PRELIMINARY OBSERVATIONS ON CYBERCRIME, CYBERSECURITY AND NATIONAL SECURITY

Gheorghe-Iulian IONIȚĂ
„Acad. Andrei Rădulescu" Reasearch Institute, Romanian Academy
Faculty of Law, Alexandru Ioan Cuza University
Faculty of Law, Romanian-American University
Bucharest, Romania
ionita.gheorghe.iulian@profesor.rau.ro

***Acknowledgement**: This work was supported by the strategic grant POSDRU/159/1.5/S/141699, Project ID 141699, co-financed by the European Social Fund within the Sectorial Operational Program Human Resources Development 2007-2013.*

Abstract: *The draft law on Romania's cybersecurity has given birth to much debate. In order to stress a number of issues, the author presents concepts such as cybercrime, cybersecurity and national security, their significance/trends, their relationships and how they stem from internal regulations and activity reports of competent organisms in the field.*
Keywords: *cybercrime, cybersecurity, national security.*

1. GENERAL OBSERVATIONS

As we have already indicated (Sandu, F., Ioniță G.-I., 2005: 265) (Ioniță G.-I., 2011: 9), the "computerization" of social life and perpetrators' increased technical skills have led to the occurrence (or grafting of "classic" criminal elements) of a new form of criminality in general, cybercrime, which developed and diversified invading increasingly all sectors of activity.

Due to the size of this phenomenon, authorities have raised the issue of whether it is a threat to Romania's national security and, since the answer was positive, Romania's Cybersecurity Strategy was drafted, followed by the promotion of a Draft Law on Romania's cybersecurity, which led to much debate.

2. THE CONCEPT AND TRENDS OF CYBERCRIME

2.1 The concept of „cybercrime"

A. Romania's Cybercrime Strategy (SCND, 2013) define cybercrime as (art. 3) all the acts stipulated by the criminal law or any other special laws which represent a social danger and which are carried out willingly through or against cyberstructues.

B. The Draft Law on Romania's cybersecurity (CoD, 2014) (the initial version), the definition of "cybercrime" seems to have been taken (under art.5 point 5) from Romania's Cybersecurity Strategy (art. 3) because, in the Advisory opinion on this draft law (LC, 2014), at point 6, the Legislative Council specified that the definition of "cybercrime" considers the essential features of the crime, as stipulated in the 1968 Criminal Code, and not the definition set through the provisions of art.15 of the new Criminal Code (Law no.286/2009). At any rate, in the version adopted by the Chamber of Deputies and sent to the Senate, the definition of cybercrime is no longer included.

2.2 Cybercrime trends

According to Directorate for Investigating Organized Crime and Terrorism (DIOCT, 2014: 63-66), the concrete analysis of solved cases also confirmed for the year 2013 a statistically growing trend; thus, it was noted that:

- the number of files remaining from the previous years has grown (1784 files in 2013 as compared to 1602 files in 2012), just like the number of new files (1836 files in 2013 as compared to 1521 files in 2012).
- the number of solved files has grown (1121 files in 2013, as compared to 852 files in 2012), simultaneously with the number of indictments (173 indictments in 2013 as compared to 168 in 2012) and the number of convicted persons (373 defendants in 2013 as compared to 351 defendants in 2012).

From among the important files solved by Directorate for Investigating Organized Crime and Terrorism in 2013, here are some of the most relevant (DIOCT, 2014: 67-74).

A. In file no. 100/D/P/2011 of the Territorial Bureau of Sibiu, under the indictment, arraignment was decided for 54 defendants (out of whom 13 in remand) for acts of setting up, adhering to or supporting, under any form, an organized criminal group as stipulated at art. 7 of Law no. 39/2003, fraud with particularly serious consequences in continued form, as stipulated at art. 215 paragraphs 1, 2, 3, 5 of the Criminal Code with enforcement of art. 41 paragraph 2 of the Criminal Code, electronic fraud in continued from, as stipulated at art.48 of Law no.161/2003.

The defendants were part of a group organized in order to obtain financial benefits from misleading several damaged parties, money transfer units within banking institutions, supermarkets and other companies, by having the employees thereof enter incorrect data in the money transfer applications. Thus, the defendants contacted employees of the damaged parties under a false identity and pretending to be calling from the bank headquarters and, under the false pretense of system trials, asked them to operate money transfers onto the names of persons especially recruited to this end. Subsequent to the operations and after the transaction code was obtained, it was sent by SMS to other members of the group, who, against a fee, withdrew quickly the amounts from the accounts where they had been transferred in order to avoid the transaction being blocked. In some cases, the group members sent electronic messages to employees' professional emails, whereby they were informed that "simulations" were to take place

for the system, and they also specified a phone number which was previously identified by defendants by deviating the call to the mobile phone number used by them in jail.

The damage created following these acts was estimated to RON 154,600 and EUR 235,000, while the amount of damaged goods was RON 180,000.

The file was referred for settlement to the Court of Prahova.

B. In file no.89/D/P/2010 of the Territorial Bureau of Maramureş, under the indictment, arraignment was decided for a defendant who committed the crimes stipulated at art.48 and art.49 of law 161/2003, both with enforcement of art.41 paragraph 2 of the Criminal Code, art.290 of the Criminal Code, with enforcement of art. 41 paragraph 2 of the Criminal Code, art. 29 paragraph 1 letters a and b of Law 656/2002 (money laundry), art.246 of the Criminal Code with reference to art.258 of the Criminal Code, all with the enforcement of art. 33 letter a of the Criminal Code.

The defendant, an employee of B.C.R. Branch from Şomcuta Mare, Maramureş County, damaged over 30 natural persons and legal entities (customers of the bank) through the electronic system used, then used the amounts so as to obscure their origin through investments in the construction of a building.

The total damage due to these criminal acts was estimated to RON 1,114,492.03, EUR 55,350 and USD 495, and in order to recover this amount, insuring measures were established on the defendant's movables and immovable properties.

The file was referred for settlement to the Court of Maramureş.

C. In file no.64/D/P/2011 of the Territorial Bureau Craiova, under the indictment, arraignment was decided for 23 defendants for committing crimes stipulated at art. 7 paragraph (1), with reference to art.2 letter b points 14 and 18 of Law 39/2003; art.25 of the Criminal Code with reference to art.42 paragraphs (1), (2) and (3) of Law 161/2003 with reference to art.41 paragraph 2 of the Criminal Code; art.26 of the Criminal Code with reference to art.49 of Law 161/2003, with enforcement of art.41 paragraph (2) of the Criminal Code; art.27 of Law no.365/2002 with enforcement of art.41 paragraph (2) of the Criminal Code; art.26 of the Criminal Code with reference to art.215 paragraphs (1), (2), (3) and (5) of the Criminal Code with enforcement of art.41 paragraph (2) of the Criminal Code; art.293 paragraph (1) 2nd thesis and paragraph (2) of the Criminal Code and art.29 paragraph (1) letters a and b of Law 656/2002.

It was noted that, in the period 2006-2011, the defendants organized a criminal group which operated in a coordinated manner in order to commit several serious crimes on the territory of Romania, the USA, England and Canada, committing crimes such as electronic fraud, unauthorized access to computer systems, money laundry, and false identity. More precisely, a network was organized and specialized in fraudulent Internet transactions which estranged important amounts from people mostly of American, British and Canadian citizenship. The group members used false documents (IDs, passports, driving licenses, false diploma degrees) which they provided to accomplices in order to withdraw money. The amounts obtained from these crimes were used to buy movables and immovables, but they were also divided among several persons in order to obscure their origin.

The total damage due to the defendants' criminal activity was estimated to RON 858,088 and in order to recover it, the measure of distraint was decided upon some movables and immovables.

The file was referred for settlement to the Court of Gorj.

3. THE CONCEPT AND SIGNIFICANCE OF CYBERSECURITY

A. Romania's Cybersecurity Strategy (SCND, 2013) defined cybersecurity (art. 3) as the normality condition resulting from the enforcement of a proactive and reactive set of measures which ensure the confidentiality, integrity, availability, authenticity and non repudiation of information in electronic format, of public or private resources and services from cyberspace.

In this context (SCND, 2013), proactive and reactive measures (which are applied in order to ensure normality) may include policies, concepts, standards and guides of security, risk management, training and awareness activities, the implementation of technical solutions for the protection of cyber infrastructures, identity management, consequence management.

The need to adopt the Cybersecurity Strategy, as presented in the Substantiation Note to Government Decision no. 271/2013 (on the approval of the enforcement thereof) (GoR, 2014a), is represented by:

- setting the conceptual, organizational framework necessary to ensure cybersecurity;
- developing the national risk management abilities in the field of cybersecurity and reaction to cyber incidents under a National Program;
- promoting and strengthening the security culture in the cyber field;
- developing international cooperation in the field of cybersecurity.

In a synthesis (MoFA, 2014), Romania's Cybersecurity Strategy presents the main objectives, principles and directions for the awareness, prevention and fight of threats, weak points and risks related to Romania's cybersecurity and for the promotion of domestic interests, values and objectives in cyberspace.

B. The Draft Law on Romania's cybersecurity (CoD, 2014) takes over (art.5) the definition of cybersecurity (including observations on proactive and reactive measures) from Romania's Cybersecurity Strategy (art. 3).

This normative draft (CoD, 2014) stipulates (art. 4) that cybersecurity aims:

- to create the resilience of cyber infrastructures;
- to increase the ability to react to cyber incidents and to diminish their impact on the resources and services of cyber infrastructures;
- to ensure the protection of data managed through cyber infrastructures;
- to ensure the trust necessary to develop the information society and business environment in cyberspace;
- to ensure equal and non discriminating access of persons to public information and services provided through cyber infrastructures;
- participative, democratic and efficient governance of cyberspace;

- to make cyber infrastructure owners aware of the need to ensure cybersecurity;
- to ensure the climate necessary to exert people's fundamental rights and freedoms in cyberspace.

It also mentions [art.3 paragraph (1)] (CoD, 2014) activities which ensure cybersecurity, namely:

- knowing, preventing and fighting threats and attacks, and diminishing the weak points of cyber infrastructures for the purpose of managing risks related to the security thereof;
- preventing and fighting cybercrime;
- cyber protection.

4. THE CONCEPT AND SIGNIFICANCE OF NATIONAL SECURITY

A. Romania's National Security Strategy (SCND, 2007) mentions (in its first sentence), the significance of national security, namely that it:

- represents the fundamental condition for the existence of the Romanian nation and State (as well as a fundamental objective of government)
- refers to national values, interests and objectives.

In the same context (SCND, 2007), it has been stressed that national security:

- is an imprescriptible right which derives from complete sovereignty of the people;
- relies on constitutional order;
- occurs in the context of the European construction, Euro Atlantic cooperation and global evolutions.

As for the measures/activities which ensure national security, the following are specified (SCND, 2007):

- appropriate political, economic, diplomatic, social, legal, educational, administrative and military measures;
- the activity of information, counter information and security;
- efficient crisis management (in compliance with the conduct norms of the European and Euro Atlantic community and the provisions of international law).

B. Law no.51/1991 on Romania's national security (PoR, 2014) defines Romania's national security (art. 1) as the condition of lawfulness, balance and social, economic and political stability necessary for the existence and development of the Romanian national state as a sovereign, unitary, independent and indivisible state, the conservation of order, as well as the climate favorable to the exertion of citizens' fundamental rights, freedoms and duties, according to the democratic principles and norms stipulated in the Constitution.

This normative act (PoR, 2014) also mentions (art. 2):

- the measures which ensure national security, namely the awareness, prevention and removal of internal or external threats which may impact the fundamental values specified in the definition of national security;
- the moral duty to contribute to the organization of national security which all Romanian citizens have as an expression of their loyalty to the country.

5. THE RELATIONSHIP BETWEEN CYBERCRIME, CYBERSECURITY AND NATIONAL SECURITY

A. The Explanatory memorandum (GoR, 2014b) to the Draft Law on Romania's cybersecurity stipulate that:

- cyber threat is among the most dynamic threats to national security (as indicated by the recent evolution of cyber-attacks in our country)
- cybercrime prevention is an essential element which contribute to cybersecurity, an essential component of Romania's national security (as specified by the representatives of the Public ministry - Directorate for Investigating Organized Crime and Terrorism and those of the Ministry of Internal Affairs – General Inspectorate of Romanian Police).

The Draft Law on Romania's cybersecurity (CoD, 2014) stipulates [art. 3 paragraph (1)] that cybersecurity:

- is a component of Romania's national security;
- is also conducted through the prevention of cybercrime.

In the same context (CoD, 2014), the draft of the same normative act [art. 3 paragraph (2)], specifies that:

- cybercrime is prevented under the terms of Law no. 161/2003;
- cybercrime is prevented by judicial bodies under the terms of the criminal legislation.

B. The Substantiation Note to Government Decision no. 271/2013 (GoR, 2014a) stipulates that, given the unprecedented development of information technologies and information society, cyberspace has (gradually) developed into an environment for the promotion and strengthening of conventional threats to national security and cyber attacks against national information and communication systems.

C. It has been noted (SCND, 2007: 4) that Romania's Cybersecurity Strategy aims (among others) to achieve information and electronic security.

This strategy has mentioned (SCND, 2007: 12) that information or electronic aggressions:

- are new, asymmetric threats;
- tend to increase in terms of dangers and occurrence likelihood;
- can seriously affect the security of Romanian citizens, the Romanian state or the organizations of which Romania is part.

It has also been mentioned (SCND, 2007: 37-38) that national security includes, structurally, the security of information and communication systems.

It has also been noted (SCND, 2007: 40) that, for individual safety, the security of communities and of the business environment to reach European standards, special endeavors are necessary to fight activities which endanger, among others, the safety of information and telecommunication networks.

6. CONCLUSIONS

The importance of cybersecurity is obvious given the unprecedented development of information technology and the society's increasingly high dependence on technology.

It is also clear that, mentioned in the Draft Law on Romania's cybersecurity [art. 3 paragraph (1)], cybersecurity is a component of Romania's national security and it is also achieved by fighting cybercrime.

In exchange, the meaning granted to such concepts is debatable, just like the manner in which the initiators of the Draft Law on Romania's cybersecurity have understood to approach this issue because, unfortunately, cybersecurity can turn into "cyber espionage" (Manolea, B., 2014).

REFERENCES

[1] Chamber of Deputies (CoD) (2014). *Draft Law on Romania's cybersecurity*, Pl-x no. 263/2014. Retrieved from http://www.cdep.ro/pls/proiecte/docs/2014/cd263_14.pdf.

[2] Directorate for Investigating Organized Crime and Terrorism (DIOCT) (2014). *Activity Report 2013*. Retrieved from http://www.diicot.ro/images/documents/rapoarte_activitate/raport_2013.pdf.

[3] Government of Romania (GoR) (2014a). *The Substantiation Note to Government Decision no. 271/2013*. Retrieved from http://gov.ro/fisiere/subpagini_fisiere/nf-hg-271-2013.pdf.

[4] Government of Romania (GoR) (2014b). *Explanatory memorandum to the Draft Law on Romania's cybersecurity*. Retrieved from http://www.cdep.ro/proiecte/2014/200/60/3/em263.pdf.

[5] Ioniță, G.-I., (2011). *Infracţiunile din sfera criminalităţii informatice: incriminare, investigare, prevenire şi combatere*. Bucharest: Universul Juridic Publishing House.

[6] Legislative Council (LC) (2014). *Advisory opinion on the draft law entitled „Law on Romania's cybersecurity"*. Retrieved from http://www.cdep.ro/proiecte/2014/200/60/3/cl263.pdf.

[7] Manolea B., (2014). *Ce verem: Securitate cibernetică sau securism cibernetic?*. Retrieved from http://legi-internet.ro/blogs/index.php/ce-vrem-securitate-cibernetica-sau-securism.

[8] Ministry of Foreign Affairs (MoFA) (2014), *Romania`s National Cyber Security Strategy*. Retrieved from http://www.mae.ro/node/28367.

[9] Parliament of Romania (PoR) (2014). Law no. 51/1991, republished in the Official Gazette no. 190/18.03.2014.

[10] Sandu, F., Ioniță, G.-I., (2005). *Criminologie teoretică şi aplicată*. Bucharest: Universul Juridic Publishing House.

[11] Supreme Council of National Defence (SCND) (2007), *Romania`s National Security Strategy*. Retrieved from http://www.presidency.ro/static/ordine/SSNR/SSNR.pdf.

[12] Supreme Council of National Defence (SCND) (2013). *Romania`s National Cyber Security Strategy*, Government Decision no. 271/2013, published in the Official Gazette no. 296/23.05.2013.