Security Service of the Republic of Moldova was recommended to ensure the elaboration of the Information Security Conception and of the Information Security Strategy [30]. In this context, on 29 April 2015, during the ministerial session on cybersecurity, the minister of Information Technology and Communications of the Republic of Moldova launched a public debate for the Cybersecurity Programme Draft that contains a set of actions for the safety of processing, circulation, storing and accessibility of data in the digital environment.

5. Conclusions

The dynamics of the contemporary security environment makes the issue of regulating cybersecurity an essential objective for the national security policy. The solutions identified so far both in Romania and in other European states create the impression of a partial and deficient regulation. The national security policy actors

denounce the need for an adequate regulatory framework that would be effective against the numerous threats and danger in cyberspace. At the same time, regulating such a vulnerable field imposes respecting fundamental human rights, like the right to respect for private life and communications or the right for protection of personal data. Judicial review and the appointment of independent civil supervisory authorities are, in an equal measure, aspects concerned when elaborating any democratic legislation. In this respect, it is considered that the adoption of the NIS Directive (Network and Information Security) regarding the measures for ensuring a high common level of network and information security will have a positive impact on the regulation of cybersecurity in the states of the European Union.

Bibliography:

Băhnăreanu C., Resurse energetice, crize, conflicte, Bucureşti, Editura Militară, 2008.
Berbeca V. ş.a., Studii de securitate, București, Editura Cavallioti, 2005.
Dupic E., Droit de la Sécurité intérieure, Gualino éditeur, Lextenso éditions, 2014.
Gohin O., Latour X. (sous la direction de), Code de la sécurité intérieure, Paris, LexisNexis, 2014.
Irimia I., Balaban Ghe., Deac L. (coordonatori), Actualitate și perspective în dezvoltarea științei militare, I. Securitate și apărare națională. Securitatea națională a României și securitatea europeană, București, Editura Academiei de Înalte Studii Militare, 2003.
Jura C., Securitatea statelor, Privire specială asupra minorităților, București, Editura C.H. Beck, 2013.
Marin I., Ordinea constituțională și securitatea națională în contextul integrării și globalizării, Craiova, Editura SITECH, 2009.
Robinson P., Dicționar de securitate internațională, Traducere de Monica Neamț, Cluj-Napoca, CA Publishing, 2010.
Sgârcitu B., De la „M'Aider" la „Mayday", Impactul globalizării asupra securității naționale, București, Editura Tritonic, 2007.
Stoina N., Baboș Al., Sfârlog B., Studii privind problematica securității contemporane, Sibiu, Editura Academiei Forțelor Terestre, 2006.
Timofte Al.-R. (coordonator), Securitate şi societate: provocările mileniului trei, Secţiunea: Securitate şi siguranţă naţională, Securitatea la începutul mileniului trei, Editura A.N.I., Bucureşti, 2004.
Troncotă C. (coordonator), Neliniștile insecurității, București, Editura Tritonic, 2005.
Ţenu C., Deaconu Ghe. (coordonatori), Dimensiunea militară a securităţii, Bucureşti, Editura Universităţii Naţionale de Apărare „Carol I", 2009.
Ungureanu R.-S., Securitate, suveranitate și instituții internaționale. Crizele din Europa de Sud-Est în anii '90, Prefață de Andrei Miroiu, Iași, Polirom, 2007.

References:

[1] Dumitru A., România în noul context european, coordonate ale securității naționale, in Cristian Troncotă (coordonator), Neliniștile insecurității, București, Editura Tritonic, 2005, pp. 98-99.
[2] Sgârcitu B., De la „M'Aider" la „Mayday", Impactul globalizării asupra securității naționale, București, Editura Tritonic, 2007, p. 20.
[3] Stoica V., Managmentul comparat ca sursă de securitate, in Ion Irimia, Gheorghe Balaban, Liviu Deac (coordonatori), Actualitate și perspective în dezvoltarea științei militare, I. Securitate și apărare națională. Securitatea națională a României și securitatea europeană, București, Editura Academiei de Înalte Studii Militare, 2003, p. 159.
[4] Marin I., Ordinea constituțională și securitatea națională în contextul integrării și globalizării, Craiova, Editura SITECH, 2009, p. 19.

[5] Ungureanu R.-S., Securitate, suveranitate și instituții internaționale. Crizele din Europa de Sud-Est în anii '90, Prefață de Andrei Miroiu, Iași, Polirom, 2007, p. 44.
[6] Ibidem, p. 36.
[7] Dungaciu S., Securitatea politică şi securitatea societală. Securitatea dincoace şi dincolo de graniţele statului, în Veaceslav Berbeca ş.a., Studii de securitate, București, Editura Cavallioti, 2005, p. 146.
[8] Stoina N., Baboș Al., Sfârlog B., Studii privind problematica securității contemporane, Sibiu, Editura Academiei Forțelor Terestre, 2006, p. 106.
[9] Ţenu C., Deaconu Ghe. (coordonatori), Dimensiunea militară a securităţii, Bucureşti, Editura Universităţii Naţionale de Apărare „Carol I", 2009, p. 108.
[10] Braun N. D., Securitate și apărare. Prezent și perspective, in Ion Irimia, Gheorghe Balaban, Liviu Deac (coordonatori), op. cit., p. 179.
[11] Stoina N., Baboș Al., Sfârlog B., op. cit., p. 175.
[12] Băhnăreanu C., Resurse energetice, crize, conflicte, București, Editura Militară, 2008, p. 18.
[13] Radler D., Securitatea economică şi a mediului, in Veaceslav Berbeca ş.a., op. cit., p. 119.
[14] Creţu Ghe., Subdezvoltarea, foametea şi sărăcia riscuri la adresa securităţii statelor, in Alexandru-Radu Timofte (coordonator), Securitate şi societate: provocările mileniului trei, Secţiunea: Securitate şi siguranţă naţională, Securitatea la începutul mileniului trei, București, Editura A.N.I., 2004, p. 234.
[15] Robinson P., Dicționar de securitate internațională, Traducere de Monica Neamț, Cluj-Napoca, CA Publishing, 2010, p. 208.
[16] Jura C., Securitatea statelor, Privire specială asupra minorităților, București, Editura C.H. Beck, 2013, p. 21.
[17] Lanciu I., Războiul informațional și securitatea națională, in Cristian Troncotă (coordonator), op. cit., p. 307.
[18] For details see Robinson P., op. cit., p. 207.
[19] Ionel Lanciu, op. cit., p. 307.
[20] Published in the Romanian Official Gazette, Part I, no. 757 of 12 November 2010. Approved with changes by Law no. 18/2011.
[21] Published in the Romanian Official Gazette, Part I, no. 757 of 12 November 2010.
[22] Published in the Romanian Official Gazette, Part I, no. 388 of 2 June 2011.
[23] Published in the Romanian Official Gazette, Part I, no. 555 of 4 August 2011.
[24] Published in the Romanian Official Gazette, Part I, no. 296 of 23 May2013.
[25] Expunere de motive a Proiectului de lege privind securitatea cibernetică a României, p. 1(http://www.senat.ro/legis/lista.aspx)
[26] Published in the Romanian Official Gazette, Part I, no. 79 of 30 January 2015.
[27] For details see Gohin O., Latour X. (sous la direction de), Code de la sécurité intérieure, Paris, LexisNexis, 2014.
[28] Dupic E., Droit de la Sécurité intérieure, Gualino éditeur, Lextenso éditions, 2014, p. 257.
[29] Ibidem, p. 258.
[30] http://www.presedinte.md/rom/presa/consiliul-suprem-de-securitate-a-examinat-chestiuni-legate-de securitatea-informationala-a-republicii-moldova