CRITICAL INFRASTRUCTURE PROTECTION IN THE CONTEXT OF THE SECURITY NETWORKS

Daniel ROMAN

Abstract: Security is one of the reference elements of an entity, regardless of its nature and of how it is reported at the micro- or macro-dimensional level. Due to the complexity of the reference environment against which the state of security is defined in a contemporary context, this poses a major challenge to specialists in all areas: political, military, social, economic, information, infrastructure and environment. Therefore, identifying those viable solutions for preventing, counteracting or eliminating the effects of a crisis, depending on its nature, may only be possible by understanding the "operating mechanisms" of each area. Following the dynamics and describing the interaction relationships of the responsible social systems can be one of the methods of managing a potential complex crisis that may occur at a given time. In this article, we have intended to argumentatively support the need for an integrated approach to the security of the identified "pillar systems" by focusing on critical infrastructure protection and designing, planning and deploying military actions. For the first time, based on integrating the dynamics of the risks and the vulnerabilities of the social systems, we have argumentatively developed the concept of network interaction. By monitoring and analyzing the essential descriptive parameters of each security field, we can decipher their security states due to the identified network connections, and moreover, we can anticipate a potential crisis or the possible occurrence of a major negative event.

Keywords: security; critical infrastructures; military action; crisis; vulnerabilities; collaborative workflow; negative event.

1 THE COMPLEXITY OF THE INTEGRATED SECURITY ENVIRONMENT

The notion of security, in most definitions, essentially covers that state that expresses the existence or the performance of the activities of an entity in order to fulfill its established role or objectives without a direct or indirect influence factor of any kind being capable to affect or hinder it. Depending on the nature of the domain we make reference to, the state of security is described in detail and is reflected in the absence of danger. Understanding the terms that refer to the state of security is paramount in all attempts to express, define, or describe the position of an entity related on a micro- or macro-dimensional level. Knowing the parameters that describe the dynamics of the evolution of an entity, an analysis of the entity's state can be made, as well as a formulation of those solutions required for maintaining the systemic balance. The problem arises when, due to being ignorant of the transformations of the existence of the subject entity, extreme values of the descriptive parameters are generated or new connections appear influencing other entities in the same or in different domains. In this sense, we can consider that decoding the reality with respect to a certain entity is the starting point in constructing the influence connections between one or more entities based on certain types of functional networks created due to mutual influences.

Regarding the introduction of the concept of a "network of influences", the state of security of an entity exceeds the area of its own descriptive parameters and transits in another area of interaction with other identified or unidentifiable entities. Because of this, it is noticeable that new network connections are born and there are a number of role changes of the elements becoming network nodes. In other words, even if mathematically argued relationships between different entities are developed, the concept of integration into a particular network or into multiple networks shows that the nature of the relationships between the entities and the context of mutual influences is not a simple well designed puzzle or just one way of assembling it, but rather a very complex system in which the components fit in so many configurations, almost impossible to define [1]. By launching the hypothesis by which any socio-technical system is capable of developing its own personality and implicitly of adapting to its own environment, it results that at the level of the network it is possible to have functioning laws based on self-organization.

Through the intuitive application of the concept of network and the transposition of the components of a socio-technical system, such as a political, military, social, economic, informational or environmental one, a series of infrastructures with different roles and distinct geometry is constructed.

Due to the relationships established between the network elements of the socio-technical systems and due to their role in society, the infrastructures were classified according to their role in: ordinary infrastructure, special infrastructures and critical infrastructures [2]. From the point of view of network geometry, infrastructures are born and grow differently, depending on the degree of association and belonging to that network of all its constituent elements. Figure 1 shows that the newly connected elements (the white rings) join the network by establishing connections with the most connected network elements (the black rings). Depending on the role they perform, each network element modifies the geometry of the network according to the connections made, and extends it to the area of greatest interest or importance. Translating each element into its own network and according to the connections it has to other elements from other

networks involves making new connections between two or more networks. Thus, connections are made between two or more networks/domains of interest and there are a number of advantages and drawbacks which will be addressed later on.

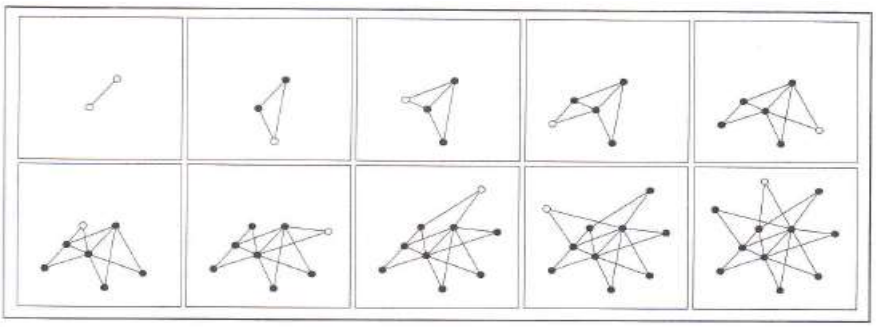

Fig. 1 Variants of design and self-organization of networks
Source: Albert Laszlo Barabasi.

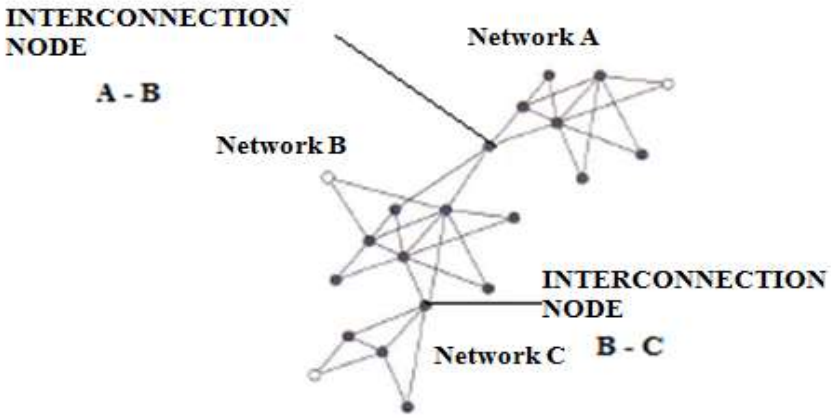

Fig. 2 Variants of connections between two or more networks/areas of interest
Source: Directive 114/2008, 345/77.

The more the network connection element is "more connected" to its own network, the stronger the connection between networks is. This way of explaining the connections between infrastructures or areas of interest can be helpful in understanding the "mechanism" of occurrence of a crisis or a major negative event at a given time. Identifying solutions to surmount a potential crisis or to help the entity concerned survive the major impact negative event involves "locating the entity in the network of influences." The network of influences is given by the nature of the connections between the entities that interact directly or indirectly. We will refer to two areas, namely the critical infrastructure protection and the area of military action. As defined in EU Directive 114/2008, a critical infrastructure is "an element, a system or a component thereof located within the territory of the Member States that is essential for the maintenance of vital societal functions, health, safety, security, social or economic well-being of persons and whose disruption or destruction would have a significant impact on a Member State as a result of the inability to maintain those functions". The military component is the essential factor of a nation or an alliance that guarantees security against the military action of a potential aggressor [3]. Due to the destructive power resulting from the military action (material damage and loss of life), it is necessary to reposition the critical infrastructure protection at the conceptual level. This implies achieving an integrated vision of the two areas of interest: the military and the critical infrastructures. This integrated approach, as previously formulated, relocates the security components and defines the multitude of connections between the network nodes and their importance, an aspect which will be highlighted in the case study on the cyber attacks in the capital of Estonia, Tallinn.

2 CRITICAL INFRASTRUCTURES IN MILITARY ACTIONS, EFFECTS AND CONSEQUENCES

The complex situation in the spring of 2007 in the capital of Estonia, Tallinn, can be considered as one of the major reference to which the security environment needs to be redefined. Although at that time the cyber attacks could not be considered hostile military action, their effects and especially their consequences have shown that the security environment can no longer be described as the property of only one security entity. The coincidence of the cyber attacks with the deterioration of the Russian-Estonian political-diplomatic relations amid ethnic-social dissatisfaction regarding the transfer of certain symbols of high significance to the Russian minority in the Estonian national territory is the starting point of a potential crisis of a certain extent. By this extent we mean the degree to which the problem of cyber attacks escalates.

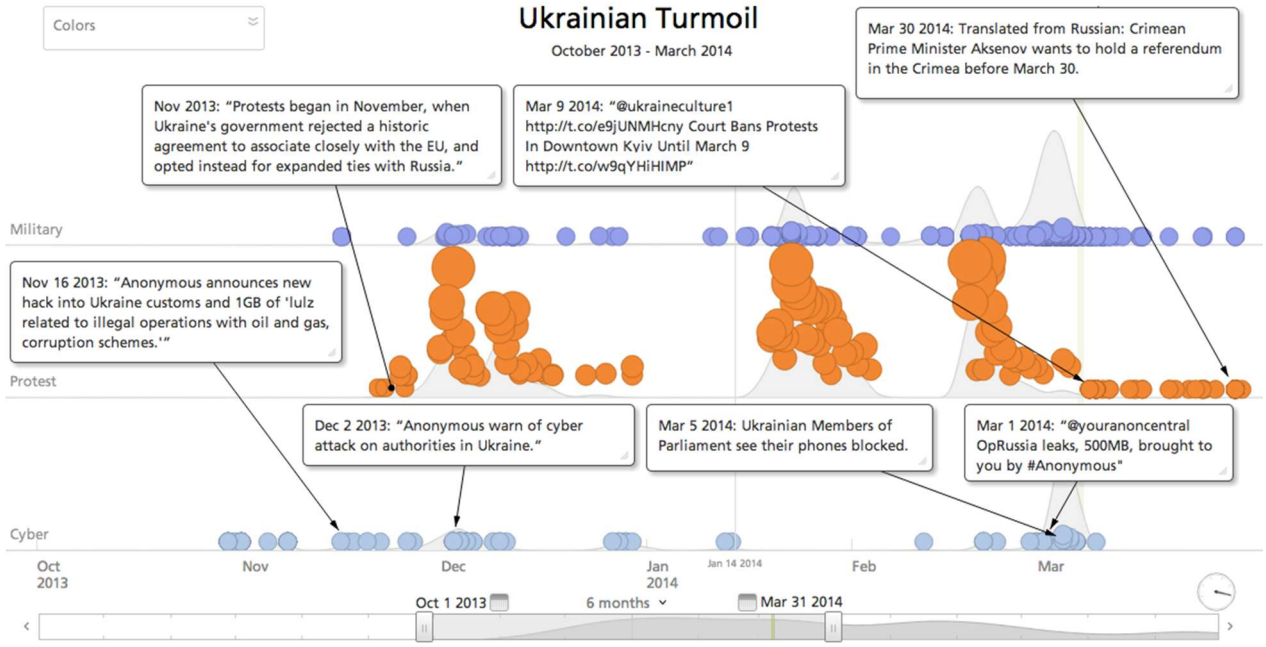

Fig. 3 Chronologic representation of complex incidents that precede a cyber attack
Source: [4].

Paralyzing the Estonian state institutions and causing important damage to critical infrastructure components due to cyber attacks in NATO's vision was "an operational security issue" handled as seriously as possible. In hypothetical terms, if the effects of the cyber attacks were to seriously affect the existence and the functionality of the attacked Estonian critical infrastructures, by the degree of their damage, namely material damage and/or loss of human lives, the state of necessity would have been for sure declared, the combat capacity would have gradually increased and the military structures would have engaged the aggressor. Without tackling technical details, the cyber attacks on the institutions in Tallinn in 2007, due to the lack of NATO and EU legal bases, could not have been regarded as clear military action. However, the involvement of the security factors: political, economic, military, social, information and infrastructure, clearly shows the nature of their relationships and their behavior in managing the incident through a certain shape and geometry specific to a security network or multiple networks.

The concept of network action of the security factors for managing an event with a negative impact on one or more states can be the key to anticipating the occurrence of attacks of a specific nature aimed at destabilizing the state of security. The combination of the two components: the critical infrastructure protection and the defense specific for the military field, in our view, must be intersected and positioned "operationally convergent". One of the strongest arguments is given by the number of victims and the volume of material damage that can be attributed to attacking a critical infrastructure and by the conduct of military operations or exercises that could get out of control. The explosion of an atomic-power plant due to its failure to operate under nominal technical parameters due to cyber attacks or terrorist actions may have consequences similar to military attacks such as the explosion of a nuclear rocket. Hence, defining hybrid war remains one of the most difficult

tasks assigned to military experts. In April 2016 another nuclear power plant from Germany was the target of ingenious cyber attacks that could have had catastrophic consequences. The computer viruses "W32.Ramnit" and "Conficker" were identified in the Gundremmingen B unit in Germany, aiming to corrupt the computer data of the equipment responsible for handling the nuclear fuel bundles [5]. The mode of action of a computer aggressor in this case is described as a remote action on a computer system when it is connected to the Internet. The consequences of such an attack, apart from major material damage and loss of human lives following a nuclear explosion occurring at the atomic power plant can be anticipated and described on the basis of the relationships established according to the model of a coherent network of security factors.

Under another determination report, a state's critical infrastructure may be damaged by the outburst of a military conflict. The supply of drinking water for the population or the supply of water needed for industrial or agricultural activities can be seriously affected by military operations, as was the case in the military conflict in Ukraine. Air transport, viewed as part of a designated critical infrastructure in a state, may be affected as a result of military conflicts. We mention the destruction of a civilian aircraft in Flight MH-17 of Malaysia Airline by the military missile type SA-11 in the aviation catastrophe in the Donetsk region on July 17, 2014 resulted in the death of 298 people [6]. A first observation is on the degree of involvement of the institutions responsible for the security, which determines a certain geometry of the network of influences. In other words, overlapping the effects of the actions or inactions of the security factors, regardless of how the network connections are made, assigns different values to network nodes depending on the context of the affected domain. The implications of the Russian Federation's military action near NATO borders concluded on November 24, 2015 with engaging a military aircraft Suhoi Su-24 in Turkey's airspace [7]. Although it did not result in huge material damage or significant loss of human lives, the consequences of such an incident had a major impact on the political and military security pillars, with direct and indirect influences on the economic and energy fields.

Another aspect, particularly important for the typology of the network of security factors influences is the military conflict in Syria. In this case, the situation becomes even more complex due to the number of actors involved in the conflict, as well as the particularly serious consequences on all areas: political, military, economic, social, information, infrastructure and environmental. Assigning a theater of military operations includes all aspects related to the infrastructure of the operation area. The critical infrastructures of the theater of military operations are one of the fundamental elements of conducting combat. The geographic region of a military conflict, defined at political level, may be delimited to execute or support military operations in one or more areas of joint operations. Due to the important geographic extent, the military operations (the situation in Syria) can take place in several combat environments, which can lead to successive and different threats both within and outside the conflict territory [8]. One of the major dangers of a military conflict like the one in Syria, beyond the possibility of the military conflict expanding beyond the geographical boundaries, is to create imbalances at the wider level of the conflict area. The phenomenon of the population migrating outside the military conflict area may affect the parameters of the designated critical infrastructures in the territory of the countries affected by migration, or may generate social incidents of an ethnic or religious nature, as well as imbalances at State or Union level in some states. In other words, a military conflict can directly or indirectly generate effects of an economic, social, political or other nature, both on the territory of the state undergoing a conflict and on the territory of other states, irrespective of the distance to the epicenter of the war. The consequences, based on causes and effects, in a specific area of military operations, depending on their nature and subject matter, may be extended. Following the integration of the concept of network of influences on the designated critical infrastructures such as terrorist attacks inside states not involved in military conflicts but politically supporting these conflicts is one of the key arguments for an integrated approach to critical infrastructure protection concerning the conduct or the support of military action.

3 NEW HORIZONS ON THE CRITICAL INFRASTRUCTURE PROTECTION IN MILITARY ACTION

The reality of contemporary society, characterized by a profound complexity of problems in all security areas, combined with access to state-of-the-art technologies, is one of the challenges defense specialists have to face. Cyber attacks have become increasingly sophisticated in terms of technology, which calls for resorting to specific measures but also for establishing specialized rapid reaction structures for the emergency situations in the cyberspace. For preventive purposes, NATO and EU institutions have moved on to adopt those technical measures and to create those specialized structures capable of building and maintaining the state of security and intervention in the event of a crisis or occurrence of an event having a major negative impact.

In this respect, specific to critical infrastructure protection, according to EU Directive 114/2008, a security mechanism has been set up, which, through the operator security liaison officer, implements the critical infrastructure operator's security plan [9]. Following the above mentioned examples, we can admit that a certain degree of amplification of

vulnerabilities of the designated critical infrastructures is directly proportional to the level of connection of the subject within the network of influences. We have overlooked the fact that the vulnerabilities of an atomic power plant or a military operator exponentially increase with the level of their or their systems' connectivity in cyberspace. In other words, the network of influences is not just a conceptual network; it can be physically not just conceptually identified at a given moment in cyberspace. Another aspect is the operational technical knowledge of the "security pillar" domains that cannot be limited to just a certain segment of infrastructures. The level of connectivity can generate cascading effects, and a seemingly insignificant cyber attack on a particular structure can lead to major catastrophic effects for the other connected or unconnected infrastructures.

One of the current security trends regarding those infrastructures considered critical is the technical isolation of the main responsible systems in the cyber space for commanding and controlling vital systems of the critical infrastructures and eliminating all external connection possibilities. The installation of antivirus software and the physical protection against unauthorized access to electronic systems is still one of the most common security measures. The scenarios of the security incidents demonstrate that a number of innovative cyber attacks and a certain technological complexity can still be generated. Therefore, the competent security forces have initiated specific legislative procedures on working in the cyberspace. In order to cope with the increased evolution of cyberspace threats, the US has adopted the concept of Active Cyber Defense (ACD) in cyber defense strategy. Active cyber defense has already become a very controversial topic. The controversial aspect is given by the Responsive Cyber Defense (RCD), defined as "cybernetic infrastructure protection against an ongoing cyber attack through measures directed against the cybernetic infrastructure from which the attack originated or against an infrastructure as a third party thereof" [10]. Apparently similar, the two concepts are totally different in terms of area and specific mode of action. RCD addresses a cyber attack in progress and does not involve preemptive or retaliatory actions. While defining a policy in the narrow sense of the RCD, this implies the application of offensive, punctual cyber-measures in clearly defined situations [11].

Regarding "the position" of defending against or countering the threat such as a cyber attack or a terrorist attack, at least two strategies can be distinguished: the reactive and the proactive strategies. In line with the position of the subject in question(reactive or proactive) in a possible network of influences, he will manifest different behavior to the external factors (of aggression). Depending on the ability of the subject to adapt to the environment, it is assumed that he will be able to cope with any unforeseen hazard. Due to the implementation of the concept of network and the assimilation of the states of security specific to critical infrastructures in military operations, we notice the existence of more than just one security level. The systemic approach, to which we have referred, connects the elements of several distinct domains. The degree of connectivity of the elements and the nature of the connections between them form the direction of threat manifestation

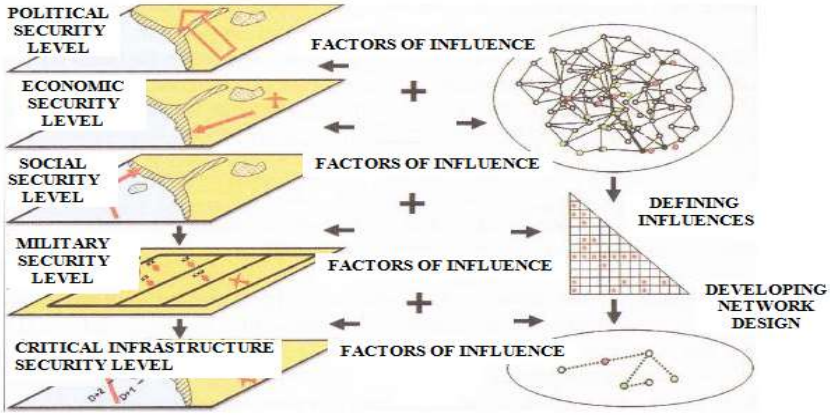

Fig. 4 Representation of the security levels and the network geometry according to influences
Source: [4].

The conceptual creation of networks based on the influences between the nodes connected to a particular connection scheme may outline a particular state of crisis and, implicitly, the possibility of a proactive attitude of counteracting the crisis, regardless of its nature. From an international perspective, two or more states interconnected at one or more "security pillars" can be affected by the same crisis differently, depending on the "geometry of the network of mutual influences." The same can be said

in the case of a negative event with a major impact on the critical infrastructure on the territory of a state having direct or indirect causes, as a result of incidents occurred on the territory of the neighboring state or of another state. The military conflict in Syria has produced or is about to cause serious damage to critical infrastructures across the territory of other states in multiple ways: from social, economic, infrastructure, cultural, etc. point of view, both in the short term and especially in the medium and long term, with particularly difficult, unavoidable consequences.

4 INSTEAD OF CONCLUSION

Decoding the reality of how a crisis develops or how a negative event with a major impact on a state or several states occurs is the fundamental aim of researches into the concept of a "network of security pillars". Understanding thoroughly how the security systems or the critical infrastructures on the territory of a state or states work helps us identify their vulnerabilities. The vulnerabilities of each system in the concept of a "network of influences," as we have argued in the contents of this article, can be interpreted as a "crack in an amorphous body" where the body can be that "system of systems." Therefore, the vulnerabilities of a subsystem may represent in different percentages depending on the situation or the degree of connection of this system with the other systems, different threats on the macro system that all the networked subsystems create.

Another observation resulting from the systemic interpretation of the network of influence focuses on the performance of the critical infrastructure managers and on their ability to conduct a collaborative workflow. The specific manner of working towards mitigating or removing the vulnerabilities of a security system cannot guarantee the security of the entire security macro-system, be it at the level of a single state or the level of several states. For this, we suggest a possible working solution for the responsibility factors, in the sense of mutual awareness or sharing the information resulting from overcoming dangerous situations they had been exposed to in the past. This may be possible extending the concept of a network of influences based on the collaborative workflow typology. In other words, we can anticipate and better defend against an aggressor threatening a state-entity if within the collaborative workflow the strengths or weaknesses and lessons learned from an earlier confrontation of the aggressor with the collaborative partner of the state-entity have been disseminated. This can be done by building those common databases that are available to the parties included in the collaborative workflow network, as previously mentioned.

The conduct of the mutual awareness activities as well as the systemic interaction of each security pillar on the territory of one or more states is the starting point for decoding the connections of the network of influences and implicitly the implementation of a proactive behavior of identifying and countering a crisis. In this respect, we support the idea of the specialists in all areas of security collaborating, focusing their efforts on understanding the causes of the vulnerabilities and identifying the similarities of their manifestations. Critical infrastructure protection in the context of the security networks is a way of preventing and counteracting a crisis or of preventing the occurrence of a major negative event, and this subject can be elaborated in a much more thorough research by specialists in the field of security and not only.

We conclude by urging each owner or decision maker of a critical infrastructure to initiate and develop vulnerability scenarios based on potential threats in a network of mutual influences, and to identify solutions in a joint context consistent with the collaborative workflow principle, involving security or other systems

References

[1] BARABASI, A. L.: *Linked noua ştiinţă a reţelelor*. Timişoara : BrumaR Publishing House, 2017. p.12.

[2] *Official Journal of the European Union*, Directive 114/2008, L 345/77, RO.

[3] MARTIN, I.: *Raţionament şi argumentare în planificarea operaţiilor*. Bucharest : "Carol I" National Defense University Publishing House, 2015.

[4] Available at: https://www.recordedfuture.com/russia-ukraine-cyber-front/, accessed on 15.06.2018.

[5] Available at: https://www.reuters.com/article/us-nuclearpower-cyber-germany/german-nuclear-plant-infected-with-computer-viruses-operator-says-idUSKCN0XN2OS, accessed on 30.08.2018.

[6] Available at: https://www.independent.co.uk/travel/news-and-advice/mh17-anniversary-malaysia-airlines-plane-crash-russia-ukraine-conspiracy-theories-a8450501.html, accessed on 10.09.2018.

[7] Available at: https://cyberleninka.ru/article/n/the-sukhoi- su-24-incident-between-russia-and-turkey, accessed on 28.08.2018.

[8] Available at: https://www.worldvision.org/refugees-news-stories/syrian-refugee-crisis-facts, accessed on 10.06.2018.

[9] Available at: https://www.sri.ro/upload/Studiu%20-%20Protectia%20Infrastructurilor%20Critice.pdf, accessed on 10.09.2018.

[10] Available at: http://intelligence.sri.ro/cyber-noul-domeniu-operational-nato/, accessed on 08.09.2018.

Other Sources

[1] ALEXANDRESCU, G., VĂDUVA, G.: *Infrastructuri critice. Pericole, ameninţări la adresa acestora.* Bucharest : Sisteme de protecţie, "Carol I" National Defense University Publishing House, 2006.
[2] National Defense Strategy for 2015-2019, document approved by decision of the Supreme Council of National Defence no. 128 of 10 December 2015.
[3] Communication of the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, Bruxelles, 2009. Available at: http://ec.europa.eu/ transparency/regdoc/rep/1/2009/RO/1-2009- 149 -RO-F1-1.Pdf.
[4] Directive 2008/114/CE of the Council of 8 December 2008 regarding the identification and designation of European critical infrastructures and the assessment of the requirement to improve their protection, Bruxelles, 2008. Available at: http://ccpic.mai.gov.ro/docs/directiva114_RO. pdf?uri=OJ:L:2008:345:0075:0082:RO:PDF.
[5] DRACK, M.. Ludvik von Bertalanffy's early system approach. In *Systems Research and Behavioral Science,* Volume 26, Issue 5, September/October 2009, p. 566. Available at: http://journals.isss.org/index.php/proceedings52 nd/article/viewFile/1032/322.
[6] STEPHEN, P. R.: *Organizational Theory: Structure, Design, and Applications.* New Jersey : Prentice Hall, 1990.

LTC Assoc. Prof. Daniel ROMAN, PhD.
"Carol I" National Defence University
Panduri Street, No. 68-72, sector 5
Bucharest
Romania
E-mail: danutroman2@yahoo.com

LTC **Daniel ROMAN** is an Associate Professor within the Land Forces Department of the Faculty of Command and Staff, at "Carol I" National Defense University in Bucharest.