THE PERSPECTIVE OF MILITARY ACTION PLANNING IN THE CONTEXT OF THE DEVELOPMENT OF THE RESILIENCE CAPACITY IN THE CONTEMPORARY SOCIETAL ENVIRONMENT

Colonel Daniel ROMAN, PhD

"Carol I" National Defence University, Bucharest

The security and safety in fulfilling the roles of the institutions of a state are essential characteristics of any contemporary society. In order to understand the complex of threats and vulnerabilities, as well as the dynamics of their manifestation in generating crisis situations, it is required to take a comprehensive approach to the decision-makers in the societal domains: political/diplomatic, military, economic, social, critical infrastructural, informational and environmental.

In this context, the development of the resilience capacity in the contemporary societal environment takes place in the perspective of the contribution of all the decision-making factors based on efficient inter-institutional planning and their proactive participation. Due to the specifics of each societal field, the situation can be understood under different coordinates, which causes difficulties in developing estimates of the crisis situations and initiating measures to prevent and counteract them. One of the solutions identified for the decision-makers to conduct a proactive behaviour in crisis situations specific to the contemporary societal environment can be expressed within the operational art of military action planning. Thus, we deem appropriate to extend the operational art specific to the military field to other societal fields and redefine the resilience capacity in the contemporary societal environment facing the new complex of threats and vulnerabilities as the COVID-19 pandemic situation.

Keywords: military action planning; critical infrastructure; crisis; resilience; societal security;

INTRODUCTION – THE DEVELOPMENT OF THE RESILIENCE CAPACITY IN THE CONTEMPORARY SOCIETAL ENVIRONMENT

Periodically, modern states define their own national strategies for defending the country in terms of legislation and the changes that have occurred in the security and safety conditions for fulfilling their institutional roles. The contemporary societal environment is strongly characterised by the presence of a permanent and specific array of threats and vulnerabilities that the decision-making factors of the societal fields (political/diplomatic, military, economic, social, critical infrastructural, informational and environmental) have to face and to counteract with solutions (*NATO's Military Concept for Defence against Terrorism*, 2005). A crisis situation, such as the COVID-19 pandemic, has the particularity of manifesting itself both in the spatial and temporal coordinates and especially in the figures of societal indicators. By societal indicators we mean mainly the status parameters that define the existence and the proper functioning of a society as a whole, such as: the territorial area, the number of citizens, the forms of organising the communities and their institutionalised structures, the system of facilities for providing essential goods and services, the system of public order, national defence and security/PONDS, the relations and the typology of relations with other states, the nature and the level of transactions between them, the cultural-historical background of assertion as a state and internationally recognised entity, other such state identity landmarks. The state of security and safety of a nation can be expressed by means of societal indicators and their quantifiable values. Reaching certain boundary values of the societal indicators, previously identified or not identified, may lead to a situation where one or more societal domains becomes incapable to function properly, also known as a crisis situation for that particular domain.

The contemporary societal environment is strongly characterised by the presence of a permanent and specific array of threats and vulnerabilities that the decision-making factors of the societal fields (political/diplomatic, military, economic, social, critical infrastructural, informational and environmental) have to face and to counteract with solutions.

One of the essential characteristics of a crisis is the impossibility of predicting and efficiently counteracting the effects through which it manifests itself (Chifu, 2019, p. 16). In this regard, in order to solve the problem, a series of concepts specific to each societal field have emerged, so as to guarantee the existence and the proper functioning of the community or society in question. The development of the resilience capacity of a state entity lies in taking over the concept of preserving or returning to the physical, technical and functional properties of some objects found in nature, which, after experiencing a shock and undergoing changes in the properties that define them, regain through their own efforts their physical, technical and functional characteristics that they had before the above-mentioned shock. The absolute resilience of the object in question is proven by completely restoring its physical, technical and functional characteristics after experiencing the shock. Similar to an object in nature that has suffered a specific shock and proves a resilience capacity by returning to its properties, exclusively through its own efforts, each societal field can manifest a certain capacity for resilience. Therefore, the *resilience of a societal field* is its ability to return through its own efforts to the pre-shock state.

One of the essential characteristics of a crisis is the impossibility of predicting and efficiently counteracting the effects through which it manifests itself. In this regard, in order to solve the problem, a series of concepts specific to each societal field have emerged, so as to guarantee the existence and the proper functioning of the community or society in question.

The resilience of an entity can be explained by the model of a physical object and we choose to exemplify through a first experiment, that with a sponge that has certain properties of size, shape and colour. In situation A, the sponge experiences a shock by a sudden mechanical action, under the incidence of a blow with a hammer. In situation B, the same sponge undergoes a sudden thermal shock, under the incidence of being exposed to an open flame device. After analysing the two situations, A and B, it results that the same item subjected to shocks shows different resilience depending on the nature of the aggression factor. To develop the subject of resilience, we continue with another experiment, by which we subject the same sponge to the conditions of situations A and B, but we change the means of applying the shocks. This time, to express a proactive behaviour, in experiment A, we cover the sample with a resistant metal case before applying the mechanical shock and in experiment B we place a heat-resistant foil on the item before subjecting it to the flame.

Briefly, under a combined aspect, the inter-relating societal domains, just like the physical objects, show different resilience capacities depending on the context and on the aggression factors, thus mutually influencing each other according to their individual operational characteristics. Therefore, we find out that the manifestation of the effects of some crisis situations will differ depending on the specific capacities of the domains, and even more, on the nature of the relations between them. One of the important observations we can identify refers to the militant nature specific to each societal domain, in the sense that the entities belonging to the domains are designed to interact with the external environment according to their specific physical, technical and functional characteristics.

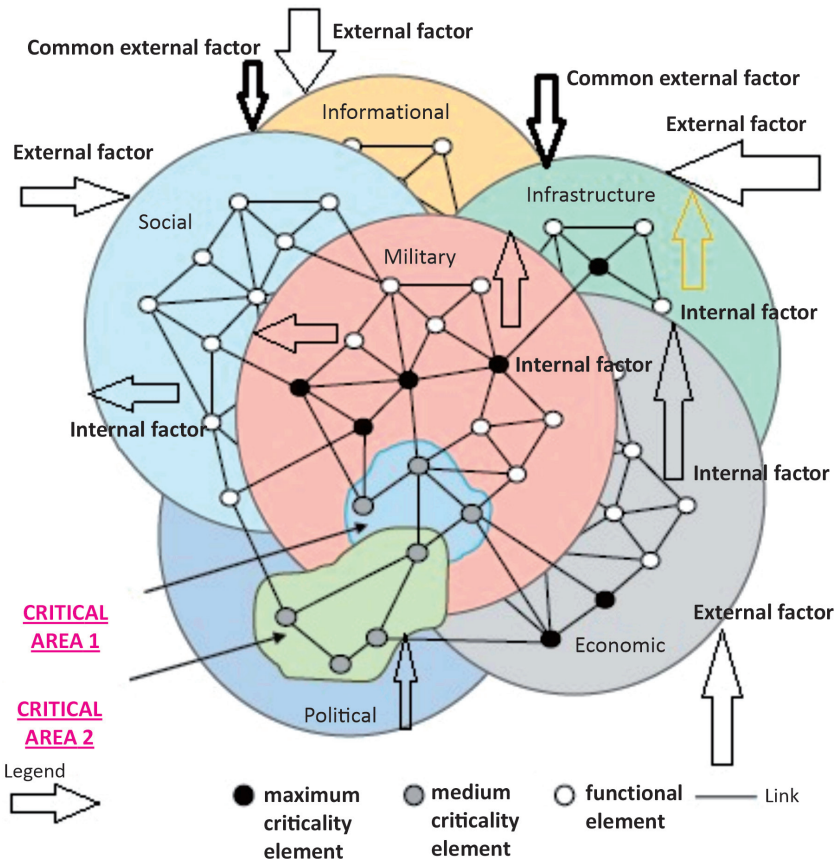

Figure no. 1: Graphical representation of the interdependencies of the influencing factors in the network of societal fields (Dincovici, 2014, p. 89).

Under a combined aspect, the inter-relating societal domains, just like the physical objects, show different resilience capacities depending on the context and on the aggression factors, thus mutually influencing each other according to their individual operational characteristics. Therefore, we find out that the manifestation of the effects of some crisis situations will differ depending on the specific capacities of the domains, and even more, on the nature of the relations between them.

As shown in *figure 1*, each interconnected societal domain interacts with its reference environment and, at the same time, establishes node-type relationships and network connections with the other societal domains (Ibid.). The dimensions and the geometries made for such a network are in permanent dynamics, influenced by the number, characteristics and intensity of the aggression factors, either internal or external to each societal field. In the situation of the COVID-19 pandemic, the aggression factors are not limited only to the manifestation of the SARS-CoV-2 virus, which is of course the main factor responsible for the pandemic. Due to the network connections between the societal domains and the geometry of the inputs and outputs based on the relations between them, the societal domains become more widely and more subtly affected (Barabasi, 2017, pp. 3-25).

In the situation of the COVID-19 pandemic, the aggression factors are not limited only to the manifestation of the SARS-CoV-2 virus, which is of course the main factor responsible for the pandemic. Due to the network connections between the societal domains and the geometry of the inputs and outputs based on the relations between them, the societal domains become more widely and more subtly affected.

In order to decode the effects following the manifestation of the pandemic situations on each societal field, it is necessary to use those concepts of *security* and *safety* specific to the societal domains that employ the notion of aggressor or enemy, as in the military societal field. The concept of *security* centred on the notion of *enemy* is specific to the operative art of the military field. But the operative art does not contain the integrated term of *resilience* and therefore we can speculate such a situation by conducting the transfer of know-how between the societal fields, especially for solving the crisis situation against the background of the COVID-19 pandemic. Integrating the term *resilience* in the operative art implies developing those threat scenarios specific to the societal field of critical infrastructures. Based on the threat scenarios, the protection of the critical infrastructures is achieved by adopting a proactive behaviour and, implicitly, by adopting the notion, transformations of the mechanism of producing situation estimates can occur[1]. (Leaua, Ardeleanu, 2014, pp. 145-148).

Due to the complexity and multitude of connections made between the societal domains, the contemporary societal environment becomes one of the most difficult environments to decode (Stanciu, 2016, pp. 28-35). The development of the resilience capacity in a societal field becomes dependent on the development of the resilience capacity of all the other societal domains with which it is interconnected,

1 A situation estimate is a notion belonging to the operational art.

a fact achievable by applying the operative art in the perspective of military action planning, based on four main directions:

- understanding the operational problem in a societal context;
- comprehensively and systemically understanding the roles of the decision-makers specific to the societal domains;
- developing the joint network operational approach in order to find and implement the solutions for solving the crisis situation;
- redefining the operational problem, in case the changes occurred in the situation require it.

By adopting the suggestion to develop the resilience capacity in the contemporary societal environment within the operative art, we overlap at least two societal domains: the military domain and the critical infrastructure one.

UNDERSTANDING THE OPERATIONAL PROBLEM IN THE CONTEXT OF THE BROAD SOCIETAL ENVIRONMENT

The description of the connections of the network nodes of the societal domains in a permanent dynamic represents the decoding of the contemporary societal environment that is the foundation for understanding the operational problem in the societal context (Stephen, 1990). Military action planning under crisis conditions, similar to the COVID-19 pandemic, cannot be limited to fulfilling the direct purpose of the military actions in a military conflict. This is further supported by the fact that the basic rules and concepts guide the use of military force and cover the full range of operations in peacetime, in crisis situations and in war (F.T.-1, 2017, p. 5). In a comprehensive approach, according to NATO, all institutions responsible for managing a crisis must have a common understanding of the desired objectives and the end state. It entails a unitary projection of the common resilience capacity based on the inter-institutional connections. Due to the dynamics of the relationships established *(figure no. 1)*, the development of the common resilience capacity cannot be the sum of all the resilience capacities of the interconnected societal domains. The concept of resilience in the societal field of critical infrastructures consists in the unitary expression of the values of the descriptive parameters for the provision of the quotas of products and services essential to life, under those safety and security conditions required for each critical infrastructure (Roman, 2018).

Military action planning under crisis conditions, similar to the COVID-19 pandemic, cannot be limited to fulfilling the direct purpose of the military actions in a military conflict. This is further supported by the fact that the basic rules and concepts guide the use of military force and cover the full range of operations in peacetime, in crisis situations and in war.

For example, we will relate the understanding of the operational problem in the societal context to only two areas: the military domain and the critical infrastructural one (Directive 114/2008). It opens a new perspective of military action planning, similar to the COVID-19 pandemic situation, where, by applying the concept of NA5CRO (NATO non-Article 5 crisis response operations), a particular importance is placed on collaborative planning of operations. Due to the complexity of the contemporary crises, the planning of actions within the societal domains cannot be fully consistent for all domains. The manifestation of the proactive behaviour and the establishment of the boundary values for the development of the resilience capacities within the societal domains can determine destructive actions on the other societal domains based on the mutually interdependent links. Thus, the development of a collaborative culture in designing the resilience capacities between the societal domains can be achieved by applying the operative art in the analysis and the reconfiguration of the network connections according to the model shown in *figure no. 2*.

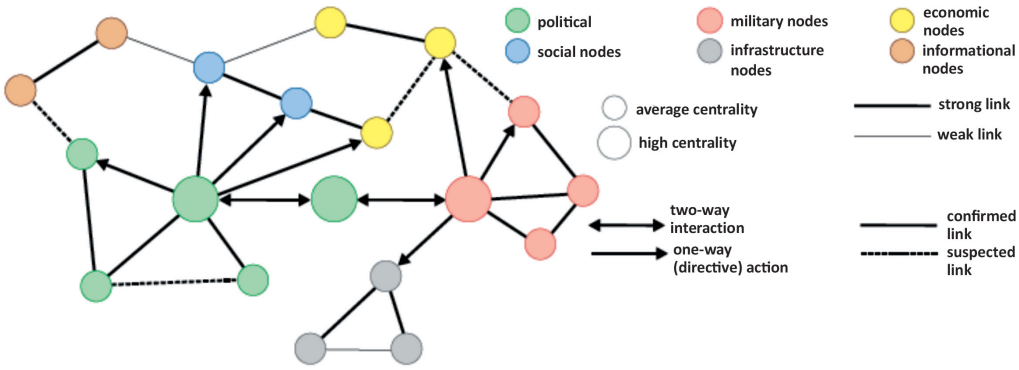

Figure no. 2: Example of a network analysis diagram
(JP2-01.3, 2014, p. III-45)

Due to the fact that the measures and the degree of their implementation within each societal field are not expressed, in case of a negative event with major societal impact or of the manifestation of an extended crisis situation, such as the model of analysis for determining the geometry of the relations between the societal domains *(figure no. 2)*, the mentioned solution is not enough. Within the process of designing the security and safety systems specific to the field of critical infrastructures, they become explicit

by nominating the boundary values obtained following the development of their resilience capabilities. In comparison, in the military field, there are nominations regarding the value and weight of the criteria for comparing the courses of action that underlie the *war games*. The conceptual overlap of developing the resilience capabilities in the context of the war games in an effort to find viable solutions to counter the actions of an enemy or the effects of an ongoing crisis brings forward the need for a new perspective on the military action planning.

The comprehensive understanding of the societal operational environment is the key to determine the network connections and the nature of these connections, which is why, when substantiating them, the military planners express and explain the military concepts in terms that are intelligible to the civilian partners in the field of critical infrastructure protection and other societal fields, and, in their turn, the latter do the same with their military partners. The advantage of such an approach of relating between the societal domains produces a continuous analysis of the societal operational environment in which the real consequences of the military actions but also of the other actors contributing to the implementation of the whole process of counteracting the effects of the ongoing crisis are thoroughly evaluated (Moștoflei, Alexandrescu, Bogzeanu, 2009, pp. 3-7). Based on the network connections according to the analysis shown in *figure no. 2*, the links between actions and effects can be anticipated and identified, especially the second and third order effects, which analysed in the evaluation points established in the operation planning, lead to a new flow of actions and real effects corrected and correlated with the results of the development of the resilience capacities of the involved societal domains. The comprehensive understanding of the societal operational environment in the above-mentioned manner based on the links shown in *figure no. 2* can be considered one of the mandatory measures for all decision-making forums at the level of each societal field. When formulating landmarks in the national defence strategy of NATO and EU states, strengthening resilience and reducing vulnerabilities call for consensus action based on a flexible multidimensional concept and a broad systemic perspective, in which the risks associated with the effects of the crisis are jointly approached.

When formulating landmarks in the national defence strategy of NATO and EU states, strengthening resilience and reducing vulnerabilities call for consensus action based on a flexible multidimensional concept and a broad systemic perspective, in which the risks associated with the effects of the crisis are jointly approached.

DEVELOPING THE NETWORK OPERATIONAL APPROACH FOR PLANNING AND IMPLEMENTING SOLUTIONS TO SOLVE A CRISIS SITUATION

The efforts of the specialists in the field of security and safety in maintaining or recovering the physical, technical and functional properties of the societal domains or their components consist in providing estimates regarding the future evolution of the negative situations having a destructive impact. One of the relevant solutions to this request may be to develop a joint network operational approach. The joint network operational approach, in the variant of developing the resilience capacity in the contemporary societal environment can be organised in several stages, as follows:

- conducting the analysis of the critical factors, namely the centralisation of the boundary values of the descriptive parameters of state and functioning for each societal field separately;
- developing the design of the connections between the societal domains and respectively between their components, based on the dependencies between their inputs and outputs (the totality of the provided goods and services);
- developing individually the threat scenarios within each societal field based on the identified aggression factors and the known vulnerabilities of our own assets;
- jointly developing the threat scenarios for the interconnected societal domains according to the diagrams of relations *(figure no. 1)*;
- planning and implementing the individual and common measures designed to prevent the materialisation of the negative situations having a destructive impact (manifestation of proactive behaviour);
- planning and implementing the individual and common protocols and procedures designed to limit and neutralise the effects and consequences of 1st, 2nd and 3rd level in case of occurrence of negative situations having a destructive impact (manifestation of reactive behaviour);
- checking and validating all projects regarding the network architecture, modifying its geometry when the societal

environment conditions change or whenever the situation requires it.

When we developed the joint network operational approach algorithm, we started from planning the analysis of the operational environment specific to the military action planning where we introduced the principles of designing security and safety systems specific to the critical infrastructures in order to develop their resilience capacities. As pointed out at the beginning of this paper, it is important to understand the resilience of a societal field. We exemplified it by approaching the societal field similarly to an object in nature, in which case the assertion of an entity's resilience is directly related to the physical, technical and functional characteristics of the subject, to its exclusive possibilities, to the nature of the aggression factor and the duration of its action, to the context of the occurrence of the shock and last but not least to the influence of the measures taken due to the proactive behaviour of the subject.

When we developed the joint network operational approach algorithm, we started from planning the analysis of the operational environment specific to the military action planning where we introduced the principles of designing security and safety systems specific to the critical infrastructures in order to develop their resilience capacities.

Implementing the solutions to a crisis situation is the most difficult and, at the same time, the most expensive stage. It is determined by the fact that crisis situations require a fully developed approach, namely *complex systems of analysis* (Wade, 2016). Because of the unpredictability of the enemy or aggression factor and of the environmental conditions that are continuously dynamic, the *operational design* is recommended as the most appropriate working method. The operational design approach is a challenge to establish that authority invested in choosing the optimal course of action. At state level, the governing political institutions establish the key policy of the way of managing the resources that support the solutions to counteract the effects and consequences of a crisis situation. Based on the resource management policy of any kind, they give new configurations to the network and therefore new network connections are established or others are permanently or temporarily suspended.

In the context of transforming the network connections (*figure no. 3)*, it results that the operational design has a double role in choosing the solutions to counteract the effects of a crisis.

Firstly, by operational design we express the current situation and the direction of evolution of the societal environment, by the nature of the connections between the societal domains. The second role of the operational design is that of a tool to correct the direction

of the evolution of the general situation by intervening in each societal field and by transforming the links between the societal domains. One of the important observations is that a crisis, just like a *"living organism"*, will behave according to a certain pattern, as a decision-making body that pursues its own goals similar to the actions of an enemy decoded through the operative art. Therefore, a crisis situation such as the COVID-19 pandemic can be effectively counteracted if the laws of its manifestation are known, a fact of which the specialists in the field of security and safety of societal fields are not ignorant (Seiple). This explains the solution to isolate in case of the pandemic to prevent the spread of the virus and not to counteract it by applying a vaccine that does not restrict the freedom of social interaction.

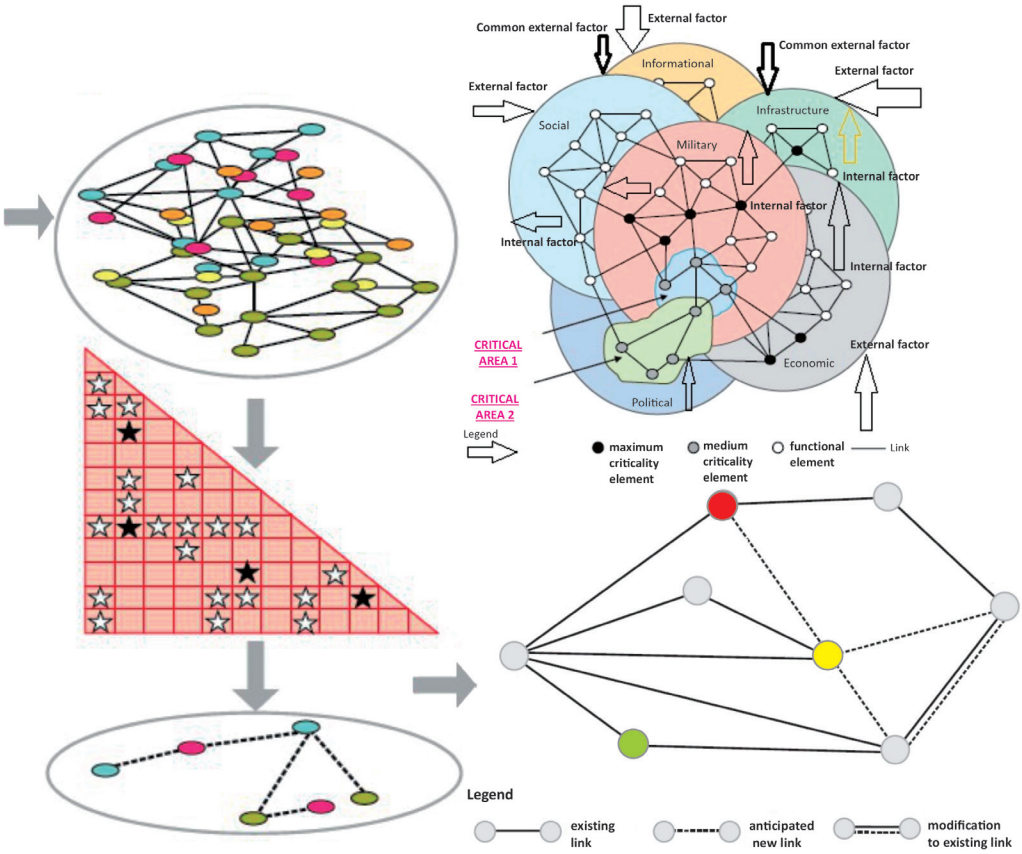

Figure no. 3: Scheme of network-level transformations in the societal environment due to the decisions made by the factors responsible for allocating resources
(adaptation and integration of (1) JP2-01.3 Joint Intelligence Preparation of the Operational Environment, 2014, figure V-2, figure III-14, figure V-4)

The problem that the operative art uncovers following the development of resilience in the contemporary societal environment from the perspective of military action planning is to highlight the fragility of the links between the societal domains and to proceed to their consolidation through corrective measures taken by the decision-making forums. In other words, knowing the values of the descriptive parameters for each societal field, respectively the nature of the connections between them, we can identify the directions of manifestation of an ongoing crisis or to detect the formation of new crises, of another nature, much deeper and much more dangerous for the society. The operationalisation of the *planning work* regarding the inter-institutional links between the societal domains based on the *situation estimates* (a notion which is specific to military action planning) substantially contributes to the decision-making at the level of each responsible body, which represents the decisive point in creating the operational network approach. In this regard, the practical implementation of the theoretical apparatus in the area of mlitary action planning involves the design and development of a collaborative network between the decision-making forums based on the model of the connections between the societal domains, similar to the functioning of the alert platforms specific to critical infrastructure. The advantage of the operationalisation that we have suggested is the establishment of the necessary conditions for the development of the estimates regarding the crisis situations and the initiation of the measures of preventing and counteracting them.

Knowing the values of the descriptive parameters for each societal field, respectively the nature of the connections between them, we can identify the directions of manifestation of an ongoing crisis or to detect the formation of new crises, of another nature, much deeper and much more dangerous for the society.

The development of the joint network operational approach can be the starting point in the elaboration and implementation of the solutions for solving a crisis situation. This is possible according to the model of the critical infrastructure protection procedures, applicable in the COVID-19 pandemic situation. Thus, in order to restore the operating conditions within the projected parameters, each societal domain affected by the pandemic will trigger its own procedures for developing resilience and implicitly determine a change in the geometry of the network connections between all societal domains. Changing the geometry of the network connections that we have previously mentioned can be one of the causes of the initiation of new crisis situations, much more unpredictable and more difficult

to manage. The joint network operational approach, as in the case of military action planning, involves the formulation of solutions based on the model of courses of action specific to war games. Identifying and managing the sets of descriptive parameters for each societal field according to the model of critical infrastructure protection for developing resilience contributes to accurately describing the position of each societal field in the network of influences *(figure no. 1)*. Following the overlap of the theoretical literature of the societal domains – military and critical infrastructure -, new determinations regarding the development of the resilience capabilities occur. In other words, there is a risk that, following the development of the resilience capabilities in one societal field, they will be the starting point for new crisis situations for the other societal domains. In this context, new perspectives of theoretical assimilation with practical applicability emerge regarding the background of the risk management problem for each societal field.

The phrase "hybrid warfare" can be defined as "that accumulation of actions directed in a planned way towards producing direct or indirect intentional effects on the connections in the societal network, by disparately affecting two or more of the societal domains, having a major direct of 2nd or 3rd degree impact".

INSTEAD OF CONCLUSIONS – HYBRID WARFARE

Because of the difficulties in identifying, understanding and explaining the problems specific to the contemporary social environment, the specialists in the field of social security have resorted to the use of the phrase *hybrid warfare* (Lehaci, 2019, pp. 78-84). Although the term *hybrid warfare* seems fashionable and widely used, it remains difficult to understand it thoroughly and even more difficult to formulate perspectives for resolving a crisis situation in a contemporary societal context. As we have demonstrated throughout this paper, the justification of the nature of the influences between the societal domains can be made according to the relationships that can be described by the model of the network interactions. In this way, the phrase *"hybrid warfare"* can be defined as *"that accumulation of actions directed in a planned way towards producing direct or indirect intentional effects on the connections in the societal network, by disparately affecting two or more of the societal domains, having a major direct of 2nd or 3rd degree impact"* (Ibid.). The disparate impact on the societal domains can occur through low intensity and indefinite duration actions in order to fulfil some goals that are difficult to identify and without the need to trigger the development

of the resilience of the targeted domains. According to the model of the critical infrastructure protection, based on the boundary values (minimum or maximum) necessary for activating the measures of developing the resilience capacity, it becomes impossible to identify and prove the deliberate attack on the social network connections. Instead, by applying the operative art, estimates can be formulated on the statuses expressed and interpreted by approximating the values of the descriptive parameters to the boundary values area. By combining specific methods of critical infrastructure protection with elements of the operational art in the field of military action planning, a new perspective can be obtained on the nature of the hybrid warfare, but also on the crisis phenomenon such as the COVID-19 pandemic. In this way, the analysis of the number but especially of the map of the affected areas, depending on the intensity of the damage, can lead to formulating predictions and developing courses of action based on the situation estimates in order to identify the *"behaviour of the enemy"* and its objectives. By overlapping the *impact plans* expressed according to the links between the contaminated areas and the plans of the network connections between the societal domains, a pertinent picture of the future situations or the new crisis situations different in nature than the pandemic will result. The impact plans may be specific to the interconnected societal domains: political/diplomatic, military, economic, social, critically infrastructural, informational and environmental, and the nature of the hybrid warfare may focus on one of the forms of interaction of two of the societal domains.

The combination of the elements of the mechanisms for developing the resilience specific to each network societal field represents the emergence of new directions regarding the possibility of preventing and counteracting a crisis. The efforts of the security specialists will migrate around the weaknesses of each societal domain, to the weak nodes of the network connections established based on the influences between the societal domains.

The combination of the elements of the mechanisms for developing the resilience specific to each network societal field represents the emergence of new directions regarding the possibility of preventing and counteracting a crisis. The efforts of the security specialists will migrate around the weaknesses of each societal domain, to the weak nodes of the network connections established based on the influences between the societal domains *(figure no. 3)*. Therefore, we can anticipate the possibility of designing that tool for analysing and predicting the future directions of manifestation of an ongoing crisis and even more, the development of a possible treatment scheme based on the improvement of the specific critical situations through doses of compensating the impact on each societal field involved.

However, *hybrid warfare* remains one of the mysteries of modern society, a powerful challenge for analysts, planners, and security decision-makers. Following the operationalisation of the situation estimates (implemented from the operative art) within the threat scenarios (critical infrastructure protection) we consider that new working and intervention tools will be developed for the military action planning in the context of developing resilience in the contemporary societal environment.

BIBLIOGRAPHY:

1. Barabasi, A.L. (2017). *Linked: noua ştiinţă a reţelelor*. Timişoara: Editura Brumar.
2. Chifu. I. (2019). *Decizia în criză*. Bucureşti: Editura RAO.
3. Coşcodaru, I. et al (2013). *S.M.G./P.F.-5 Doctrina planificării operaţiilor în Armata României*. Bucureşti.
4. Dincovici, C. et al (2014). *Manualul privind pregătirea întrunită de informaţii a mediului operaţional*. Bucureşti.
5. Leaua, L., Ardeleanu, D. (2014). *Protecţia infrastructurilor critice – perspective de dezvoltare*. Bucureşti: Editura Academiei Naţionale de Informaţii.
6. Lehaci, N-T. (2019). *Componeneta intelligence în combaterea ameninţărilor de tip hibrid*. Bucureşti: Editura Universităţii Naţionale de Apărare *"Carol I".*
7. Moştoflei, C., Alexandrescu, G., Bogzeanu, C. (2009). *Managementul consecinţelor*. Bucureşti: Editura Universităţii Naţionale de Apărare *"Carol I"*.
8. Robbins, S.R. (1990). *Organizational Theory: Structure, Design, and Applications, Prentice Hall*. New Jersey.
9. Roman, D. (2018). *Protecţia infrastructurilor critice în context NA5CRO*, http://ccpic.mai.gov.ro/docs/directiva114_RO.pdf?uri=OJ:L:2008:345:0075:0082:RO:PDF, retrieved on 6 September 2020.
10. Seiple, C. *Another perspective on the domestic role of the military in consequence management*, http://wearcam.org/decon/victims_videotaped_trough_decon_line.htm, retrieved on 12 September 2020.
11. Stanciu, C. (2016). *Fizionomia operaţiilor militare în mediul de securitate contemporan*. Bucureşti: Editura Universităţii Naţionale de Apărare *"Carol I".*
12. Wade, N.M. (2016). *Counterterrorism, WMD and Hybrid Threat SMARTbook* (Critical infrastructure protection five-step process). The Lightning Press: Lakeland. Florida.
13. COM (2009). Brussels. *Communication from 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.
14. *Council Decision 2007/124/EC*. Euratom on 12.02.2007, Art. 2, lit. b.
15. *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*, Brussels.
16. F.T.-1. *Land Forces Doctrine* (2017). Bucureşti.
17. JP2-01.3 *Joint Intelligence Preparation of the Operational Environment* (2014).
18. *Legea no. 225/2018 pentru modificarea și completarea Ordonanței de urgență a Guvernului no. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice*. Romanian Parliament.
19. *NATO's military concept for defence against terrorism* (2005). Annex A, http://www.nato.int/ims/docu/terrorism.htm, retrieved on 28 August 2020.