



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



**PRESENT AND NECESSITY IN THE NATIONAL APPROACH
OF CRITICAL INFRASTRUCTURES PROTECTION IN THE
CONTEXT OF HYBRID WARFARE THREATS**

ARAMĂ, Ghiță, military instructor

“Nicolae Bălcescu” Land Forces Academy of Sibiu

Abstract:

The contemporary citizen is increasingly facing challenges, for which he was not only not prepared, but which even in the most pessimistic scenarios he could not anticipate. They fall into the category of specific threats to hybrid conflict, a highly effective way of influencing and destabilizing the national security and security of a state through the effects it can cause on critical infrastructures. This paper is the first step in an extensive scientific research project that aims to identify vulnerabilities, risks and threats to national security and to create the prerequisites for raising awareness, analysis and elimination, where possible, of risks, as well as for the development/strengthening of the legislative framework for critical infrastructures.

Key words: threats; risks; hybrid warfare; critical infrastructure; resilience;

1. Introduction

Threats, whatever form they manifest, have always been and will always be an integral part of everyday life. However, humanity has not known such a high level of threats for a very long time, among the most common being non-military ones. The new challenges specific to the times we live in far outweigh the most difficult scenarios for which humanity was prepared. Among them, some are notable for the scale with which it manifests and spreads and by the effects felt by the large mass of the population: the medical and economic crisis generated by the COVID-19 pandemic, cybercrime, the phenomenon of organized crime manifested at the highest levels, poor infrastructure and the underfunding of rehabilitation and development projects with immediate effects on the economy and the daily life of the population, the demographic impasse generated by high mortality in conjunction with migration of young and skilled labor, the effects of which are difficult to estimate for the future.

This continuous change in the current security environment is accompanied by new ways of dealing with relations between states, in which case differences, whether of an ideological, political or religious nature, can escalate at any time by immediately turning into military conflicts: "if the twentieth century, from a security perspective, kept at the forefront the military dimension of threats, the present more visibly imposes a hybrid dimension. In an attempt to preserve security, states face a totally new typology of threats." [1]

The dynamics of the change in the current security environment oblige national security officials to work hard to identify vulnerabilities, risks and threats [2] to state integrity through the effects they can have on critical infrastructures and to create the premises for awareness, analysis and elimination, where possible, of risks as well as for the development/strengthening of the legislative framework related to the field.



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



The attractiveness and emergence of the field derives from the possibility of interpenetrating the scope of the approach to the vulnerability of sectors and activities with high criticism and impact on the safety of the citizen and the desire to ensure territorial integrity in the context of the manifestation of hybrid warfare.

2. The approach of critical infrastructures in national defense planning documents

The conceptual register of initiation of this scientific approach is based on the clear directions established by the new National Defense Strategy of the country for the period 2020-2024, which states directions of action specific to the defense and intelligence dimensions, counterintelligence and security, among those of interest being:

- "Facilitating the implementation of the NATO-EU cooperation agenda, in particular in the areas of cyber defense, combating hybrid threats, countering terrorist threats, resilience, strategic communication and military mobility;
- Support and coordination with other institutions for the development of critical infrastructure that can also be used in the field of defense;
- Strengthening the legal, procedural and operational framework specific to the protection of critical infrastructures;
- Preventing and countering hybrid threats, resulting in hostile conjugated actions, carried out by state or non-state actors, in political-administrative, economic, military, social, informational, cyber or organized crime" terms. [3]

The same defining document in the management of the national priority objectives for ensuring the security of Romania and citizens provides those interested with the constituent elements of the "strategy for the development of effective tools for strengthening societal resilience and critical infrastructures", of which we recall only "awareness of the population, central and local public institutions and the business environment on the importance of measures to protect critical infrastructures for the continuous and safe functioning of basic public services and utilities (electricity, water, heat, sanitation, public transport, social services)". [3]

At the same time, Romania's membership in the North Atlantic Organization is a security generator, while positioning on the eastern flank of the alliance is an issue worth considering, mainly due to the geoclimate in which a world superpower such as that of Russia is manifested. Thus, "the risks and threats of a military nature to Romania's security are manifested on several levels. As a member state of NATO and the EU we have an obligation to participate in ensuring national and Allied security. At the same time, at regional level, we see the destabilization of the security situation in the Black Sea Extended Region (REMN), against the background of the actions carried out by the Russian Federation to strengthen the zones of influence".[4] This instability in the Black Sea is accentuated by Ukraine's situation in relation to Russia, by the frozen conflict in the North Caucasus, but especially by Turkey's desire to transform Turkey from regional power to a global one.



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



3. Contextualization of critical infrastructure approaches based on paradigms specific to classical warfare and hybrid warfare

The concept of "hybrid warfare" is not a new one, but the thorough study and bringing it to the table of military theorists has been carried out in recent years. The "hybridity" of war derives from the use of non-military instruments to achieve political and strategic goals. If at the beginning of its use, hybrid warfare was used by the little against the great, by the weak against the powerful, by the few against the many, nowadays, this cannot be called into question, with the great regional and world powers addressing such strategies in order to limit the loss of life, financial resources and not least image. For its implementation, the aggressor aims, whether alongside a classical form of war or not, to diminish the power of governance through techniques of manipulation and influence of public opinion aimed at reducing the level of public confidence in state institutions due to internal political struggles, while exploiting grievances generated by social imbalances, interethnic and/or religious conflicts/differences.

In a 2013 article published in the Chief of the General Staff of the Russian Federation, Valery Gherasimov, wrote that "the role of non-military means has increased and in many cases has exceeded, in efficiency, the force of arms".[5] Thus the hybrid character is found throughout the spectrum of combat actions and profoundly alters the conduct of modern warfare. This and in general the conception of military actions is substantially changing, so that "the extent of political, economic, cultural and religious interests that manifest themselves in the current geopolitical and geostrategic context, leads us to consider that diplomatic, political, informational and economic aspects, as well as other non-military measures, occupy a special place in shaping the operational environment today. Their importance is felt not only during the escalation of the crisis and at the stage of its end, but even during military operations".[6]

By paying sufficient attention to the statements made by the Russian official, we can infer that critical infrastructures are points of real interest in the context of hybrid warfare, being easy, niche and convenient objectives for the aggressor due to vulnerability and lack of concern for limiting criticism, this facilitating their destruction or disruption with a significant impact on the target state.

Critical infrastructure is defined, in accordance with Council Directive 2008/114/EC of December 2008, as 'an element, system or component thereof, located in the territory of the member states, which 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 in a member state as a result of the inability to maintain those functions. [7]

Critical infrastructures are ubiquitous in everyday life, by the characteristic of necessity to ensure the normal conduct of social processes, regardless of the level at which they manifest themselves. In its position, States, which are at different levels of economic performance, have adopted different approaches to the concept of critical infrastructure security, resulting in their definition and diversified application at national level.

In their efforts to establish methodologies for identifying and evaluating critical infrastructures, Greek researchers N. Petrakos and P. Kotzanicolaou present the idea that "since in most cases critical infrastructure holders and/or operators are private entities, any process of identifying national critical infrastructures,..., requires an exchange of information between the parties involved in accordance with the principle of stakeholder cooperation in a Public-Private



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



Partnership".[8] Even if in the field of National Security, we will meet only operators but not holders of critical infrastructures, good cooperation is required at all institutional levels so that updating the legislation in the field and how to implement it at all levels ensures the desire to which we aim, a more viable approach to the protection of critical infrastructures. Specifically, in relation to the central approach to this work, the National Security sector is regulated at national level by means of the following subsectors: 'country defense, public order and national security; borders, migration and asylum; the national security industry, production and storage capacities and facilities; emergency situations; justice and prisons. [9]

Security, including military security, can no longer be seen today only in shades of white (lack of threats) and black (multiple, asymmetric threats), the spectrum of analysis being much more diversified, with multiple economic, ecological, social correlations, the military field being "trained" implicitly in this Framework of the VUCA type (Volatility, Uncertainty, Complexity and Ambiguity). Concepts such as dynamic capabilities, business continuity, governance and resilience [10] are increasingly developed and applied, extensively and intensively, multi-stage and multispectral. Basically, as polish researcher Grzegorz W. Kolodko observed, "there is no shortage of threats and opportunities, but our objective is to multiply and exploit the latter to the fullest, actively reacting to the former. In many situations there will be more and more rational behaviors and decisions, because many processes overlap, and this co-operation will be decisive. The coexistence of changes in values, global institutions, technical progress and the knowledge-based economy, as well as the ubiquitous Internet, will have effects. However, we will not lack threats to sustainable development. We must be constantly cautious, because now there is a great battle for the world of the future". [11]

The study of a historical security perspective of critical infrastructures is an important indicator of their military significance, some of them with strong reverberations in the history of universal or national military art, some significant examples in this regard being: the Great Wall of China, the Maginot Line, the Fortified Fortress of Bucharest, the Trans-Siberian, Apolodor's bridge, the launch of the Sputnik 1 satellite, the Apollo 11 mission, the Pentagon building, the Focsani-Namoloasa-Galati Defense Line.

“Focsani Gate”, the last mentioned in the above enumeration is a defensive component of tremendous importance within a state on the eastern border of the most powerful global alliance. „Having in mind Romania’s neighbourhood, it can be added to the general conclusion the reality that one of the most powerful, militarily speaking, country in the world, possessing, among other weaponry, one of the most destructive nuclear arsenal, has proved to be politically and strategically restless, choosing to tramp over its word by breaking promises, arrangements and treaties it put its signature on. The most important idea to be kept in mind is that this key terrain, acting as a mobility corridor, is clustering and, at the same time, it is opening operational and strategic directions that are covering Romanian territory and, more than that, are going beyond it, to the Central Europe and to the Balkans. The logical implication is that the Focşani Gate must always be in friendly hands if NATO’s and EU’s defence are to be ensured” [12].



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



Fig.1 The schematic of strategic and operational avenues of approaches on the south-eastern and southern part of the European Continent that are open once the Focsani Gate is cleared [12].

In a closed connection with strategic military elements, in the E-SE area of Romania, raised to our attention some objectives of national and regional interest on which we must lean carefully and patiently in an extensive process of interministerial/interdisciplinary cooperation in the hope of achieving all the objectives assumed to protect them. I would only recall the Romanian Black Sea coast with the Constanta port area, the Cernavoda Nuclear Power Plant, the Galati industrial area, the petrochemical infrastructure at Năvodari, the Danube-Black Sea canal, the Lower Danube waterway, the Bucharest urban-industrial agglomeration, with various objectives of interest in relation to the central subject of this topic, in which a special role in the current pandemic context lies with "Cantacuzino" Medical-Military Research and Development National Institute.

4. Conclusions

The evolution of the field of critical infrastructures will be equally dynamic and challenging and will continue to bring to the attention of theorists and practitioners multiple challenges, with varied implications on security, in all areas as economic, ecological, individual, collective, national, urban, human, etc., and subsequently, on defense, which is also confirmed by references to this in the defense planning documents (National Defense Strategy).

The response of specialists must be carefully documented and applied on scientific foundations following one of the extensive consolidated research process integrating theory with practice, which consists of:

- analysis of the data in the literature, a process involving bible documentation aimed at clarifying and specifying precisely the level at which knowledge has now reached in the field



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



addressed; and direct documentation of reality with the aim of a more accurate knowledge of the reality of the field of interest;

- using modeling & simulating critical infrastructure protection [13] for different types of attacks, tracking how to propagate domino effects on national security; primordial, following the modeling of the interactions that manifest themselves between different critical infrastructures, with the help of existing software in the field;
- applying the questionnaire technique of scientific value (using recognized software, e.g. IBM SPSS), a method of interest for population survey, on the perception of residents in/outside risk areas and decision-makers about the risks arising from critical infrastructures and implemented protection measures.

References:

- [1] Tiberiu Lazăr, *Hybrid warfare. Weapons and alarms*, <https://intelligence.sri.ro/razboiul-hibrid-arme-si-alarme/>, accessed 07.09 2020.
- [2] Dorel Badea, *Conceptualization of a knowledge management framework dedicated to the security of critical infrastructures*, The 14th International Scientific Conference “Defense Resources Management in the 21st Century”, Braşov, November 7th-8th 2019, pp. 13-17, ISSN 2248-2385 (on line).
- [3] ***National Defense Strategy for period 2020-2024, https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf, accessed 06.09.2020.
- [4] *** National Military Strategy of 28 september 2016, <http://legislatie.just.ro/Public/DetailiDocument/182367>, accessed 06.09.2020.
- [5] Valery Gerasimov, *The value of science in prediction*, Military-Industrial Kurier, (27 February - 5 March 2013), http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf. Robert Coalson, [http:// inmoscowsshadows.wordpress.com /2014/07/06/the-gerasimov-doctrine-and-russian-nonlinear -war/](http://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-nonlinear-war/), accessed 08.09.2020.
- [6] Ispas Lucian, Cîrdei Alin Ionuț - *Conventional features of hybrid warfare*, The 15th International conference Strategies XXI, April 2019, pp.1-2.
- [7] *** Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
- [8] Nikolaos Petrakos, Panayiotis Kotzanikolaou, *Methodologies and Strategies for Critical Infrastructure Protection*, în *Critical Infrastructure Security and Resilience*, Springer Publishing, 2019, pp.18-20.
- [9] *** [Law 225/2018](#) to modify and complete the [Government Emergency Ordinance no 98 from 3rd of November 2010](#) regarding the identification, designation and the protection of critical infrastructures.
- [10] Olga Bucoveţchi, Dorel Badea, Romana Oancea, Radu D. Stanciu, *Considerations on modelling resilience governance for decision support systems*, University Politehnica of Bucharest Scientific Bulletin Series B-Chemistry And Materials Science, Volume 80, Issue 2, pages 181-192, 2018.
- [11] Grzegorz W. Kolodko, *Whither the World: The Political Economy of the Future*, Polirom Publishing, Iaşi, 2015, p. 311.



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



[12] Mircea Mîndrescu, Gregory Melcher, Phillip Petersen - *The Focşani Gate - a Key Terrain for European Security*, New Strategy Centre, Decembre 2019, accessed 28.10.2020.

[13] Dorel Badea, Marin-Marian Coman, Dumitru Iancu, Olga Bucoveţchi, *Critical Infrastructure Protection in the Knowledge Society: Increasing the Safety Level by Use of Learning based on War Gaming Expertise*, BRAIN. Broad Research in Artificial Intelligence and Neuroscience, vol. 9, Issue 4, pp. 38-48, ISSN 2067-3957, 2018.