sciendo International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXVI No 1 2020

VIEWS ON THE MOST IMPORTANT THREATS FROM THE NATIONAL DEFENSE STRATEGY - CORRUPTION, ORGANIZED CRIME TRANSNATIONAL ORGANIZED CRIME TERRORISM (CYBER TERRORISM)

Violeta Ioana NAGÂȚ

"Mihai Viteazul" National Intelligence Academy, Bucharest, Romania
vio_nag@yahoo.com

Abstract: *New threats from cyber bullying, new risks and vulnerabilities, can have serious consequences for national security. For this reason, it is necessary for specialists in preventing and combating terrorism and organized crime to be noticed through ingenuity, predictability and a good knowledge of human psychology. This will ensure the information filter necessary to make the best decisions for the defense of the Romanian state. The Italian intelligence service considers that the terrorist threat is the main security priority and that" Islamic radicalism remains a first-rate threat, despite the significant losses suffered by Daesh (Arabic acronym of the Islamic State - no) " in Iraq and Syria. In addition to terrorism, the Intelligence Services also warn of several other potential threats to the security of the states, including increasing the presence of extreme right-wing groups characterized by racism and intolerance. "These groups have been set up, which have a good implantation especially among the youngest, and the best organized ones do not lack the connections with other organized crime networks. In line with the fight against corruption, it is necessary in the new National Security Strategy to ensure an important place to combat the phenomenon and causes of corruption, corruption being considered a threat to national security.*

Keywords:The National Defense Strategy, Corruption, Organized Crime, Terrorism, New National Security Strategy

Introduction

The National Security Information Doctrine aims to establish and define fundamental concepts specific to the field of information activity for the defense of national security, in accordance with the provisions of the Constitution and with the need to make connections to the organizational and institutional culture of Euro-Atlantic security.

The national doctrine of information for security offers a quasi-exhaustive definition of the concept of "national security": "the state of the nation, of social communities, of citizens and of the state, based on economic prosperity, legality, balance and socio-political stability, expressed by the order of law and ensured by actions of an economic, political, social, legal, military, informational and other nature, for the purpose of the unrestricted exercise of citizens' rights and freedoms, the full manifestation of the freedom of decision and action of the state, its fundamental attributes and of the subject quality of international law".

Thus, national security becomes "the integrating concept of all fields of activity competing in its achievement and defense; the fundamental strategic components of national security are": *national defense, national security and public order*. It is

DOI: 10.2478/kbo-2020-0012

clear that we already have two definitions of the concept of "national security" used by the political and social environment

The biggest problem of the national security legislation of Romania is the so-called "package of laws" which will provide, after the natural follow-up of the legislative process, the necessary framework for the optimal functionality of all structures with attributions in the field and the design of an adequate perception in civil society (so it is about the following draft laws: a) Law on the activity of information, counterintelligence and security, b) Law on the professional and career status of the information officers, c) Law on the organization and functioning of the Romanian Intelligence Service, d) Law on the organization and functioning of the Foreign Intelligence Service).

In Romania, some clarifications are also required on what is meant by "intelligence / intelligence services", more precisely between national intelligence / intelligence services (autonomous administrative authorities, SRI and SIE), security services, (STS, SPP), but also the departmental structures with informative attributions that are subordinated to M.Ap.N (DGIA, comprising DIM and D.Ci.SM) and MAI (DGPI).

Chapter I

***National Strategy for the Defense of the Country for the period 2015 - 2019,* and transnational threats**

The National Strategy for the Defense of the Country for the period 2015 - 2019, is considered the document that reflects the new vision of National Security of Romania, but also the main document that reflects the security policy of the country - *The National Strategy for the Defense of the Country for the period 2015 - 2019* - a higher level document to other documents related to the security policy of the country, such as: the government program, sectoral strategies in the field of national security, but under the conditions that - in the "National Doctrine of information for security" 2 - it shows - which are the fundamental strategic components of national security: national defense, national security and public order.

The strategy was structured on four chapters:

- Defining national security interests and objectives;
- Assessment of the international security environment;
- Threats, Risks and Vulnerabilities (Chapter III);
- Directions of action.

Thus, on a global level, the security environment is undergoing a continuous transformation, which is mainly reflected in the increase of interdependencies and unpredictability in the system of international relations and the difficulty of delimiting risks and threats of the classical type from the asymmetrical and hybrid ones. The strategy also presents the most important threats to the National Security and we stopped on - Corruption, Organized Crime (transnational organized crime - especially the informational form) and Terrorism (cyberterrorism).

***Chapter II Corruption in* the Defense Strategy**

Interestingly, the Defense Strategy speaks very little about the danger posed by corruption. There are unequivocal references, but there is not so much emphasis on the subject. For example, among the "national security interests" we find "defense and strengthening of constitutional democracy and the rule of law", but nothing about corruption as a major threat to state security.

Finally, references to corruption appear only in two places. In the chapter "Risks" regarding the national security, in one of the points it is shown: "The non-fulfillment of the development objectives of Romania can be generated by the persistence of the economic difficulties, the proliferation of the underground economy and the

corruption, the tax evasion, the precariousness of the infrastructure, but also by external factors such as the perpetuation of the development gaps at the level of the European Union and the low degree of resistance to the major turbulences on the external markets, especially on the financial - banking area".

Finally, in the chapter on Vulnerabilities, it is indicated, lastly, Corruption: "corruption weakens the state, generates damage to the economy and affects the potential of developing the country, good governance, decision for the benefit of citizens and communities, as well as trust in the act of justice and in state institutions. Externally, the persistence of corruption has a negative impact on the credibility and image of our country".

Of course, we can say, however, that Corruption is a threat to democracy, to the rule of law, social equity and justice, erodes the principles of efficient administration, undermines the market economy and endangers the stability of state institutions. Therefore, the fight against this phenomenon must be carried out by the legally certified authorities, with the support of civil society, without any obstruction, so that no one is perceived as being above the law. In this context, the prevention of acts and facts of corruption, by monitoring conflicts of interests and incompatibilities, as well as by controlling the assets acquired illegally, must be the support of any strategy in this field. Adopting adequate measures to prevent the phenomenon of "corruption" requires knowing its real size, its complexity, the triggering mechanisms and the consequences produced.

Chapter III Organized transnational crime

Organized crime is a phrase used for the generic definition of the association of persons, organized on the basis of a structural hierarchy, in order to ensure, directly or indirectly, the profit and power in a certain territory or in certain areas of socio-political life, through legal and illegal activities, some committed with violence [1].

Starting from this notion, it reaches one of the serious global threats in evolution, organized transnational crime, which has acquired the capacity to influence the politics of states and the activity of democratic institutions. It is both an expression of the proliferation of negative phenomena that are amplifying under the conditions of globalization, as well as a direct consequence of the inefficient management of the profound political, economic and social changes that have taken place in Central, Eastern and South-Eastern Europe in the disappearance of communist regimes.

By their nature and scope, such activities are favored by the existence of local conflicts and, in their turn, can promote terrorism and the proliferation of weapons of mass destruction, or they may contribute to the perpetuation of separatist regimes. But organized crime can create, in extreme cases, risks and threats to national security and virtual space.

Likewise, the elaborated legislation also considered the areas or activities in which the related harmful effects of the illegal actions of organized crime may appear: the Romanian border, repatriation, movement of persons abroad, customs system, citizenship, extradition of convicted persons, witnesses, trafficking auto, labor market, financial investments, acquisitions, e-commerce, information systems, pharmaceuticals, nuclear activities, etc.

Moreover, some previously drafted laws have been updated, adapted to the criminal situation and the institutional system, harmonized with EU law, such as that of combating money laundering or the one concerning the regime of foreigners in Romania, so that they become more instruments precise, including in the fight against cross-border organized crime.

Appropriate measures have also been taken regarding the legislation on preventing and combating cybercrime. In the National

Defense Strategy, it is emphasized that the cyber threats launched by hostile entities, state ornon-state, on the informational infrastructures of strategic interest of the public institutions and companies, are generated by the IT crime.

Computer crime *is the phenomenon characterized by the most dynamic evolutions, having its part among the most invisible modes of operation, among the most intelligent authors, of the most sophisticated electronic equipment, thus being a difficult phenomenon to control, both based on the exposed trumps, but also against the background of legislative shortcomings, which govern the Internet environment, where the most frequent and spectacular results are developed and carried out* [2].The same phenomenon can become a threat to national security, depending on the size, the aim targeted by the authors and the effects produced, all starting from a powerful computer, an Internet connection and the desire for big profits, by any methods and means. Dissociation from the Internet environment would be to ignore some clues or hints to investigate the phenomenon. Thus, cyber-attacks carried out by cybercrime groups or extremist cyber-attacks launched by hacking groups directly affect national security of national security interest. The main categories of actors that generate threats in the cyber space are also presented in the **Cyber Security Strategy of Romania** [3], which refers in this context to:

- persons or groups of organized crime that exploit the vulnerabilities of the cyber space in order to obtain patrimonial or non-patrimonial advantages;
- terrorists or extremists who use cyber space for conducting and coordinating terrorist attacks, communication activities, propaganda, recruitment and training, fundraising, etc., for terrorist purposes;
- states or non-state actors that initiate or carry out operations in the cyber space, in order to gather information from the governmental, military, economic or other fields in order to materialize threats to national security" [3].
- Cyber threats launched by hostile entities, state or non-state, on information infrastructures of strategic interest of public institutions and companies, cyber-attacks by cybercrime groups or extremist cyber-attacks launched by hacking groups directly affect national security.

Terrorism is a persistent threat, with forms of manifestation difficult to anticipate and counter, including from the perspective of identifying and destroying the recruitment and financing flows of these activities. National contingents participating in external missions are exposed to the risks and threats generated by the actions of terrorist forces, organizations and groups. Growing fundamentalist propaganda, especially in the virtual environment, favors the emergence of new cases of radicalization or involvement in extremist-terrorist actions.

Cyber terrorism is, in theory, the convergence of terrorism in the computer space. It is generally understood as being made up of illegal attacks, information thefts and the use of the internet as a means of mass terror [4].

According to the US Federal Bureau of Investigation, cyberterrorism is "any politically motivated, premeditated attack on information, computers, and networks that could result in violence or any other kind of harm" [5].

One of the first attacks labeled an act of terrorism was the 1999 incident, when a group of hackers attacked NATO computers, using a DoS (Denial of Service) attack, blocking access to them.

Computer terrorism is an attractive alternative for modern criminals for several reasons:

- it is much cheaper than traditional terrorist methods, all a person needs are a computer and an internet connection.
- secondly, it is a more anonymous way of achieving its goals. Like many Internet surfers, they can use nicknames or log in

to a site as a 'guest', making it harder for government agencies to identify them.

- third, the variety of targets is huge. A computer terrorist can attack the networks and computers of governments, individuals, utilities or even private airlines. The huge number of potential targets ensures the attacker a much higher chance of success than in the case of more direct measures.
- the fourth reason is that cyberterrorism can be carried out remotely. A very attractive facility for terrorists. The IT environment implies a much lower risk, less training and travel.
- fifth, as the ILOVEYOU virus first showed, cyberterrorism has a very high potential to affect more people at the same time, generating a much larger audience, which is ultimately what they want.

Chapter IV Basic document for national security- National Defense Strategy.

In order to face foreseeable challenges or not, it is necessary to adapt to the designated missions, the cooperation between the different defense and security structures in order to achieve common goals, the capacity to deal with major crises, the restructuring of the support and administrative structures. as well as emphasizing the importance of operational missions.

In order to assure national security, the basic document is the National Defense Strategy. This is the working tool through which, starting from the need to defend the country, national security interests, values and objectives, it manages risks, threats and vulnerabilities.

Thus, organized crime becomes a threat, when:

- penetrates the main governing bodies of the state and extends its influence on the political life, on the economic sector, especially the financial-banking, commercial, industrial sector, but not least on the media, which it tries to control and use it in formation of distorted images in connection with their illicit activities;
- the degree of professionalization of criminal media and structures is consolidated, and individuals with such concerns occupy official positions in the field of trade, justice, administration, communications, logistics, financial banking etc.;
- the merger with the political world is carried out, important funds resulting from corruption and mafia-type business (drug trafficking, high-smuggling acts, tax evasion, blackmail, collection of the protection tax) being injected into organizations and political and administrative structures so that they can be keep in power and be able to guarantee the groups of criminals the success and the multitude of dirty businesses that they initiate;
- the direct dispute between the criminal groups for acquiring or maintaining the supremacy in certain areas such as: drug trafficking, weapons, human trafficking, bootlegging, cigarettes, works of art as well as the dispute for areas of influence is intensifying;
- the forms and procedures used to launder dirty money multiply.

The case law reveals that the activity of interest groups (including those of pressure and lobby) is insufficiently regulated in Romanian law, the only references being made in the new Criminal Code regarding organized criminal groups.

Conclusions

In line with the fight against corruption, a new National Security Strategy is needed, in which to ensure an important place to fight the phenomenon and the causes of corruption, the great corruption being considered a threat to the national security [4].

In conclusion: corruption affects democracy and the rule of law [5], as:

- it induces a high level of risk, which generates multiple vulnerabilities for the state;

- allows organized crime networks, terrorist groups and other vectors threatening to attack and not to strengthen the security of the individual;

Of course, the new threats from cyberbullying, new risks and vulnerabilities, can have serious consequences for national security. For this reason, it is necessary that the specialists in the prevention and combating of terrorism and organized crime should be noted for their ingenuity, predictability and good knowledge of human psychology. This will ensure the information filter necessary to make the best decisions for the defense of the Romanian State.

Moreover, the Intelligence services consider that the terrorist threat is a security priority and that "Islamic radicalism remains a first-rate threat, despite the significant losses suffered by Daesh (Arabic acronym for Islamic State - no)" in Iraq and Syria.

In addition to terrorism, the Intelligence Services also warn of several other potential threats to the security of the states, including increasing the presence of extreme far right groups characterized by racism and intolerance. "These groups have been set up, which have a good implantation especially among the youngest", and the best organized ones do not lack the connections with other organized crime networks.

Of course, under the current conditions another threat causes thousands of dead in the world is the pandemic.

Thus, until March 26, 2020*, the COVID-19 pandemic caused the death of over 15,000people in Europe*[6].

In total, 15,500 deaths were reported in Europe due to SARS-CoV-2 infection, most of them in Italy (8,165), Spain (4,089) and France (1,331), the European countries most affectedby the pandemic. With 268,191 officially declared contamination cases, Europe is the continent where the COVID-19 pandemic is progressing fastest. The first case of infection with the new coronavirus was reported in Hubei province, central China, at the end of December 2019 [7].

We consider that the current concerns of the states in order to ensure national security by organizing more efficiently the national intelligence, can be effectively implemented by developing and implementing security strategies that include intelligence. In this sense, Romania should also follow in the direction of these guidelines the sense in which it should return to the elaboration of a new security strategy for the next stage 2020-2025, in which some threats of asymmetrical type such as threats as pandemics or various biological weapons deliberately or not out of control can be counteracted by effective strategies.

References

[1] Alina Lefter, *Organized crime. Doctrinal approachesandinternational legal instruments,*https://www.juridice.ro/504857/criminalitatea-organizata-abordari-doctrinare-si-instrumente-juridice-internationale.html, accessed on 10.03.2020.

[2] *Computer crime reachesthenationalsecurity,*http://intelligence.sri.ro/criminalitatea-informatica-atinge-securitatea-nationala/, accessed on 10.03.2020.

[3] Bythe CSAT Decisionno. 16/2013 and GD no. 271/2013 wasapprovedtheCyberSecurityStrategy of Romania, whichestablishesthe conceptual, organizationalandactionframeworknecessarytoensurecybersecurityandwhichaimstoprotectcyberinfrastructures in accordancewiththenewconceptsandpolicies in thefield of cyberdefenseelaboratedandadaptedto NATO leveland of the European Union - https://www.mae.ro/node/28367, accessed on 10.03.2020.

[4] Cătălin Stoian, *Terrorismin CyberneticSpace. FormsandPossibilitiesof ContractingCyberTerroristActions,*Infosfera Magazine, no. 1/2009 https://www.mapn.ro/publicatii_militare/arhiva_infosfera/document/2009/1_2009.pdf, accessed on 10.03.2020.

[5] Ileana Ștefan, *Prevention Of Informatic Terrorism*,http://oeconomica.upm.ro/O_X/180%20-%20193%20PREVENIREA%20TERORISMULUI%20INFORMATIC.%20Ileana%20STEFAN.pdf, accessed on 10.03.2020.

[6] NOTE: According to the Constitution, the President of Romania represents the Romanian state and is the guarantor of national independence, unity and territorial integrity of the country; monitors compliance with the Constitution and the proper functioning of public authorities.

[7] *Corruption and its fight. Towards a model of building our integrity*, World Bank, *Irecson Institute*, Bucharest, 2003, p. 14.

[8] *Accordingto a report by France Presse based on officialsources, Thursday at 17:00 GMT.*https://www.agerpres.ro/mondorama/2020/03/26/coronavirus-numarul-deceselor-din-europa-a-depasit-15-000--475132.

[9] AGERPRES/AS, Tudor Martalogu, editor: Mariana Ionescu, online editor: Irina Giurgiu), https://www.agerpres.ro/mondorama/2020/03/26/coronavirus-numarul-deceselor-din-europa-a-depasit-15-000--475132.