CYBERSECURITY. RISKS, THREATS, AND TRENDS OF MANIFESTATION IN ROMANIA

Ileana-Cinziana SURDU

National Institute for Intelligence Studies, 'Mihai Viteazul' National Intelligence Academy, Bucharest, Romania

Abstract: *Over the past three decades, the internet has become a vital engine of contemporary life. In addition, a nation's electronic systems are seen as being part of its critical infrastructure, firstly because its malfunction implies a series of dangers in all societal aspects, and secondly because modern life is impossible if it's not "connected". While the need for cyber-security has emerged with the development of the first military computer networks during the later part of the Cold War, the implications of security incidents in cyber-infrastructure have multiplied exponentially since. Thus, the security of individuals and of cyber networks gained political significance in relation to the state, to the society, to the nation and to the economy. Given that the cybernetic infrastructure intersects with the financial, transportation, energy and national security infrastructures, Romania has been increasingly confronting cyber-threats, the citizens, the nation as a whole, and also the business and the governmental environments being affected. The paper analyses the reflection of the concept of "cybersecurity" in strategic documents and in the European legislation, as well as the trends of causes of cyber-insecurity at the level of the state and the individual, focusing on the situation in Romania. The analysis aims to track and describe the threats, the risks, the vulnerabilities, as well as their manifestation and the policies developed and implemented in order to ensure cybersecurity in Romania.*

***Keywords**: cybersecurity; cyber infrastructure; cybersecurity policies; cybernetic consumption behaviour*

1. INTRODUCTION

The internet has become over the last three decades a "vital engine" of the contemporary life, and the cybersecurity system is considered one of the most important infrastructure worldwide, once because its malfunction can lead to damaging results, and second, because of the "connected" characteristic of the modern life. (Simon *et al.*, 2009). The concept of "cybersecurity" has emerged as a reply to the technological innovations during the later part of the Cold War, when the first military computer networks have been developed. As a reply to the geopolitical conditions occurred after the Cold War, the security of the individuals and of the cyber networks became central factors of political interest in relation to the state, to the society and to the economy (Hansen, Nissenbaum, 2009: 1155).

Security threats are hard to identify, and, as such, are difficult to counterattack in an equal manner to the impact of their risks. Because functional fields at national level have become dependent on the cyber infrastructure, Romania has been confronting cyber threats in important sectors, like the financial system, transportation, energy, national defense, the business environment, the government, and the citizens as users. Seen as an interaction and communication facility, the cyber space offers different advantages too to the modern society, through the channels it provides for different actions, like: the promotion of national policies, the development of the business environment, the raise of quality of life as a result to the access to information, the understanding of national strategies, the access to warnings regarding the avoidance of risks and threats to the national security etc. (HG 271/2013: 10, 11).

Even though statistical data indicate a low level of internet utilization by Romanians, in comparison to the situation in other European states, the majority uses it to access social networks, a friendly and easy environment for cyber-attacks: 62.8% of the Romanian population in comparison to 80.2% of the European population (Internet in Europe Stats, 2017). At the same time, cyber-threats have increased over the last years, in Romania, and are set to follow an ascendant trajectory, justifying the necessity to define cybersecurity policies as a state priority.

2. THE CONCEPT OF CYBERSECURITY

The concept of cybersecurity has been initially used by scientists in the computers field at the beginning of the ’90s, to describe the insecurities of the computers which were network configured (Hansen and Nissenbaum, 2009: 1155). The term may have been included in a document for the first time in 1991, in the report of the COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD (CSTB), which described security as “protection against exposing, changes and unwanted destruction of data from a system and, also, the protection of the systems themselves” (CSTB, 1991:1, *apud* Hansen and Nissenbaum, 2009:1160). Cybersecurity has gained significance in the technical field regarding computer security when it was found that digital technology can become a threat for the society (Hansen and Nissenbaum, 2009: 1155). The cyber-space is non-governmental, according to Barnard-Wills and Ashenden (2012), who describe the internet through the filter of the vulnerabilities of the IT&C to cyber-attacks.

Cybersecurity is defined by THE ROMANIAN GOVERNMENT through the HG 271/2013 as “the normality state resulted after the implementation of and ensemble of proactive and reactive measures, which ensures the confidentiality, the integrity, the availability the authenticity and the non-repudiation of information in electronic format, of resources and public or private services, from cyber-space” (HG 2017/2013:7).

3. CYBERSECURITY: THE EUROPEAN FRAMEWORK AND MEASURES

The modern society is dependent on IT&C in its daily file, and the alert development of the technological system imposes drastic adjustments of the economic, political, cultural systems, and even at the level of the individuals’ living styles. The dynamic, the freedom and the anonymity of the cyber space act as opportunities for transferring information, but also as functional risks, factors which determine the necessity of promoting a cybersecurity culture among the state institutions, among companies, and among citizens.

The fight against cybercrime at the level of THE EUROPEAN UNION (EU) and The NORTH ATLANTIC ORGANIZATION (NATO) has started as a reply to the exponential increase of cyber-attacks and organized criminal groups who attack critical cyber infrastructure at the level of the member states.

The idea of cybersecurity has been included on the NATO agenda in the summit from Prague in 2002, reintroduced at the summit from Riga in 2006, an in the summit from Bucharest in 2008 has been adopted a cybersecurity policy. Because of the amplification of cyber-attacks, the field has gained a higher importance; as such, in the summit from Lisbon in 2010, a strategic concept has been adopted, which addresses the types of cyber-threats, their impact over the critical infrastructures, and prevention, counteraction and reaction proposed strategies. The summit from Whales in 2014 placed cybersecurity in the responsibility of NATO in what concerns the collective defense; the member states are also responsible for protecting the national networks. During the summit from Warsaw in 2016, cyber-space has been ascertained as an operational field, which is to be treated with the same importance as the air space, the terrestrial space and the maritime area (The Ministry of Foreign Affairs: MAEb).

THE EUROPEAN COMMISSION (EC) has identified the priorities and the strategic actions in the field of cybersecurity, at the level of the EU member states. The process resulted in a cybersecurity strategy, which targets to ensure a free and safe cyber-space. The strategy has been elaborated as an effect of the necessity to respect the fundamental rights, the democracy and the legislation in the online area. The EC (2013) underlines the importance of the collaboration between the government and the private sector in the process of ensuring cybersecurity at national level, both parts holding and using a significant amount of the cyber-space. Cybersecurity is defined by the EC (2013) through the actions implemented in the direction of protecting the cyber-space, both in the civil and in the military worlds. The cybersecurity strategy at European level starts from the premises that the threats can be of any nature: political, terrorist, disasters or simple errors. The document states that the EU’s economy has already been affected by cyber-crime, which targeted the private sector and the citizens, manifested through data theft, economic espionage, fraud, the mass distribution of hate materials, or attacks of cyber-systems. The strategy establishes five strategic priorities to be assumed by European institutions and the member states:

1) the achievement of a high level of cybernetic resiliency, by developing a cooperation environment between the public and the private sector, and by benefiting of the support of THE EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA) and having as base The NIS

Directive. The EU strategy (2013) proposes the implementation of a legislative framework in every EU member state, in order to appoint an authority to implement the NIS Directive, to develop a computer emergency response team institution, to adopt a national strategy and a cooperation plan similar to the NIS Directive. In order to facilitate these measures, in 2012 has been established an emergency team, responsible of the cyber systems of the EU, THE COMPUTER EMERGENCY RESPONSE TEAM (CERT-EU); an EU financing line (Connecting Europe Facility – CEF) is destined to the key infrastructure of an efficient cooperation in this area.

2) the drastic decrease of the level of cyber-crime. According to the EU Strategy (2013), cyber-crime includes a series of criminal acts, which implies computers and cyber systems, used as instruments or as targets, aiming to attack them or to spread offensive information. The solution proposed is to implement a collaborative and coordinated inter-state approach, in accordance to the regulations resulted in "The Convention of the Council of Europe on Cybercrime", from Budapest. The development of a specialized entity in the field at the level of each EU state is a precondition in order to achieve this priority. THE EUROPEAN CYBERCRIME CENTRE (EC3) is a center which supports the EU states in this area, responsible for the alignment of counteracting cybercrime, using a selection of good practices.

3) the elaboration of cybersecurity policies and the development of afferent capacities, having as base the Common Security and Defense Policy (CSDP). The defense dimension represents a pylon of cybersecurity, which targets the increase of the resiliency in the case of communication and computer systems, through detecting, response and recurrence measures. In order to achieve this priority, it is necessary a better cooperation between governments, between the private sector and the academic one, and between civil and military communities.

4) the development of technological and industrial resources for cybersecurity, including the hardware and the software components, used by critical services and infrastructures; they have to be safe and trustful and to guarantee the protection of personal data.

5) the establishment of international policies concerning cybersecurity. These policies must contribute to maintaining a free, open and safe cyber-space and can be implemented only with the cooperation of EU, international organizations, international partners, the private sector and the civil society. (European Commission, 2013)

The EU aims to respect freedom, security and justice for the citizens, no matter the place they migrate to. As a response to the last years' threats and terrorist attacks, radicalization and violence manifestations, the EU elaborated a cooperation synergy through The European Agenda on Security (2015). The document prioritizes for each EU state the security against terrorism, organized crime and cyber-crime. The Agenda (2015) argues that the main pylon in confronting cyber-crime is by strictly implementing the afferent European legislation.

In 2016, THE EUROPEAN PARLIAMENT and THE EUROPEAN COUNCIL have elaborated the network and information systems (NIS) Directive, which provides measures of ensuring the security of cyber networks and systems in the EU. The Directive substantiates the essential impact which the computer systems and services have over the society, as their security represents a vital factor in the efficient functioning of economic, social and internal market spheres. The document places the responsibility of cyber networks and systems in the yard of each EU member state, through the essential services operators ("entities which offer an essential service for the implementation of societal and/or economic activities of high importance") and the digital service suppliers (The NIS Directive, 2016: 14, 27-29). Considering that a high and common level of cybersecurity can be achieved more efficiently at the level of EU instead of at the level of each state, the Directive imposes the development of a support group in the process of strategic cooperation between the states. The group has the role to "support the member states in adopting a coherent approach in the process of identification of the essential services operators" (*idem*: 14). The document also imposes the functioning of an intervention network (CSIRT), the adopting of a national strategy of cybersecurity by each member state, and the establishment of national contact points of CSIRT; this last entity has the responsibility to ensure the border cooperation with other member states, with the cooperation group and with the CSIRT network.

The UE Directive (2016) considers necessary the institution of a cooperation group at the level of the EU member states, composed out of representatives of the states, of the EC and of ENISA. The group would support the strategic cooperation in the area of cybersecurity, and would help to implement a general and common mechanism, able to reply to the dynamism and amplitude of the risks and threats, as not every EU state has the necessary response capacities. As such, ENISA organizes CyberEurope exercises every year, which have the role to prepare the states for possible incidents: the exercise from 2016 involved over 1000 participants from 30 European states, representatives of over 300 organizations from IT&C and experts in cybersecurity (The Ministry of Foreign Affairs: MAEc).

The ”EU Global Strategy for Foreign and Security Policy” (2016) is another instrument that targets the security at UE level, which resulted after the consultation of the EU member states, of the European institutions and of the civil society regarding the characteristics and the common needs of the countries. This strategy establishes among its priorities the guarantee of cybersecurity at the European level. As such, it states that this desiderate will be possible only after the proper endowment with the necessary equipment and by ensuring an assistance service at the level of each state. The strategy establishes that each state must implement a process of consolidation of the technological capacities, by implementing innovative IT&C systems, by including it in the political priorities, and by developing cooperation platforms. Also, the promoting of a cybersecurity culture is an essential step in ensuring cybersecurity, as a result of the cooperation between the EU member states, institutions, the private sector and the civil society.

The constant communication of the support proves to be and essential factor in the inside – and between states-cooperation. As such, in 2017 the EC published “A Strategic Approach to Resilience in the EU's External Action”, which ensures the support from EU to the member states in the process of raising of resiliency level to the global challenges, through a process of developing capacities to anticipate, prevent and prepare. Jean-Claude Juncker, confirmed the priority of actions in cybersecurity in the Address from 13 September 2017. He argues that it is necessary to cooperate in order to protect Europeans in a digital era, by implementing new rules of protecting the intellectual property, of cultural diversity and of personal data, but also through a better equipping for preventing and counteracting cyber-attacks. Juncker evaluates that cyber-attacks can be “more dangerous to the stability of democracies and economies than guns and tanks”. He continues with the proposal to establish an European Cybersecurity Agency, as a reply to the approximately 4000 cyber-attacks per day registered at European level.

4. CYBERSECURITY AT NATIONAL LEVEL: THE ROMANIAN FRAMEWORK AND MEASURES

Romania answers through its objectives and actions to the EU and NATO initiatives, understanding the risks and the vulnerabilities of the country to possible cyber-threats and attacks. As such, “The Cybersecurity Strategy of Romania” shapes the directions and lines of action of cybersecurity at national level, aiming to promote the national security interests and the objectives in what concerns the cyber-space.

The measures proposed through the strategy include anticipation, protection, identification and counteraction of threats, attacks, incidents and even actions against acts of cyber-terrorism and cyber-espionage. The cyber-terrorism is seen as “premeditated activities implemented in cyber-space by individuals, groups or organizations politically, ideologically or religiously motivated, which can result in material destructions or victims, aimed to provoke panic or terror” (HG 271/2013:8). The cyber-espionage, on the other hand is described as “actions developed in the cyber-space, aiming to obtain unauthorized and confidential information, for the interest of a state on non-state entity” (*ibidem*).

As such, these measures can be included in policies, guides, regulations, security instructions, and their implementation can begin with technical solutions for protecting the cybernetic infrastructures (HG 271/2013:7-8). The measures imply a series of principles of relationship between the responsible entities: the coordination of the activities in an unitary vision, cooperation, the efficient management of available resources, the prioritization of securing the cybernetic infrastructures, the dissemination of good practices, the protection of the right to privacy and other human fundamental rights, the assuming of the responsibility of se security of cybernetic infrastructures by owners and users and the separation of internet networks from the networks that ensure the functioning of the state. (*idem*: 8-9)

In order to implement the proposed measures, the strategy establishes ten steps:

1) adapting the normative and legislative framework to the specific of cyber-threats;

2) identifying and applying security standards of cybernetic infrastructures with impact over the critical infrastructures at national level;

3) educate the competent authorities, the state institutions, the companies and the individuals in the field of cybersecurity and resiliency;

4) using cyber-space to promote the national interests and objectives;

5) promoting cooperation and partnership between the private and the public sectors, and also with other international entities;

6) elaborating instruments for developing cooperation and a mechanism of warning, alert and reaction;

7) promoting trust at international level in using cyber-space;

8) stimulating research and innovation in the field of cybersecurity;

9) developing resiliency of cybernetic infrastructures;

10) supporting the functioning of public or private entities in the field of cybersecurity. (HG 271/2013:6, 7, 11, 12)

The most of the times cyber threats end through cyber-attacks over the national infrastructure, which disturbance constitute a danger to the national security. These actions can lead to damages, or blackmailing legal or private actors. The main actors who are a threat to cybersecurity are, usually, individuals or organized crime groups who exploit vulnerabilities in order to obtain different benefits, terrorist or extremists who use the cyber-space to communicate, state or non-state actors who collect information or initiate threats to national security. (*idem*: 10).

The main purpose of the cybersecurity strategy is the establishment of a national entity who would supervise the logical implementation of the warning and resiliency measures to cyber-attacks, which target national private or public institutions. The proposed entity, THE NATIONAL CYBERSECURITY SYSTEM (SNSC), gathers public authorities and institutions who act in the field of cybersecurity, targeting to coordinate the cybersecurity activities, including the collaboration with the academic field, with the business environment, with associations and non-governmental organizations (The Ministry of Foreign Affairs: MAEa). SNSC provides the necessary information in order to implement cybersecurity measures, and ensures the efficient reaction to cyber-threats and cyber-attacks (HG 271/2013:12-14). SNSC is coordinated through THE OPERATIVE COUNCIL OF CYBERSECURITY (COSC), which includes representatives of ministries and entities with responsibility in ensuring cybersecurity; THE ROMANIAN INTELLIGENCE SERVICE ensures the technical coordination of COSC and THE ROMANIAN GOVERNMENT coordinates the security activity in the field of electronic communication conducted by public authorities which are not members of COSC (*idem*: 14-15).

As a response to the EU requests, THE ROMANIAN NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAM (CERT-RO) has been created through HG 494/2011. Its role is to offer support in case of informatics emergencies, to manage risks and incidents and to cooperate with other CERT institutions at European level and with the EU. In 2012 ENISA has launched the “European Cyber Security Month – ECSM”, an awareness campaign among European citizens, where CERT-RO took part in every sessions, as a national partner (cert.ro, July 2017).

In case of cyber-attacks over Romania, SNSC collaborates with homologous institutions from other countries. SNSC also has established “the national cyber-alert system (SNAC), targeting to prevent and counteract cyber-risks and attacks; as such, SNAC evaluates the risk management of cybersecurity in Romania and establishes the levels of cyber-alerts (NAC). (The Ministry of Foreign Affairs: MAEa)

The National Strategy regarding the Digital Agenda for Romania 2020 (2015) proposes the development of the IT&C sector, as base in the process of economic development and aiming to increase the country’s competitiveness on the international market. In this context, CERT-RO represents a confirmation of the development process in the national cybersecurity field. The agenda (2015) foresees the collaboration between the private and the public sector to protect the cyber-space and considers that there is a need of improvement of the afferent legislation.

Taking into account the international legislation in the field of cybersecurity, the Romanian state is working on the national normative framework, aiming to facilitate the cooperation between and with the responsible and competent entities in order to combat the use of critical infrastructure in terrorist or criminal purposes. The law project published in April 2016 addresses public authorities, legal and private entities who own, manage or use cybernetic infrastructures. The institutional working group (GLI) is the main actor responsible with the promoting of the cybersecurity law. (The Ministry of Foreign Affairs: MAEa)

HG 718/2011 provides measures of protection for the critical infrastructures, the cybernetic dimension of equipment being considered a category with major risks in the functioning of computer systems (European Commission, 2016).

The Romanian National Strategy of Defense for the period 2015-2020 (SNAP) sets among its objectives the consolidation and the protection of critical cybernetic infrastructures (SNAP, 2015).

The SNAP (2015) characterizes the current security environment as complex and dynamic, open to multiple challenges, ones predictable, and others unpredictable. The document finds that the cyber-threats are 1) launched by hostile organisms, state or non-state ones, with an impact over the cybernetic infrastructures of the state institutions and of companies at national level, or 2) developed by criminal groups, or 3) by hackers.

A comparison to the priorities established through SNAP (2015) and the previous version of the security strategy, that is "The National Security Strategy of Romania" (SSNR, 2006), shows that the concept of cybersecurity has been first introduced in the SNAP. SSNR treats the critical infrastructures with the same level of importance, referring to the computer systems and networks. The document identifies computer aggressions as asymmetrical threats, military or civil, originating from external sources and only a few from internal ones, with a harmful impact over the citizens, over the state institutions and over the security entities of the state.

The SNAP guide (2015) a sequential process in establishing ways of eliminating cyber-aggressions and attacks, of identifying possible sources and targets of it, and also of understanding the final purpose of the whole process of cybersecurity, in relation to the national objectives and interests. (SNAP guide, 2015:25-33)

In order to implement the lines of actions proposed, the SNAP guide (2015:27-32) proposes also ways of implementation, targeting a gradually route in the process of eliminating cyber-threats and accentuates the importance of communication, of dialogue, of cooperation and partnership, at internal level and also at external level. The measures target to install reaction capabilities, the learning from good practices, and collaboration with diverse entities from the field of cybersecurity, all of it being actions which can strengthen the Romanian state's capacity in crisis situations.

5. CYBERNETIC CONSUMPTION BEHAVIOURS

Cybersecurity has gained importance after several European countries have been subject to cyber-attacks in the last years. The special Eurobarometer on cybersecurity (2017), which collected data in June 2017 at the level of 28 EU countries, on a sample of 28,093 respondents, shows that for 56% of the subjects cyber-crime represents a very important challenge for the internal security of the EU, and only for 7% it is not important. The data show an increase in perception regarding this aspect with 14% from 2015 and with 13% from 2011. 37% of the respondents consider that the public authorities in their countries aren't doing enough to fight cyber-crime. The data show an increase in concerns regarding internet usage, in comparison to the situation registered in 2014 and 2013: 45% of the subjects (N=22,236) are worried about misusage of their personal data (43% in 2014 and 37% in 2013) and 42% are concerned about online payments (35% in 2013). Out of the respondents who are internet users (N=22,472), 45% have installed an anti-virus or have changed the software because of security privacy issues and 39% of them declared that they are less likely to give personal data on websites. At the same time, 51% of the respondents declared they are not well informed regarding cyber-crime. Romania registers the lowest proportion of respondents who declared that are very well informed about the risks of cyber-crime (4%) after Italy (2%). The most frequent form of cyber-crime people have experienced (N=22,236) was discovering malicious software on the devices (42%), followed by receiving fraudulent e-mails or phone calls, asking for personal data (38%). In case of people who were victims of cyber-crime, 85% said they called the authorities in case of theft, 76% for banking fraud, and 76% for encountering child pornography. In 21 of the total EU member states, the majority of people would contact an authority in case of bank related fraud; the lowest proportions have been registered in case of racial hatred speech, or religious extremism.

In Romania, CERT-RO has received during the whole year of 2016 110,194,890 cybersecurity alerts, out of which 1,363 have been manually solved, registering an increase of 61.55% in comparison to the situation in 2015. The safest operation systems in Romania have proved to be Windows (0.57% of the alerts) and UPnP OS (8.08% of the total alerts). The most alerts were classified as fraud (37.05%) and only 2.71 as cyber-attacks. Romania has been the subject of cyber-attacks several times: the GoldenEye effect in 2017, which blocks the computer system and requires 300 $ to unblock it, the malware campaign which urges people to click on a virused message, or the Scam campaigns in 2013, which tricked people to register for fictive vouchers or plane tickets (cert.ro).

Any malicious action in the cybernetic sphere is made known to people accompanied by a solution of response (whenever it is possible), by the associated risks, and by ways of prevention and detection. The development of an attitude and of a behavior in accordance to a cybersecurity approach is, thus, supported by national entities, which addresses the citizens; they are the ones who represent the essential element of ensuring cybersecurity.

5. CONCLUSIONS & ACKNOWLEDGMENT

The establishment and the maintaining of cooperation and partnerships between the public and the private environments are primordial actions in order to ensure the cybersecurity at national level. As such, communication and dialogue are the base for a functional relationship, and also the share of available resources as instruments to implement the measures and lines of action established through the strategies and norms of regulation the cybersecurity field at national level. Thus, the cooperation with partner or ally international entities, and adapting international efficient measures, are aspects that strengthen the capacities of the responsible entities with cybersecurity, at national level.

Although the statistical data show a low level of usage of the internet in the case of Romania, in comparison to other European states, the majority of the people uses it to access social networks, the most common and propitious channel for cyber-threats. At the same time, the level of cyber-threats is set on an ascendant trajectory, justifying the need to treat cybersecurity in relation to the state's priorities.

The authors take full responsibility for the contents and scientific correctness of the paper.

BIBLIOGRAPHY

1. Barnard-Wills, D. & Ashenden, D. (2012). Securing Virtual Space: Cyber War, Cyber Terror, and Risk. In *Space and Culture*. Vol. 15 (2). 10-123.
2. CERT-RO. (July 2017). *European Cyber Security Month 2017*. [online]. URL: https://www.cert.ro/citeste/ecsm-2017-preview. [14/09/2017]
3. CERT-RO. (2016). *Raport cu privire la alertele de securitate cibernetică procesate de CERT-RO în anul 2016 – Raport*. [online]. URL: https://www.cert.ro/vezi/document/raport-alerte-cert-ro-2016. [14/09/2017]
4. CERT-RO. The alert section. [online]. URL: https://www.cert.ro/tag/alerte. [14/09/2017]
5. European Commission. (13 September 2017). *European Commission – Speech. President Jean-Claude Juncker's State of the Union Address 2017*. [online]. URL: http://europa.eu/rapid/press-release_SPEECH-17-3165_en.htm. [20.03.2018]
6. European Commission. (2017). *Joint Communication to the European Parliament and the Council. A Strategic Approach to Resilience in the EU's External Action*. [online]. URL: https://eeas.europa.eu/sites/eeas/files/join_2017_21_f1_communication_from_commission_to_inst_en_v7_p1_916039.pdf. [20.03.2018]
7. European Commission. (September 2017). *Special Eurbarometer. Europeans' attitudes towards cyber security*. [online]. URL: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2171. [24/04/2018]
8. Hansen, L. & Nissenbaum, H. (December 2009). Digital Disaster, Cyber Security, and the Copenhagen School. In *International Studies Quarterly*. Vol. 53 (4): 1155-1175.
9. Internet in Europe Stats. (2017). *Internet User Statistics & 2017 Population for the 53 European countries and regions*. [online]. URL: https://internetworldstats.com/stats4.htm#europe. [20.03.2018]
10. Simon, S., de Goede, M., Goede P. A., Anderson and Graham, S. (January 2015). Cybersecurity, Bureaucratic Vitalism and European Emergency. In *Theory, Culture & Society*. Vol. 32 (2): 79-106.
11. The European Commission. (2013). *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. [online]. URL: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf. [08/09/2017]
12. The European Commission. (2015). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security*. [online]. URL: https://ec.europa.eu/home- affairs/sites/homeaffairs/files

/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf. [15/09/2017]

13. The European Commission. (2016). *The Directive on security of network and information systems (NIS Directive).* [online]. URL: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive. [24/08/2017]
14. The European Commission. (2016). *Viziune comună, acțiuni comune: o Europă mai puternică. O strategie globală pentru politica externă și de securitate a Uniunii Europene.* [online]. URL: http://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_ro_version.pdf. [15/09/2017]
15. The Ministry of Communication and Informational Society. (February 2015*). Strategia Națională privind Agenda Digitală pentru România 2020.* [online]. URL: https://ec.europa.eu/epale/sites/epale/files/strategia-nationala-agenda-digitala-pentru-romania-20202c-20-feb.2015.pdf. [15/09/2017]
16. The Ministry of Communication and Informational Society. *Legea privind Securitatea Cibernetică a României.* [online]. URL: https://www.comunicatii.gov.ro/?p=5862. [31/08/2017]
17. The Ministry of Foreign Affairs (MAEa). *The Cybersecurity Strategy of Romania.* [online]. URL: http://mae.ro/node/28367. [31/08/2017]
18. The Ministry of Foreign Affairs (MAEb). *Delegația permanentă a României la NATO. România în Nato: Apărarea cibernetică.* [online]. URL: https://nato.mae.ro/node/435. [31/08/2017]
19. The Ministry of Foreign Affairs (MAEc). *Problematica securității cibernetice în cadrul organizaţiilor internaţionale şi implicarea României ca membru al acestora.* [online]. URL: http://mae.ro/node/28369. [15/09/2017]
20. The President of Romania. (2015). Strategia națională de apărare a țării pentru perioada 2015-2019. O Românie puternică în Europa și în lume. Approved by the common Decision of the Senate and the Deputy Chamber, June 23, 2015. *The Official Gazette,* First Part. No. 450/ June, 23.
21. The President of Romania. (2015). *Ghidul Strategiei naționale de apărare a țării pentru perioada 2015-2019* (GSNAp). Approved by CSAT Decision no.128/ December 10, 2015. Bucharest: Presidential Administration.
22. The Romanian Government. (2013). *HG 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.* [online]. URL: https://www.comunicatii.gov.ro/wp-content/uploads/2016/02/Strategie-securitate-cib-HG-271-2013.pdf. [24/08/2017].
23. The Romanian Government. (2011). *HG 718/ 2011 pentru aprobarea Strategiei naționale privind protecția infrastructurilor critice.* [online]. URL: http://legislatie.just.ro/Public/Detalii Document/130566. [31/08/2017].