HYBRID WARFARE OR THE *"BLACK SWAN"* IN THE NEW CONTEMPORARY SOCIETAL CONTEXT

Daniel ROMAN

"Carol I" National Defence University
DOI: 10.55535/RMT.2022.2.04

The current international security situation determined by the new economic, financial, political, military and social context, in terms of the COVID-19 pandemic, is perhaps one of the major challenges that the states have to face in their development and existence. Beyond the concept of consolidated national defence, the need for an alliance and for lifting the barriers between states in the face of the waves of the SARS-CoV-2 Coronavirus contamination is a reality which is difficult to characterise. In this context, we rediscover the meaning of terms such as "uncertainty", "probability" and "knowledge" as well as the "Black Swan" – a highly improbable event, identified by rarity, extreme impact and surprise, which, despite the unexpected, could have been demonstrated predictable. Hybrid warfare – a trend in the international affairs at the beginning of the 21st century is already one of the intriguing topics of many studies on security or of epic writings about "an immediate future". The role of the military component in the societal network of the interconnected domains becomes a major one, which requires a reassessment of the military specialist's skills, in an extended situational awareness, on the critical infrastructure protection societal coordinates.

Keywords: hybrid warfare; military specialist; critical infrastructure; extended situational awareness; resilience; consolidated national defence;

THE GORDIAN KNOT DILEMMA AND THE SYSTEM OF THE CONTEMPORARY SOCIETAL VULNERABILITIES

The issue of the security of a state or an alliance entity, transposed into the coordinates of the stability generating factors, may be a wrong direction in the development of the current policies and strategies in a new contemporary societal context. This statement is based on the reality of the COVID-19 pandemic situation that the international community has been facing lately. Although the subject of the pandemic has reached high levels of concern and a number of solutions have been suggested in order to limit the effects of the crisis, new unpredicted events in the societal sphere are expected. An unpredicted event is more often than not associated with an event that is the least likely to occur, of course, on a pre-established scale of values [(the case of the nuclear power plant – a critical infrastructure, in Fukushima-Daiichi, in the event of 11 March 2011 *(Japan earthquake and tsunami of 2011)*, 9/11 attacks *(September 11 attacks)*]. An unpredicted event can be a *"surprise"* that overturns all the knowledge acquired up to that moment; there is practically a major change that has not been announced nor prepared in the past or, in other words, a *"crisis situation has just begun"*. The Gordian knot dilemma is the variant of characterising an extremely complicated problem situation that apparently has no solution. By knowing the past and identifying situations similar to the crisis initiated as the unpredicted phenomenon, a series of solutions can be formulated, which, unfortunately, do not prove to be a way out of the impasse. This is supported by the dynamic nature of the vulnerabilities of each societal area (analysed individually). The current pandemic crisis situation cannot remain an isolated issue whose solution has been identified in the possibility of vaccination and taking all the necessary measures to limit the spread of the virus. The implications of such a crisis situation can be much greater for an indefinite period of time, in the sense of propagating the *"societal shock wave"* and reconsidering the societal resilience in all areas of society.

The Gordian knot dilemma is the variant of characterising an extremely complicated problem situation that apparently has no solution. By knowing the past and identifying situations similar to the crisis initiated as the unpredicted phenomenon, a series of solutions can be formulated, which, unfortunately, do not prove to be a way out of the impasse. This is supported by the dynamic nature of the vulnerabilities of each societal area.

In order to describe and understand the destabilising phenomena that can occur in a certain PMESII (political/diplomatic, military, economic, social, infrastructure, information and environment) societal field, it is necessary to identify the extreme values for the status descriptive parameters (Roman, 2021, pp. 102-118). By status descriptive parameters we mean the description of those properties by which the analysed topic can be identified in the set it belongs to. For example: a physical object can be identified by: shape, colour, size, the material from which it is made, utility etc., all these being features by which the specific object is unique and can be nominated from a multitude of elements it belongs to. The second approach consists in the possibility of quantifying the properties of the subject (in the exemplification: the physical object) where it maintains its purpose or the utility for which it was created or selected from a certain set. The third approach consists in observing the transformations of the properties of the analysed subject, when destabilising factors act on it, under different degrees of influence. Therefore, following the three potential approaches, it is possible to express the guidelines for the protection and security of the analysed subject in relation to the nature and intensity of the destabilising factors that can act upon it. Finally, because of the loss of its properties and of the extreme actions of the destabilising factors on the analysed subject, the latter can no longer exist or can no longer fulfil its functions and meet the purpose for which it was created or selected. The fourth approach consists in identifying the relational links of the analysed subject to other subjects with which it has material or causal (influence) exchanges, entailing different effects. The fifth and last approach refers to the nature of the negative event having an impact on the analysed subject. In this context, an impacting negative event refers to the contribution of one or more influencing factors or actors, which, as a result of the action or lack of action, affect the status descriptive parameters of the analysed subject. Once these aspects related to obtaining or losing the state of safety or security of an analysed subject have been clarified, the study of the set of contemporary societal vulnerabilities can be launched. Thus, we can understand the current situation of the pandemic, as one of the general states of crisis extended internationally, specific to 1914, comparable to the general situation prior to the First World War, the moment of the *"Sarajevo attack"*. As a whole, the First World

In order to describe and understand the destabilising phenomena that can occur in a certain PMESII (political/diplomatic, military, economic, social, infrastructure, information and environment) societal field, it is necessary to identify the extreme values for the status descriptive parameters. By status descriptive parameters we mean the description of those properties by which the analysed topic can be identified in the set it belongs to.

War was a real surprise in the context of the post-Napoleonic wars peace situation, which made any historian believe that the destructive wars had disappeared at that time. In this context, initiating the study of the set of contemporary societal vulnerabilities can be the task or mission appropriate to a specific category of specialists: risk managers. Through the way of substantiating the scientific approach, a risk manager *"employs models of the past to calculate the possibilities of such an event to occur"* (Taleb, 2017, p. 71). In the work entitled *The Fifth Horseman and the New MAD* by Harlan Ullman (2021), the risk manager becomes that visionary who performs analyses of the future or situation analyses in which *"the positive disruption"* can be the right solution to counter threats and challenges posed to the regional and global security. Harlan Ullman identifies seven disruptive elements of the new MAD concept, which *"threaten both the United States and the world, by attacking the societal vulnerabilities, many of which being created – unintentionally and ironically – by the benefits of globalisation and power dispersion"* (Ullman, 2021, p. 19). The set of the network connections between the societal domains graphically represented in *figure no. 1* (Roman, pp. 102-118), by extrapolation in the new context of the *"seven disruptive forces of Harlan Ullman: failed or underperforming government, climate change, cyberspace, social networks, terrorism, explosive debt growth, and drones"* (Ullmann, p. 32), may be the new reality of the beginning of the 21st century.

The set of the network connections between the societal domains, by extrapolation in the new context of the "seven disruptive forces of Harlan Ullman: failed or underperforming government, climate change, cyberspace, social networks, terrorism, explosive debt growth, and drones", may be the new reality of the beginning of the 21st century.

The reality of the network connections of the societal domains as distinct elements or parts thereof (as shown in *figure no. 1*), based on their interactions from the perspective of the concept of the critical infrastructure protection allows us to put two directions of research and evaluation of a crisis situation in a scientific context (Barabasi, 2017, pp. 3-25). The first direction is based on the specialists' effort to understand a crisis situation by means of the *inductive knowledge*, while the second direction is based on the *reverse learning knowledge*. The two identified directions of knowledge contribute distinctly to the possibility of assessing the current security environment and are a response to the need for *extensive situational awareness*. This type of knowledge, stated and supported in the *White Paper on Defence* developed by the Ministry of National Defence, provides the formal organisational framework for managing a crisis situation (*Carta albă a apărării*). From a technical point of view, decoding the reality

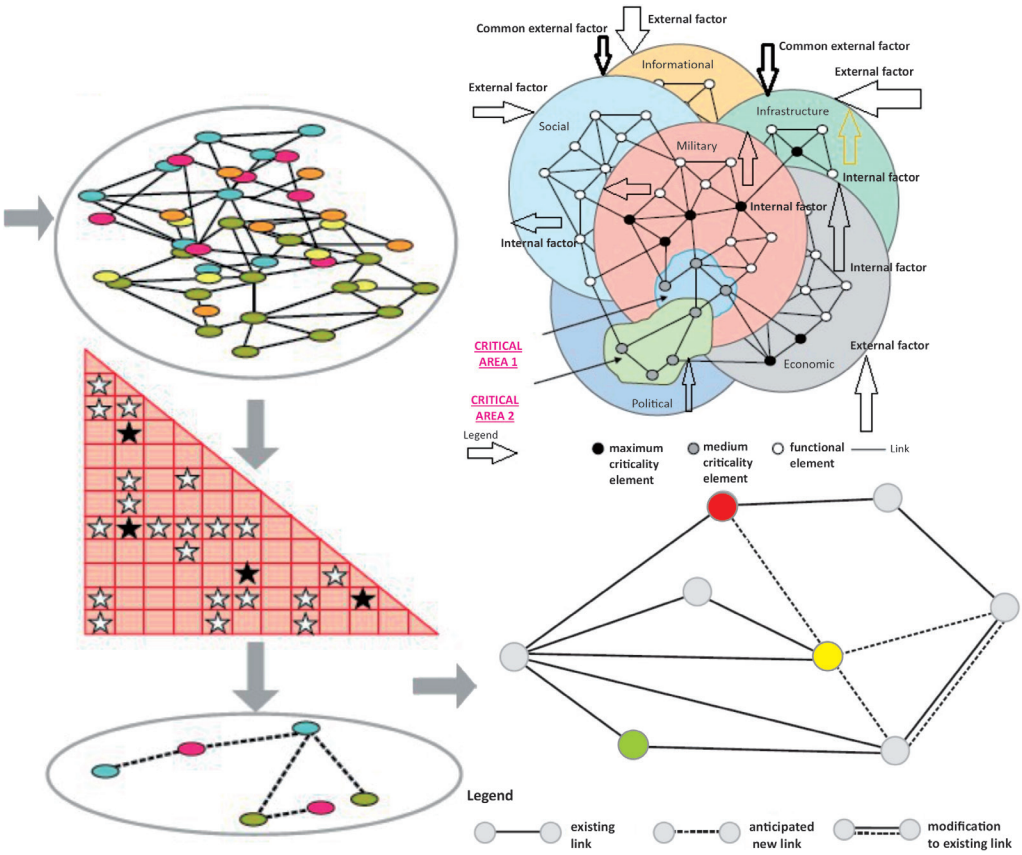

Figure no. 1: The design of the transformations at network level in the societal environment, following the decisions made by the factors responsible for allocating resources
(JP2-01.3 Joint Intelligence Preparation of the Operational Environment, 2014, figure V-2, figure III-14, figure V-4).

of the current security environment is one of the great challenges of knowing and managing a crisis situation. The military specialist intervenes and acts in accordance to the actions of a potential aggressor and thus brings together in a single effort three major components of the design of the future conflict: *analysis*, *planning*, *decision*. The difficulty of such an approach increases according to the reality of the set of contemporary societal vulnerabilities, which is why the *extended situational awareness* has been required as a response measure to counteract the hybrid threats. This brings the dilemma of the Gordian knot (Ewans, 2018) and the set of societal vulnerabilities to the forefront, namely: *What is the necessary ratio of reactive and proactive behaviour when facing hybrid threats?*

IS HYBRID WARFARE A SOCIETAL WARFARE?

In order to solve a crisis situation, first of all, it is necessary to express the identified problem correctly or to decode the reality in which the dysfunctions and the effects of the actions of the destabilising factors are visible in a difficult to characterise dynamics. Following the conceptual evolution of the *hybrid-type threat* and starting from the disruptive elements of the new MAD concept in Harlan Ullman's view, the imbalance of the network relations in the societal domains is quite obvious, to the point of affecting the existence of the target state, making the countering of such threats a matter of national defence. Compared to the results of the research conducted so far, Nathan Freier's *Quad chart* model develops the dynamics of the hybrid threats through the combined action of four types of threats: conventional or traditional, unconventional or irregular, catastrophic and disruptive (Potârniche, Petrescu, 2019, pp. 77-78). The dimensionality of a hybrid aggression results from its configuration: *"it involves a considerable effort; it must be carried out through a complex process, similar to that of operational planning (the product consists of a series of actions in all areas assimilated to military operations) and which must be conducted by an actor who is at least rational, if not super- rational"* Ib., p. 78).

The critical infrastructure protection refers to the vital elements of society, in particular to essential goods and services whose stability depends on the anticipatory attitude of the likeliness of occurrence of a risk or a negative event having major impact.

In order to manage a hybrid aggression (generating a crisis situation), we anticipate the possibility of becoming aware of it by means of two methods or two distinct directions to follow: *inductive knowledge* and *reverse learning knowledge*. For several reasons, we selected the domain of the *critical infrastructure protection* as a reference point in developing the two methods (Roman, Repez, Popa, 2017, pp. 3-21). First of all, the critical infrastructure protection refers to the vital elements of society, in particular to essential goods and services whose stability depends on the anticipatory attitude of the likeliness of occurrence of a risk or a negative event having major impact (Leaua, Ardeleanu, 2014, pp. 145-148). Secondly, the development of the concept of *resilience* is interesting, as being the ability of a subject to fulfil his/her duties or role, in relation to the performance achieved, after having absorbed the impact of the negative event he/she has been subjected to. Moreover, in the calculation of the performance achieved before and after the impact of the negative event, the *context assessment* is fundamental in the critical infrastructure protection. Taking into account the evolution of the societal domains

in relation to the societal network connections shown in *figure no. 1*, we can deduce that the occurrence of an identified risk for one of the societal domains implies the propagation of the negative effect as a *shock wave* throughout the societal network. On this subject, from the point of view of the military specialist, a negative event may be the result of the action of a hostile or enemy actor. By combining several hostile actions on different societal domains (as societal network connections) an opponent can design, plan and execute destructions other than military, which generically speaking, have been identified as *hybrid aggressions*. The gradual evolution of such hybrid aggressions includes sophisticated processes for identifying the status parameters of a state entity (similar to a physical object) or an alliance (similar to a set of physical objects), their nominal operating values, which by being modified under the action of the destabilising factors can lead to what we call a *societal disaster*. A societal disaster can be the COVID-19 pandemic when the out-of-control phenomenon of contamination could cause significant damage to several societal domains putting them in fatal danger.

The development of the courses of action is the essence of the process of counteracting the enemy's actions. Any course of action supported by the operative art sets, in space and time, the results of the predicted actions (of the enemy) and of the planned actions (of the friendly forces), so as to highlight the decisive points through which the major event or the crisis situation occurs.

Given the limited possibility of identifying the aggressor of a hybrid action, we refer to the operative art in which the military specialist deconstructs past events, makes an analysis of the conflict environment (intelligence preparation of the battlefield) (*JP2-01.3*, p. III-45) and develops the courses of action both for the opponent as well as for the friendly forces. The development of the courses of action is *the essence of the process of counteracting the enemy's actions*. Any course of action supported by the operative art sets, in space and time, the results of the predicted actions (of the enemy) and of the planned actions (of the friendly forces), so as to highlight the decisive points through which the major event or the crisis situation occurs (Wade, 2016). In other words, the EVENT lies at the foundation of such scientific approaches. Therefore, all learning is about how events occur, be they catastrophic or negative, depending on the impact they cause. The critical infrastructure protection research results in two types of behaviour depending on the occurrence of the event: the *reactive behaviour* that is manifested after the event and includes the application of the intervention and disaster limitation procedures, and the second one, the *proactive behaviour* that occurs before the event and includes measures to prevent, counteract threats,

apply rules and measures for the safety and security of the societal objectives. By extension, if we consider the proactive behaviour as a component of the post-event procedures, we can say, similarly to the modelling operations in military action planning, that we are dealing with hybrid threat/aggression countermeasures, in plain words with *"anti-hybrid operations"*. Therefore, the answer to the question *"Is hybrid warfare a societal warfare?"* must be found in the context of planning military operations and critical infrastructure protection or as a joint vision of the military specialist and the liaison officer for the critical infrastructure protection (*Legea no. 225/2018*).

The concept of *consolidated national defence*, viewed from the perspective of the comprehensive and integrated approach, stated in *Romania's 2021 Military Strategy*, cannot be explained independently of the set of the societal network connections shown in *figure no. 1*. This is the reason why a series of conceptual and operational transformations are required, in which the structures of the national security system behave (reactively and proactively) as a true system based on the interagency connections. In this way, the two directions or methods of knowledge development (inductive knowledge and reverse learning knowledge) contribute to the achievement of the *extended situational awareness*. Such awareness involves, by extrapolation, identifying the status parameters of a (societal) domain, so that its operational environment is known, the network connections with the other (societal) domains are nominated and evaluated and the functioning of the societal system or the societal network as a unitary whole is determined. In other words, consolidated national defence is the unification in terms of security and safety not only of the individual societal domains, but rather of the network connections and the transfers between the societal domains, and it can only be achieved through *contextual learning*, similar to defining the resilience within the critical infrastructure protection. Contextual learning can only happen in a multidisciplinary approach to at least two societal domains, as in *figure no. 2* (Nabil, 2011, p. 7) by developing the performance obtained by solving real situations according to the algorithm developed in the LUMAS model – a model developed by Peter Checkland (2000). Thus, by combining the *reverse learning knowledge* and the *contextual learning* we obtain the *extended situational awareness*, which generates the positioning of the EVENT as a central notion of any situation analysis

Consolidated national defence is the unification in terms of security and safety not only of the individual societal domains, but rather of the network connections and the transfers between the societal domains, and it can only be achieved through contextual learning, similar to defining the resilience within the critical infrastructure protection.

or planning and decision-making on developing the courses of action or the concepts for solving a crisis situation. This is the reason why we recommend the LUMAS model to be used in the development of the strategies to combat hybrid threats and to implement the necessary measures and procedures to prevent a crisis situation *(figure no. 2)*.

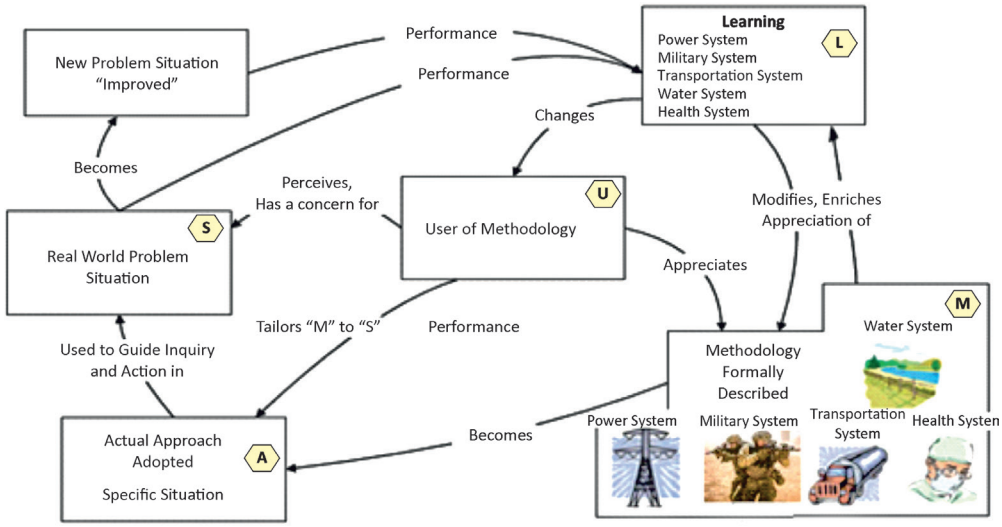

Figure no. 2: The methodology of importing/exporting knowledge underlying the system of educational systems for societal security (Lehaci et al, 2020, pp. 7371-7378)

Learning-based knowledge as a method of managing hybrid warfare or crisis situations can be efficiently achieved only by applying the methodology of importing/exporting knowledge underlying the system of education systems for the societal security. We firmly assert that only this way the notion of NEGATIVE EVENT WITH MAJOR SOCIETAL IMPACT (the centre of gravity in a hybrid- type confrontation) acquires content and can be capitalised in the training of specialists both in the military field and in any other societal domain with responsibilities in the field of safety and security.

INSTEAD OF CONCLUSIONS – WHERE IS THE *"BLACK SWAN"*?

The concepts of *resilience*, *extended situational awareness* and *consolidated national defence* are the main points of the reference documents in the development of *Romania's 2021-2024 National Defence Strategy*. This is the reason why we have developed a series

of statements in the present paper that is aimed at supporting the reader *"to see beyond the formalities"* and to perceive a new reality generated by the nature of the hybrid threats in relation to the current situation of the COVID-19 pandemic, as well as at warning on the notion of *negative event with a major societal impact*. We have placed this type of event at the centre of gravity of a hypothetical hybrid confrontation, due to *the impact of the highly improbable* or *the Black Swan* (in the concept of Nassim Nicholas Taleb). In our opinion, hybrid warfare, beyond definitions and other explanations, is *"an exploitation of the tandem of favourable and unfavourable situations by a potential adversary, by supporting and enhancing unfavourable situations until the success of the negative event with a major societal impact"*. The occurrence or the materialisation of such a negative event will have an impact proportional to its expectation rate. In other words, the destructive power of the event in the case of the hybrid warfare will materialise similarly to the appearance of a *"Black Swan"*. However, as in military operations, there is a scale of the severity of the moments of combat depending on the role of operations: support operations, modelling operations and decisive operations. Following this gradual course of operations, we can talk about the stages of the hybrid warfare as a coherent sum of events that can occur simultaneously or in stages in terms of time and space, having effects or consequences so that the target could not recognise the action conducted against it and even more so could not react accordingly. Achieving or supporting the occurrence of a negative event (regardless of the societal environment intended to be affected) is not only for causing damage and exploiting opportunities, but rather for destabilising the society as a whole, creating ambiguity in order to endanger the process of counteracting the negative hybrid-type manifestations and implicitly the whole decision-making process accordingly. Thus, addressing the *"Black Swan"* issue, in the concept of Nassim Nicholas Taleb, emphasises the fact that *"The inability to predict isolated cases implies the inability to predict the course of history, given the proportion of these events in the general dynamics of the events"* (Taleb, p. 18).

We can talk about the stages of the hybrid warfare as a coherent sum of events that can occur simultaneously or in stages in terms of time and space, having effects or consequences so that the target could not recognise the action conducted against it and even more so could not react accordingly.

A very special situation is generated by the impact of the information and communications technology on the statistical data related to the state of affairs of the societal domains at a given time. Based on these statistical data related to the status parameters of different societal components, there is a tendency to believe in the ability to predict

historical events, respectively to change the course of history. Certainly, there are phenomena that can be predicted in terms of their evolution, but the sensitive point is reached when the same solving principles are erroneously applied to similar but different domains regarding some particular properties (although water, which is a liquid, has a boiling point of 100 degrees Celsius, any liquid other than water cannot have the same boiling point, even if it is also a liquid). Therefore, as in the case of the hybrid warfare, as we have defined it, no predictions can be made and implicitly no measures to counteract a negative event can be developed. Instead, a contextual knowledge can be achieved by adopting a reverse learning-based attitude, supported by intuitive learning.

Nassim Nicholas Taleb suggests that: "Since <Black Swans> are not predictable, we must adapt to their existence (rather than naively try to predict them). There are many things we can do if we focus on anti-knowledge, that is, on what we do not know".

In conclusion, Nassim Nicholas Taleb suggests that: *"Since <Black Swans> are not predictable, we must adapt to their existence (rather than naively try to predict them). There are many things we can do if we focus on anti-knowledge, that is, on what we do not know"* (Ib., p. 19).

BIBLIOGRAPHY:

1. Barabasi, A.L. (2017). *Linked: noua ştiinţă a reţelelor*. Timişoara: Editura Brumar.
2. Checkland, P. (2000). *Soft Systems Methodology: A Thirty-Year Retrospective,* Research Paper, fig. A10/S37, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.133.7381&rep=rep1&type=pdf, retrieved on 2 April 2020.
3. Dincovici, C. et al (2014). *Manualul privind pregătirea întrunită de informaţii a mediului operaţional*. București: Editura Militară.
4. Ewans, A. (2018). *What Was the Gordian Knot?*, https://www.history.com/news/what-was-the-gordian-knot, retrieved on 27 September 2021.
5. Leaua, L., Ardeleanu, D. (2014). *Protecţia infrastructurilor critice – perspective de dezvoltare*. București: Editura Academiei Naționale de Informații.
6. Lehaci, T.-N., Roman, D., Ţuţuianu, D.-E. (2020). *The Workflow Concept in Education for Societal Security in the Context of a Major Crisis*. The 12th International Conference on Education and New Learning Technologies EDULEARN 20, 6-7 July, Conference Proceedings, Spain.
7. Nabil, A. (Chair) (2011). *Modeling and Simulation of Critical Infrastructure Systems for Homeland Security Applications*. U.S. Department of Homeland Security, Science & Technology Directorate.
8. Potârniche, M., Petrescu, D. (2019). *Modalități de contracarare a amenințării hibride la adresa securității statelor*. București: Editura Universității Naționale de Apărare *"Carol I"*, https://cssas.unap.ro/ro/pdf_studii/modalitati_de_contracarare_a_amenintarii_hibride.pdf, retrieved on 27 September 2021.

9. Roman, D. (2021). *The Perspective of Military Action Planning in the Context of the Development of Resilience Capacity in the Contemporary Societal Environment*. In *Romanian Military Thinking*, Defence Staff, no. 1.
10. Roman, D., Repez, F., Popa, E.V. (2017). *Infrastructura critică – Reglementări legislative şi de planificare a protecţiei*. București: Editura Centrului Tehnic-Editorial al Armatei.
11. Taleb, N.N. (2017). *Lebăda Neagră – impactul foarte puțin al probabilului*. București: Editura Curtea Veche.
12. Ullman, H. (2021). *Al cincilea cavaler al apocalipsei și noul M.A.D.* București: Editura Militară.
13. Wade, N.M. (2016). *Counterterrorism, WMD and Hybrid Threat SMARTbook*, 1st edition. The Lightning Press (Critical infrastructure protection five-step process).
14. Directive 2008/114/CE of the Council of 8 December 2008 on the identification and designation of the European critical infrastructures and assessment of the need to improve their protection (2008). Brussels.
15. *Japan earthquake and tsunami of 2011*, https://www.britannica.com/event/Japan-earthquake-and-tsunami-of-2011, retrieved on 22 September 2021.
16. JP2-01.3 *Joint Intelligence Preparation of the Operational Environment* (2014), p. III-45.
17. *Legea nr. 225 din 1 august 2018 pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice*. Parlamentul României, http://legislatie.just.ro/Public/DetaliiDocument/203523, retrieved on 11 September 2021.
18. *September 11 attacks*, https://www.britannica.com/event/September-11-attacks, retrieved on 22 September 2021.
19. *Strategia Națională de Apărare a Țării pentru perioada 2020-2024. „Împreună, pentru o Românie sigură și prosperă într-o lume marcată de noi provocări"* (2020). București: Administrația Prezidențială, https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf, retrieved on 17 September 2021.
20. http://ccpic.mai.gov.ro/docs/directiva114_RO.pdf?uri=OJ:L:2008:345:0075:0082:RO:PDF, retrieved on 22 September 2021.
21. https://sgg.gov.ro/1/wp-content/uploads/2021/03/CARTA-ALBA-A-APARARII-.pdf, retrieved on 17 September 2021.
22. http://www.nato.int/ims/docu/terrorism.htm, retrieved on 17 September 2021.