The 15th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 12th-13th 2020

THE ANALYSIS OF THE VULNERABILITIES FOR THE SECURITY

ZBRANCA Alexandra

MA student atRegional Department of Defense Resources Management Studies – NATO Partnership Training and Education Centre, Brasov, Romania

Abstract:
Some of the current security risks differ fundamentally from those at the end of the last century. Of course, some risks have the capacity to transcend history (war, epidemic risks, etc.), but they also change their relevance with the evolution of society. Action by the international community is constantly adapting to new realities. The challenges are not only about military conflicts between states, but are much more complex in nature. One of the causes of the change in the paradigm of risks is the emergence of non-state actors alongside state actors. When viewed systemically, the concepts under analysis are always in a well-defined report. During their coexistence, when security forecasts do not see the elimination of one too soon, risks, threats and vulnerabilities can operate in accordance with the principles of zero-sum gaming. Thus, national security can be ensured either by reducing vulnerabilities or by preventing threats or mitigating risks. It determines the orientation of the national security strategy that can focus inward, trying to reduce the state's vulnerabilities, or outward, by allocating forces and means to act directly or not on the sources of risk.
Key words: risk, threat; vulnerability; global security; regional security; national security.

1.Introduction

The risk is the probability of an event of uncertainty, with direct or indirect impact on national security. It represents the possibility of to face a potential danger. The risk is caused by the non-determination, by the inability to know the future events with certainty, representing an potential state, which under certain conditions may become effective. In a broad sense, the risk it is in the discrepancy between the positive wait and the negative event that is taking place it can also occur by its likelihood of it occurring. Vulnerability can be broadly defined as the result of the combination of risks to the public company and its ability to cope with and survive situations of emergency, internal and/or external. Vulnerabilities are the consequence of systemic failures or deficiencies,
that can be exploited or contribute to the materialization of a threat or a risk.[1] Threats are capabilities, strategies, intentions, or plans that can affect national security values, interests and objectives.

Security is about ensuring the independence and territorial integrity of the state, and is not only a new concept, but also discussing its definition. Experts in the field have reached a consensus that the term is protected from danger, a sense of trust
and peace that the absence of danger gives. Collective security is a state of relations between States, created by the adoption of joint measures to defend against aggression.[2]

2.The concept of security

Security has always been one of the deepest aspirations of humanity, a constant concern and the essential of human civilization, and security issues were counted it is among the most important and, at the same time, the oldest problems that it is in the world.

States have always tried to insure themselves security by possession of weapons, by military capabilities they developed to address threats their security. Here too, we must recognize that, in some cases, some States they survived mostly because they could count on the means defense. [3]

Security shows the feeling of trust and peace on which gives anyone the absence of danger, vulnerability. In other words, for the security environment to be real and effective, it should ideally be free from risks and threats or ensured by the state's capacity to remove them, or at least, keeping them under control.

Security is designed as a process multilateral political, the content of which includes cooperation between states to prevent the danger of war and to maintain it peace throughout the world. The interests of international security is to call for the exclusion of the possibility of new developments and unleashes armed conflicts, outbreaks of tension or any wars, [4] and for the settlement of international disputes requires the use of exclusively means political accepted by international law. It is therefore obvious that the fight of countries and forces is at the heart of security for peace throughout the earth, and peaceful coexistence, like the principle of international political relations, it has no alternative.

3. The concept of vulnerability

Vulnerabilities are conditions of things, processes or phenomena in internal life that reduce the ability to respond to, or encourage, existing or potential risks. The vulnerability analysis takes into account risk factors of all types, both within and outside the physical limits of the system, but also their internal and external consequences. Moreover, although it is covered for a long period of time, the vulnerability analysis focuses on a specific sequence of events from the moment the emergency situation occurs until a new state of stability is achieved. Hazards, risks and vulnerabilities can be analyzed, as in the case of threats, depending on the nature of the sources or the area in which they occur, resulting in more than one category: political, social, economic, military, cultural and environmental.

The vulnerability analysis takes into account risk factors of all types, both within and outside the physical limits of the system, but also their internal and external consequences. Moreover, although it is covered for a long period of time, the vulnerability analysis focuses on a specific sequence of events from the moment the emergency situation occurs until a new state of stability is achieved. Both hazards and risks and vulnerabilities can be analyzed, as with threats, according to the nature of the sources or the area in which they occur, resulting in several categories, of which, in this study, we will focus on political, social, economic, military, cultural and environmental.

Vulnerability manifests itself in the form of a system or state that allows the attacker:

- to carry out actions that have a psychological impact on the population;
- to access classified information and endanger state security;
- to attack critical points of the proper functioning of the state;
- to attack people in various ways and create chaos.

Vulnerabilities are all ways, means and ways that are omitted or threats are and affect the system.[5]

4. Cyber infrastructure vulnerabilities

Vulnerability is a weakness of a hardware or software system that allows unauthorized users to gain access to it. The main vulnerabilities in information systems are physical, hardware, software or human. Information systems are particularly vulnerable to traditional attacks when an attacker is physically able to enter the computer system enclosure and to steal confidential information. To prevent this, physical security of computer equipment must be ensured by placing it in safe areas

restricted to unauthorized personnel. Access to these areas must be made using access cards or biometric data scanning devices for authentication of users with an entry permit.

Another vulnerability of information systems is natural disasters (earthquakes, floods, fires) or accidents such as voltage drops or over voltages that can lead to physical destruction of computer equipment. The location of equipment to reduce the risk from environmental threats must therefore also be considered. [6] Particular attention should be paid to hardware components so that they do not subsequently impair the proper functioning of the information systems. For servers that provide Internet services, failure tolerance hardware must be chosen to provide the availability of network-shared services and data and to reduce the risk of hardware vulnerabilities.

These vulnerabilities are most common to data storage systems, being the most sensitive hardware. From this point of view, it is recommended that security be saved both at the information level and at the operating system level to quickly restore the information and configured services in case of failure.

There are several types of vulnerabilities from a software point of view: - that increase local user privileges without authorization; - that allow external users to access the system unauthorized; - that allow the system to be involved in an attack on a third party user, for example Distributed Denial of Service (DDoS) attack. a classification can be made according to the degree of danger posed by the vulnerabilities to the computer system under attack.

The causes of vulnerabilities in a computer system are multiple, some of them are: - operating system or application errors; - improper operating system or application configuration; - limited knowledge of system or network administrators; - lack of software developers' support in resolving errors found in software applications. Last but not least, the greatest vulnerabilities are human, given by the personnel involved in the configuration and management of the information systems. By lack of experience or inadequate documentation of specific operating system or installed applications, cyber security can be totally compromised. A particular type of vulnerability is zero-day vulnerabilities, unknown to developers and software providers and can be exploited by cyber criminals. Any computer system has vulnerabilities, so we can say that there is no 100% secure system. These vulnerabilities are used by many types of attacks targeting a computer system directly, such as malware attacks, or indirectly, if the computer system is involved in a DDoS attack.

5. Risks and threats to national security

The greatest vulnerability in terms of national security is the phenomenon of generalized corruption that creates what experts call a "state captive", i.e. a state without strong institutions, unable to ensure good governance, with an uncertain economic climate and a strong black economy developed. These system malfunctions allow easy infiltration of some entities hostile to national interest in the area of Romania's strategic decision. Lack of good governments followed by a drop in living standards are aspects that can lead to citizens' social frustrations, which, as a result of widespread deception and dissatisfaction, become sensitive to psychological war and become no longer respected the values of the state, feeling out of them, becoming vulnerable in face of propaganda and foreign interests. At Romanian level, such vulnerabilities specific to psychological war are encountered either in actions related to weakening national consciousness such as removing or reducing some materials from the system education such as latin, religion or history of Romanians, or in actions that are they aim to destroy national symbols. Lack of strategic continuity in the education sector has weakened not only the perception of the Romanian school, but also that related to its ability to train young people ready for entering the labor market. This vulnerability leads in a way indirectly toward slow socio-economic development. [7]

A new type of threat to Romania's security is represented by to actions or inactions that harm the strategic economic interests of The effect of the threat, illegal management, degradation or destruction of natural resources, forest, fish and fish funds, waters and other such resources, as well as monopolization or blocking of access to them, with consequences at national or regional level. Romania is not excluded from the map of States susceptible to attacks cyber, a risk also enhanced by the membership status of international organizations, but the risks associated with cyber aggressors are still at a level environment. Cyber security has become a national security issue because Romanian cyberspace has been found to be in the target of aggressors cybernetics. In early 2013, Romania faced two attacks large-scale cyber-related information, in particular, to access information confidential by accessing government sites and certain entities private with influence in the national economy. The degree of complexity of attacks he average of the technical knowledge of which is continuously growing it benefits the large mass of cyber-aggressors. That is the case it is explained by the fact that cyber attackers with exceptional technical skills develop tools that a novice uses later with a single click, without being a good technician and the effects that have been produced can be disastrous. Moreover, that's all government institutions, as well as business and home user records a massive flow of confidential data that is not always protected adequate. In most cases, the human factor is the weakest link in the security process, due to the lack of cyber security culture or of insufficient information on the need and ways to protect your own information systems. [8]

Outside factors of risk, security may also be affected by vulnerabilities internal forms that can take different forms. The main vulnerabilities can be: Insufficient resources allocated to security and defense institutions; deepening social inequalities; the proliferation of the shadow economy and the increase in corruption; economic crime; disruption of public order; possibility of some environmental disasters, natural disasters; keeping information infrastructure low; emigration of specialists from different top-of-the-range fields ("brainstorming"). All this has an impact on the development potential of Romanian society. [9]

6. Conclusion

Some of the current security risks differ fundamentally from those at the end of the last century. Of course, some risks have the capacity to transcend history (war, epidemic risks, etc.), but they also change their relevance with the evolution of society. The challenges are not only about military conflicts between States, but are much more complex in nature. One of the causes of the paradigm shift in vulnerabilities is the emergence of non-state actors alongside state actors. Against the background of these changes, we see the emergence of a new concept in the literature and in the various security strategies: The asymmetric risk. Asymmetric risks are identified under various references in most security strategies. In dealing with asymmetric risks, we consider the preventive, forward-looking dimension of security strategies to be important, compared to the active dimension, which aims at managing consequences. This has multiple benefits: Resources are less needed than if they were used to clear the consequences, anticipation is designed to prevent loss of life and material goods, and the direct consequence is stability of the security system and other systems.

References:

[1] Administraţia Prezidenţială, *Strategia Naţională de Apărare a Ţării pentru perioada 2015-2019.*
[2] Ionel Nicu Sava, *Security Studies*, București, Center for Regional Studies Publishing House, 200), 56.
[3] Richicinschi I. *Terorismul – pericolul destabilizării securităţii internaţionale.* Chişinău: Ed. C.E.P. U.S.M., 2005, p.6.

[4] Balaban C. *Securitatea şi dreptul internaţional – provocări la început de secol XXI*. Bucureşti: Ed. C. H. Beck S.R.L., 2006.
[5] Ion Gheorghe, *Military security of Romania in the age of globalization*, Bucharest, "Carol I" National Defense University Publishing House, 2006, 120-124.
[6] I.C. Mihai, G. Petrică, C. Ciuchi, L. Giurea, *Provocări şi strategii de securitate cibernetică*, Sitech, 2015
[7] Munteanu Răzvan, *Vulnerabilităţi şi riscuri la adresa securităţii naţionale a României specifice războiului hibrid*, disponibilă pe https://adevarul.ro/international/foreign-policy/vulnerabilitatisi-riscuri--adresa-securitatii-nationale-romanieispecifice-razboiului-hibrid-1_56eaa5ec5ab6550cb8f12d98/index.html.
[8] Ververa Adrian Victor, *Ameninţări cibernetice globale şi naţionale, în Revista Română de Informatică şi Automatică*, vol. 24, nr. 3, 2014, https://rria.ici.ro/wp-content/uploads/-2014/09/04-art-2-A-V-Vevera-Amenintari-cibernetice-globale-si-nationale.pdf
[9] Bădălan Eugen, *România în noul mediu de securitate după Summit-ul de la Instabul, în Moştoflei, Constantin (coord.), Surse de instabilitate la nivel global şi regional. Implicaţii pentru România*, UNAp „Carol I", Bucureşti, 2004, p. 14, https://adlunap.ro/uvl/lib/read.- php?id=43.