Critical Infrastructure Protection in the Knowledge Society: Increasing the Safety Level by Use of Learning based on Wargaming Expertise

Dorel Badea
Department of Management, Faculty of Military Management
"Nicolae Balcescu" Land Forces Academy of Sibiu
Revolutiei Street no. 3-5, 550170, Sibiu, Romania
Phone: 0269432990
dorel.badea@yahoo.com

Marin-Marian Coman
Military Training Center
"Nicolae Balcescu" Land Forces Academy of Sibiu
Revolutiei Street no. 3-5, 550170, Sibiu, Romania
Phone: 0269432990
coman.marian@gmail.com

Dumitru Iancu
Department of Management, Faculty of Military Management
"Nicolae Balcescu" Land Forces Academy of Sibiu
Revolutiei Street no. 3-5, 550170, Sibiu, Romania
Phone: 0269432990
dorin_dan@yahoo.com

Olga Bucovețchi
Department of Economic Engineering,
Faculty of Entrepreneurship, Business Engineering and Management
University "Politehnica" of Bucharest
Splaiul Independenței 313, 060042, Bucharest, Romania
Phone: 0214029100
olga.bucovetchi@upb.ro

Abstract

The linearity of processes is no longer valid only for strictly defined intervals, the decision-makers being forced to explore and exploit other sources and options for imposing a predicted management order in accordance with standards, procedures, policies, etc. Given the socio-technical particularities of organizations that own or manage critical infrastructures with direct implications for risk management activities, it is necessary to conduct theoretical and practical actions for testing their sensitivity by taking in consideration the variation of external factors (geo-climacterics, politics, military, economic factors, etc.) for verifying and validating the decisional variants structured at the operational management level. No matter the level of organizational maturity, the possible solutions for achieving this goal must be optimal from the point of view of the cost-effectiveness ratio and, in the same time, they should converge to a paradigmatic potential for valorizing in a timely and judicious manner the most important component of the organizational capability - the human resource. In this context, the education for sustainability becomes the objective function that needs to be optimized. As a methodological framework for learning and internalizing the procedures that should become an operating standard, the conceptual modeling and simulation are very well suited and the serious games can be chosen as an implementation tool. Therefore, the military organization has been selected as a model of good practice where the training is conducted through simulation and wargaming. When we should analyze the acquisition process of knowledge, the military organization is the proper choice because it offers a series of advantages by the way of transforming the real situation into elements of simulation and by an easy transfer of the gained experience into the real context.

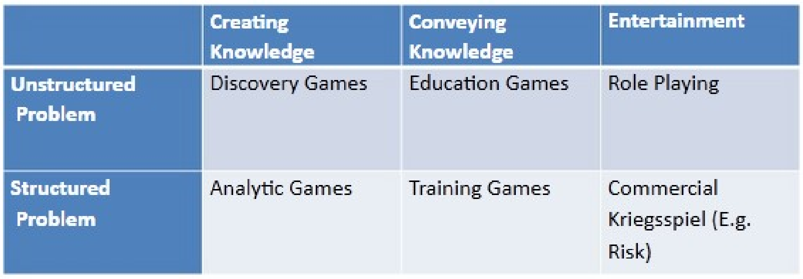
Keywords: Critical Infrastructure, Security, Wargame, Knowledge.

1. Introduction

The design of a research direction for this article, having as a framework the relationship between society, infrastructure, security and sustainability, has among arguments the Cohen approach (2010), who considers critical infrastructures to be something that people depend on, in a direct or indirect manner, at any time, in terms of life and welfare. Unlike this approach, the definitions of critical infrastructure given by different sources from the EU area, refer to the fact that it means an element, a system or a system's component, located within the territory of the Member States that is essential for the preservation of vital societal functions, health, safety, security, social or economic well-being of individuals, and whose disruption or destruction would have a significant impact in a Member State due to the inability to maintain those functions (*** Directive 114/2008). Therefore, ensuring the resilience of the society (understood as a meta-system) is a subject of the utmost importance and actuality for military, civil, public or private organizations (Walker, Cooper, 2011). More than ever, in a non-exhaustive enumeration, concepts such as the Internet of Things, Cybernetics, Process Continuity, Block Chains, and Industry 4.0 are leading the organizations to reconsider the ways to move to higher levels of maturity in terms of sustainability. Based on the complexity, nonlinearity and dynamics of the component structures it is a fact that the relations between the constituent elements are not fully and correctly identified. On the background of the existence of a certain pretension, caused by the manifestation of the gap between the vision of the future and the understanding of current reality, it is more and more obvious that in the knowledge society, the improvement or redesign of critical infrastructure performance (related to the private domain and especially to the public domain) is indissolubly linked to the improvement of the specific information processes' functionality (Denyer, 2017). Taking into consideration the proposed paper's title, the above-mentioned thesis involves fundamental aspects specific to the reaction of organizations to environmental demands, such as: the use of unequivocally specialized vocabulary, the identification of good practices and development methods, the design of appropriate security governance metrics, and last but not least, accountability to ensure critical infrastructure security. In this thematic register, as a basis for providing solid premises to generate added security, the customization of specific elements (common values, competencies, behavior, personnel) comprised in a specialized tool that has a wide applicability in the field of organizational redesign (ex. the McKinsey 7-S model) leads to the necessity of condition fulfilling which is related to the operationalization of an adequate knowledge within holding organizations of critical infrastructure.

It is essential to relate to the differences between knowing and knowledge, as already they were assumed in the literature: “Knowledge is the result of a knowing process at one point. It can be generated, structured and transformed from a form into another form, in a continuous process. Knowledge is a complex combination of conscious and unconscious, rational and irrational, direct experience of life and knowing the life, and the experience mediated in the process of learning.” (Brătianu, 2015, p. 28). Useful supplements in this direction are included in the Dictionary of Management as a reference work to demonstrate the level of theoretical and practical development of this discipline at the national level (Nicolescu, 2011). After presenting knowledge as assemblies of applicable information and abilities generated by the receiver following the use of information, which has the capacity to generate added value by using them, the two components namely the human and the economic dimension are emphasized. In accordance with the research objectives of this paper, the explanation given to the human dimension of knowledge draws attention. In this regard, it is emphasized the fact that a certain information to a particular person with a certain type of training and skills is used appropriately and generates added value, and the same information is only a simple information to a less competent person.

The issue of resources committed to generating paradigmatic value knowledge is in no way devoid of importance. The problem has mild contradictory aspects in the public sector, where, under specific budget constraints, a certain level of performance is required involving computer network-based technical solutions, using a specialized software, training, generically combined under an e-administration dome or even e-government. All this means a large amount of financial resources for the creation of such administrative infrastructure. Assuming an optimal dimensioned budget allocation, the starting point to be achieved as a fundamental criterion is the professionalization of the human resource. In this regard, the use of expert systems or specialized IT technologies raises the cost of knowledge, which should take into account the imperative of human presence and the minimum skills needed to set up adequate inputs to the learning objectives, with further influences on outputs and outcomes. In this context the mixed solutions seem to be the most desirable for the use and implementation for knowledge generation and knowledge transfer processes (Paiano, Caione, & Guido, 2015). In the sense of the conceptual approach mentioned above, the mixed solutions leave a sufficient and flexible actionable freedom, both for the object of the training and for the ways of using the tools in different situations from the point of view of the complexity of the replicated aspects of reality (Figure 1). In such a context, the organizational learning takes new valences (Treapat, Gheorghiu, 2017), in the sense that it is internalized through employees, but it is not simply a sum of individual learning outcomes, becoming an essential process for adaptability to the requirements of the macroeconomic environment.



	Creating Knowledge	Conveying Knowledge	Entertainment
Unstructured Problem	Discovery Games	Education Games	Role Playing
Structured Problem	Analytic Games	Training Games	Commercial Kriegsspiel (E.g. Risk)

Figure 1. Connections between types of knowledge and the use of gaming concept.
(source: A Compendium of Wargaming Terms (Updated 7 July 2015) Compiled by William L. Simpson Jr – http://www.mors.org/Communities/CoP- Document-Search
http://www.mors.org/Communities/CoP- Document-Search The Art of Wargaming by Peter Perla)

The wargaming concept is recognized as a dual use tool (military and civilian purposes) with broad applicability (Figure 2) especially in the military field (it also supports the experimentations *what if* type). The concept itself created an entire industry (with both intensive and extensive achievements, as well as complexity and addressability), Warren Wiggins arguing in this respect: “There are multiple reasons for the use of war games; discovery, examination of concepts, and even learning. The value of the war game is to create an enabling environment to achieve the desired objective(s). The benefits of a war game are numerous; however, for the most part they provide new ways of conceptualizing the problem, new courses of action, new elements of information needed for decisions, previously unknown relationships between aspects of a problem, understanding of the problem’s dynamics.”[1]

An interesting addition to the use of dynamic term is the one made by The Goldsworthy, Stolk&Associates, which highlights the fact that a conflict is not solely kinetic. “Conflict is always the outcome of many societal dynamics. Acknowledging those dynamics it is crucial to ensure a realistic simulated operating environment. GS&A have applied wargaming within various contexts: ministerial, NATO, universities and civil security.”[2]

Finally yet importantly, it is useful to mention David Schroeder's approach that highlights the importance of wargames in both military and business environments. Given the current development conditions of the various public or private areas of activity and based mainly on IT and related vectors, the wargaming concept is applied with a strong tradition of use in the military field (there is already a wargaming book edited in 2017 by the UK MoD that has the role to be a reference guide for all practitioners - *Wargaming Handbook*, and a dedicated annual conference - *Connections US Wargaming*

[1] https://www.csiac.org/wp-content/uploads/2016/12/CSIAC_Journal_V4N3_Nov2016.pdf
[2] https://www.goldsworthy-stolk-associates.com/?lightbox=dataItem-j66ficzt

Conference). Thus, it could be argued that the applied wargaming as a "discipline" is still in a full maturity process, there being no consensus between different specialists (military, security, education, and human resources experts, psychologists, sociologists, software development engineers, etc.) on the main directions to be investigated and the proper ways of better implementation of the results at the organizations level. Taking into consideration the general way of developing a working terminology, regardless of the type used (education, training and analytics), the wargaming is a component of the decision making process done under conditions of uncertainty, that generate the courses of actions (decisional variants) which are analyzed in the context of an emerging situation. This situation is based on a tailored scenario of which the participants are aware, that is applied sequentially and managed in a logical succession, based on the rules known by all participants.

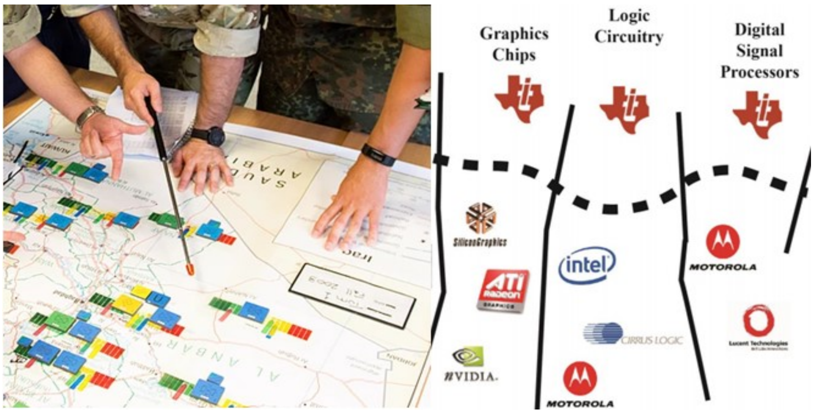


Figure 2. Ways to conceptualize wargaming in the military and IT business field.
(sources: https://www.goldsworthy-stolk-associates.com/?lightbox=dataItem-j66ficzt; http://professionalwargaming.co.uk/ConnectionsKeynote.pdf)

The training exercise, which took place in 2017 in the USA called "Navy Private Sector Critical Infrastructure War Game" is an eloquent example of good practice in field of critical infrastructure. The exercise has been conducted by involving a number of 125 players from 14 critical infrastructure sectors, that covered a wide spectrum of representativeness from public and private field: "In our war game, the attacks that were most likely to escalate to a national security incident were those on the civilian nuclear sector and sectors that had strong linkages across the national economy. Attacks on these sectors with strong linkages within the rest of the critical infrastructure created cascading effects, many of which had life or death implications beyond the initial scope of the cyberattack. Therefore, results from the war game suggest that U.S. government resources and policies should focus on the energy, transportation, communications, water/wastewater, and nuclear sectors."[3]

2. Methodology

Before presenting the solution to be implemented, it is adequate to emphasize a way that shows how the practitioners should use for training a special purpose scenario. The *Red Teaming Guide,* edited by UK DoD highlights the idea of using the red team operational thinking way in order to provide to the training audience the support for a productive training: "The idea of using red teams has been around for a long time. Commercial enterprises, such as IBM, and government agencies such as Defence Intelligence and the Central Intelligence Agency, have long used them to reduce risks and to improve their problem solving."[4]

[3] http://www.nwcfoundation.org/Files/Admin/Corp%20Logos/Navy-Private%20Sector%20Critical%20Infrastructure%20War%20Game%20Report%20%281%29%20%282%29.pdf

[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/142533/20130301_red_teaming_ed2.pdf

Usually, for a specific scenario map, the use of colors for mapping the symbols to denominate the type of party is common in military wargaming and terminology. Blue generally denotes own forces, red is for threat, green is often used to denote indigenous security forces and brown for other actors such as non-governmental organizations and the civilian population etc.

The training events based on a proper tailored scenarios can provide knowledge and abilities to practitioners related to physical protection, cyber security, cyber and physical convergence, industrial control system, information about insider treat, standards and ways to command and control, ways to counteract, etc. All of these have as training purposes the improvement of awareness, capacities to respond, build trust communities or sharing knowledge. Typically, the training audience will follow three phases for solving the problem/the crises: diagnosis phase (key assumptions, identify and question assertions, logic mapping, information check, etc), creative phase (role playing, brainstorming, what if analysis, indicators for changes, experimentation, etc.), and challenge phase (analysis of competing hypotheses, devil's advocacy, etc.).

3. Proposed solution and problem solving steps

The training event offers a framework that allows to all participants a way of working and collaborating with each other in order to apply the wargame rules for a worthwhile dialogue concerning decision-making process after reviewing case scenarios. Moreover, such a training event has to be combined or connected with other kind of training events to maximize the reach of training objectives linked to value-based decision making.

Eubella Alert is a fictitious scenario that has an imaginary situation in an imaginary setting with all other aspects being invented to achieve the exercise objectives and training objectives. The scenario is based on a major event - a cyberattack on an energetic control system, which can affect the majority of the critical infrastructure sectors. In addition, the scenario is enriched with a physical break of security (bomb threat) at an important nuclear plant belonging to a country that is part of a union, which has promulgated a common security policy regarding the energy sector.

The GOLDEN UNION (GU) located in the central EUBELLA continent has been founded in 1992 (Figure no. 3). GU comprises six neighboring countries (ROZY, TANNY, GREENH, YELLOWE, PURPLET, and TANA), which are parliamentary democracies and a federal governance system applies to all the political and economical voted policies related to the development of the union. On one hand, the GU has its own federal government, thus on the other hand, each constituent country has a national government that has to apply the internal policies in supporting their citizens welfare. The official language recognized by the GU federal govern is *Goldish language* spoken almost in majority large cities of the union. Even so, in some cities and areas from the GU countries, the population has the tendency to preserve their local habits and traditional language. The process of suburbanization and urban decentralization lead the GU citizens to have a good life. Over time, there have been popular movements for independence in some areas, the majority of them based on ethnicity issues, culture, religion, and preservation of traditional language.

Three years ago, GU promoted a new energy policy, called GREENY2015-2025, which led to a GDP's growth of the union with 20% more in the last year than in the previous one. The majority of countries from GU have natural resources and their economies are emerging.

GU is located on the central area of EUBELLA continent. Around the union are located other emergent countries, each of them trying to apply the balanced economic policies for developing the trading and market exchange with their neighborhood countries and with union countries.

The energy systems from countries inside the EUBELLA continent is based on traditional ways of obtaining the energy, however some of them are based on nuclear energy. The traditional economic development of the region, in terms of energy system, is based mainly on the oil and natural gas import and export trading. The alternative energy solutions (solar photovoltaic energy, solar thermal energy, wind energy, biomass energy, etc.) are emerging and some of the countries have implemented standards for developing them.

REDIA, a large country located in the northeast area of the continent, is one of the richest countries having a large amount of crude oil and natural gas reserve. REDIA commercializes its abundant natural resources to other countries from EUBELLA continent that do not have enough natural resources to produce the desired amount of energy necessary for the industry field or residential energy for population. The transportation system for oil and natural gas is in a developing and modernization phase. The main transportation pipeline, STREAM ALPHA 1, starts from REDIASHT city, one of the largest cities from REDIA, located at 100 km away from international border with GU. Then, STREAM ALPHA 1 goes through ROZY country territory and splits to the other countries that have trade agreements with REDIA for natural gas and oil import. (see Figure 3)

The last GU Resolution102, voted by the federal govern and endorsed in 2015, established a well-balanced policy regarding the trade of resources inside the union neighboring countries. Resolution102 supports the energy policy GREENY2015-2025. Moreover, after signing that important document, each country designated a maneuver brigade in order to form the *Golden Union Division Army* (GUDA) as a very versatile and deployable maneuvering unit along of the GU territories and international borders.

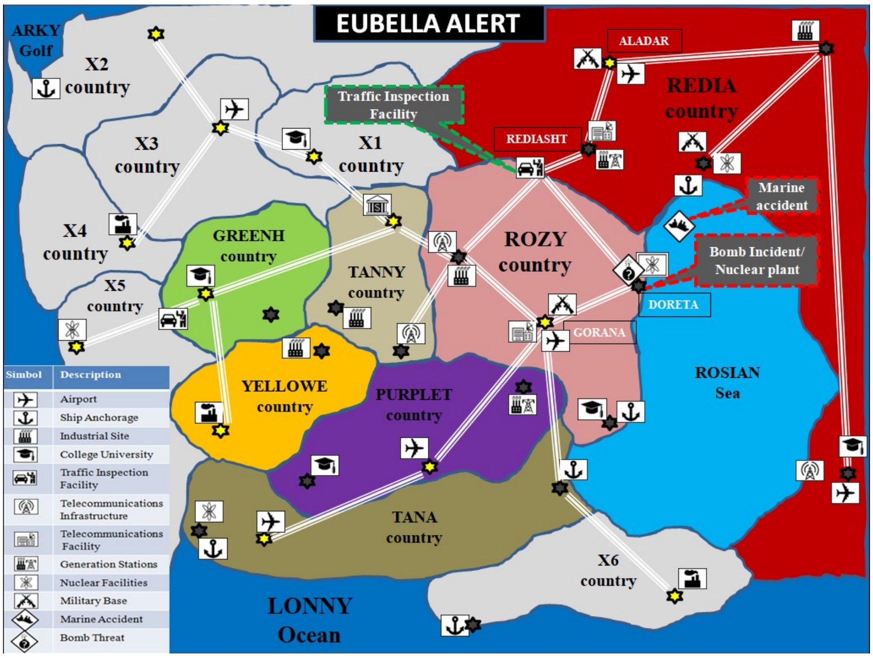


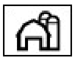
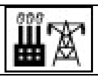
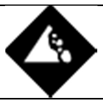
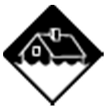
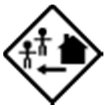
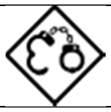
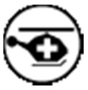
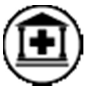
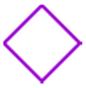
Figure 3. EUBELLA ALERT wargaming scenario map

After implementation of the energy policy GREENY2015-2025 and the Resolution102, all countries from GU started to cut down the amount of crude oil and natural gas import from REDIA. This fact, led to a real decrease of REDIA GDP and political frictions appeared between REDIA and GU countries. In addition, in the last 2 years, there were some sabotage events against main transportation pipeline STREAM ALPHA 1. The LIBERTY PANTHER GROUP (LPG) from GU that Figurehts for freedom of energy systems has claimed the sabotage events. Consequently, REDIA started to strengthen its defense system and military combat power by developing new weapon systems and a professional army. Many funds were invested to develop cyber security domain and a series of hybrid threat designed training exercises were conducted near international border of GU. On the other side, in the last year, ROZY country from GU had for three times emergency situations that were linked to bomb threat events against its nuclear plant located in the vicinity of DORETA city. The nuclear plant was built in 2012 near ROSIAN SEA, close to REDIA, and it assures 30% of the amount of necessary energy specific to energy system of the country.

Based on the tailored wargaming scenario, the training audience will make use of symbol list in order to portray on the exercise map the following elements: infrastructures, natural events, incidents, operations, and damage/operational symbology (Table 1).

Table 1. Extract (examples) from a symbol list to be used within Emergency Management process and First Responder communities at all levels of need

(sources: Symbology Reference, version 2.20, Released: September 14, 2005, https://www.fgdc.gov/HSWG/index.html; https://www.fgdc.gov/HSWG/ref_pages/PrintableChanges.htm)

SYMBOL TYPES/ SYMBOL CLASSES	SYMBOL IMAGE	SYMBOL TERMS AND DEFINITIONS
Infrastructures Symbology - examples (83 symbols)		
Agriculture and Food Infrastructure (Theme)		Production and retail services of foodstuffs.
Generation Stations (Energy Facilities Feature)		A facility equipped with special equipment used for the production of heat or electricity.
Natural Events Symbology - examples (27 symbols)		
Landslide (Geologic Feature)		A general term for a wide variety of processes and landforms involving the down slope movement under the force of gravity of masses of soil and rock material.
Flood (Hydro-Meteorologic Feature)		A relatively high stream flow that overtops the stream banks in any part of its course, covering land that is not normally under water; condition that occurs when water overflows the natural or artificial confines of a stream or other body of water, or accumulates by drainage over low-lying areas.
Incidents Symbology - examples (50 symbols)		
Civil Displaced Population (Civil Disturbance Feature)		Persons or groups of person who have been forced or obliged to flee or to leave their homes or places of habitual residence, in particular as a result of or in order to avoid the effects of armed conflict, violations of human rights, or natural or human-made disasters.
Criminal Activity Incident (Theme)		An unlawful pursuit or action in which an individual participates.
Operations Symbology - examples (46 symbols)		
Medical Evacuation Helicopter Station (Emergency Medical Feature)		The locus of an emergency helicopter landing pad, utilized to transport severely injured persons.
Health Department Facility (Emergency Medical Feature)		The locus of a facility operated by a public institution which is dedicated to the promotion of health and the prevention of disease at the community, country, state, or national level.
Damage/Operational Symbology - examples (10 symbols)		
Incident (Damage/Operational) No Levels		Not Applicable
Operation (Damage/Operational) Level 2		Operational, but filled to capacity or otherwise closed.

After the mapping process with all the scenario symbol elements portrayed on the exercise map, the training audience can apply the ways of thinking as for Red Teaming methods for identifying and assessing the assumptions, alternative options, vulnerabilities, limitations and risks for the organization. These solving methods are suitable for reacting to a crisis, in order to take in account all unpredicted situations, deepen the critical analysis, make predictions, and develop feasible courses of action (COA) (Figure 4).

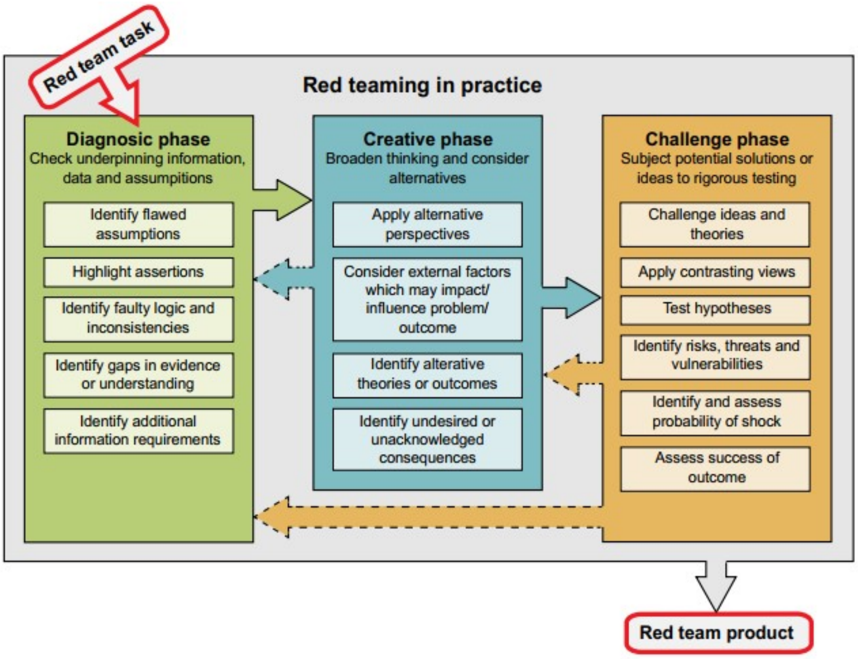

Red team task
Red teaming in practice
Diagnosic phase
Check underpinning information, data and assumpitions
Identify flawed assumptions
Highlight assertions
Identify faulty logic and inconsistencies
Identify gaps in evidence or understanding
Identify additional information requirements
Creative phase
Broaden thinking and consider alternatives
Apply alternative perspectives
Consider external factors which may impact/ influence problem/ outcome
Identify alterative theories or outcomes
Identify undesired or unacknowledged consequences
Challenge phase
Subject potential solutions or ideas to rigorous testing
Challenge ideas and theories
Apply contrasting views
Test hypotheses
Identify risks, threats and vulnerabilities
Identify and assess probability of shock
Assess success of outcome
Red team product

Figure 4. A logical way of thinking (framework) specific to a red teaming during the wargaming event (source:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/142533/20130301_red_teaming_ed2.pdf)

In order to run in an efficient manner the entire training with great outcomes, the training audience must put in practice the best COA to solve any unpredicted situation which could appear during the wargaming process. The teams should have to assess very well all the information received through the scenario, but usually they will try to evolve in their way of thinking and information assessing to enhance the level of awareness. Besides critical thinking for analysis of current situation and future implications, additional useful information could be provided by the role players who act in accordance with established training objectives. Doing that, the common operating picture (COP) will be clear enough for all participants and the effect will result in good countermeasures conducted in accordance with the development of the operational situation during the crisis.

A better way of assessing information is by making use of the degrees of confidence specific to reliability of source and credibility of information, but they must be considered independently of each other. (table 2) As a result, a combination of letter and number will be appropriate for information assessing process. Thus, information received from a "fairly reliable" source, which is adjusted as "possibly true" will be rated as "C3". This way of analysis and thinking is very useful for training audience (Threat Assessment Team) when dealing with scenarios that emphasize an immediate crisis, like an imminent terrorist attacks in urban areas (a bomb threat in the vicinity of a crowd, a bomb placed in a critical infrastructure building) that could result in a mass casualty event. Consequently, an emergency planning response must be implemented very quickly.

Table 2. Definitions of reliability of source and credibility of information (source: http://eturwg.c4i.gmu.edu/?q=node/128)

Reliability of Source (designated by a letter between A and F signifying various degrees of confidence)		
C	Fairly reliable	Refers to a source which has occasionally been used in the past and upon which some degree of confidence can be based
Credibility of Information (designated by a numeral between 1 and 6 signifying varying degrees of confidence)		
3	Possibly true	If, despite there being insufficient confirmation to establish any higher degree of likelihood, a freshly reported item of information does not conflict with the previously reported behavior pattern of the target

During the wargaming conduct, a main events list-main incidents list (MEL-MIL) will be employed. The purpose of MEL-MIL is to create challenging situations for training audience in order to meet training objectives of the exercise. The incidents will be injected as the situation develops and they will follow a logical evolution of the crisis in order to enhance the training audience's COP. In this manner, all the participants have to contribute with their expertise to solve all the incidents through a collaborative work by taking all necessary countermeasures that result in an emergency response planning.

The after action review (AAR) is mandatory to be conducted at the end of each wargame event. As a tool to get maximum benefit from every training session, AAR is a facilitated discussion conducted for discovering and learning what happened and why, focusing on performance standards, that actively involves the training audience in order to allow to all participants to become conscious about their gaps in training for future improvement on weaknesses or for sustaining their strengths.

4. Conclusions

At the national level, there is a shortage of updated professional approach in relation to the international practice of the critical infrastructure security issue (ex. USA, Canada, Australia, Germany etc.). Although, as a declarative argument, the main idea from the official document regulating the long-term activity related to critical infrastructure, stipulates that: "The economic and social development stimulated by the accelerated technological progress and the phenomenon of globalization have strengthened the strong interdependence and interaction of the systems that ensure the security and welfare of the human society. The need to interconnect systems against the backdrop of the trend of removing administrative barriers and access to new emerging markets, along with the integration of infrastructure networks, leads to global security and stability developments." (*** National Strategy on Critical Infrastructure Protection, 2011, p.10)

The starting point in writing of this article relies on the fact that the organizational proactive processes, as valuable resources, are based on a flexible learning process. These resources ensure the sustainability of public and private capacities, civil and military alike, and are coupled to the challenges of a highly dynamic macro-environment, which are characterized by uncertainty, ambiguity and volatility. In this context, asymmetric threats and especially hybrid threats, containing a complex information vector with different intensities, influence the social functionality in different basic areas such as medical services, food, defense, energy, administration and governance, communications, etc. The recent events fully demonstrate the thesis which states that the security has not only a black and white spectrum, but also gray hues, with interdisciplinary and cross-border nuances becoming the points of interest, both through the induced vulnerability potential and the means of provocation that surpass the strictly specialized military area.

Conducting the experimentation process type "what happens if" is a very costly and risky one from the perspective of actual way of carrying out, aspect which has at least the same intensity also for the critical infrastructure field. The expertise of this type of training in the military domain is accepted and the learning and education process for the security of the assets must be an effective and flexible one, built on the formulation, activation and/or updating of some mental models. The research team draws attention to the exploiting of predefined symbols, which are also employed in the military operational planning, as a less-used idea in the critical infrastructure literature, and the completion, where appropriate, with new ones. These symbols could be used for the graphical materialization of risk situations regarding the safe operation of a critical infrastructure system, according to a proper tailored scenario, in a training exercise of public authorities or private operators with responsibilities related to the management of crises based on disasters.

A special role in the process of improving knowledge dedicated to increasing the level of security of critical infrastructure must be played by the educational, military and civil institutions, through special programs dedicated to the public sector that is involved in the management of critical infrastructure issues (postgraduate courses for further training or specialization, master programs, etc.). In the knowledge of economy, universities face new challenges and they have to adapt to the new contexts. First, knowledge life cycle is decreasing and the focus of teaching and learning processes should shift from knowledge transfer to the students toward developing thinking skills (Bratianu & Vătămănescu, 2016). Through this paper it is proposed, that the tool presented as a solution for learning in the field of critical infrastructure be implemented for testing and validation within a postgraduate program conducted in the Land Forces Academy of Sibiu and within a master program conducted in the Faculty of Entrepreneurship, Business Engineering and Management/ University Politehnica of Bucharest. It is a good thing, in the sense of the above-mentioned, the fact that people are more and more aware of the role of knowledge, as an engine of generating performance in the field of security of critical infrastructures. An example supporting this statement is also one of the conclusions that emerged from the Zagreb Forum in 2017 - Resilient Critical Infrastructure (2nd Zagreb Security Forum), which encourages the application of the "knowledge for development" paradigm as the foundation for designing critical documents on the protection of National Critical Infrastructures. (https://www.zagrebsecurityforum.com)

The critical infrastructure security is a topic whose approach is achieved by taking into consideration both officially validated regulations and the level of maturity of the population's ability to objectively raise the awareness related to the main mechanisms of causes and effects specific to malfunctions that could emerge at any critical infrastructure. Based on the above assertion, the main purpose of this applied research operationalized by predominantly qualitative means is the demonstration of viability of methodological framework provided by the wargaming procedures that can be exploited in a specific way also for critical infrastructures issues. In order to preserve the integrity of the real system framework, the focus was on a few variables - actors, rules, resources - that have been considered by authors the most important factors of the research. Finally, it is brought to the attention of public authorities and all institutions involved in the management of critical infrastructure security, a feasible possibility of using a flexible and effective training method based on wargaming methodology that can be developed in an integrating way at the national level, which is in fact the added value of this paper.

References

Cohen F. (2010). What makes critical infrastructures Critical?, International Journal of Critical Infrastructure Protection, 3, 53-54.

Bratianu, C. (2015). Gândirea strategică, București: Editura Pro Universitaria.

Bratianu, C., & Vătămănescu, E.M. (2016). Students' perception on developing conceptual generic skills for business. In Moffett, S., & Galbraith, B. (Eds.), Proceedings of the 17th European Conference on Knowledge Management, Reading: Academic Conferences and Publishing International, 101-108.

Denyer, D. (2017). Organizational Resilience: A Summary of Academic Evidence, Business Insights and New Thinking. BSI and Cranfield School of Management: Cranfield, UK.

Paiano, R., Caione, A., Guido, A.L. (2015). Business Process Management - A Traditional Approach versus a Knowledge Based Approach. BRAIN-Broad Research in Artificial Intelligence and Neuroscience, 6(1), 54-69.

Treapat, L. & Gheorghiu, A. (2017). Artificial Systems and Models for Risk Covering Operations. BRAIN-Broad Research in Artificial Intelligence and Neuroscience, 8(1), 59-72.

Walker, J. & Cooper, M. (2011). Genealogies of resilience: From systems ecology to the political economy of crisis adaptation. Security Dialogue, 42(2), 143-160.

***Strategia națională privind protecția infrastructurilor critice, MONITORUL OFICIAL AL ROMÂNIEI, PARTEA I, Nr. 555/4.VIII.2011

http://eturwg.c4i.gmu.edu/?q=node/128, accessed in april 2018.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/142533/20130301_red_teaming_ed2.pdf accessed in june 2018.

https://www.fgdc.gov/HSWG/index.html accessed in july 2018.

https://www.zagrebsecurityforum.com accessed in june 2018.
http://www.nwcfoundation.org accessed in july 2018.

Assoc. Prof. **Dorel Badea** graduated the Military Technical Academy of Bucharest in 2002 and received the Ph.D. degree in Industrial Engineering (2011) from Technical University of Cluj-Napoca, currently being head of Management Department in "Nicolae Bălcescu" Land Forces Academy of Sibiu. He is holding courses in defense resource management, modeling and simulation of military actions and critical infrastructure protection. He wrote over forty essays issued in different scientific specialized reviews and proceedings on general management, military engineering and security.

Assoc. Prof. **Dumitru Iancu** is vice dean for scientific researcher at the Military Management Faculty, "Nicolae Bălcescu" Land Forces Academy of Sibiu. He holds a PhD in Management from the Lucian Blaga University of Sibiu (2011). His research interests include human resources management and applications of general management theory in security technology systems. He is author and active participant at different international conferences and participated at many activities at national level related to research and innovations strategies necessary to be implemented.

Senior Trng. Instr. **Marin-Marian Coman** is PhD Student in Industrial Engineering at University Politehnica of Bucharest and graduated "Nicolae Bălcescu" Land Forces Academy of Sibiu (2000). He holds a M.Sc. in Management and Technology at the same military university (2015) and a M.Sc. in Science and Computer Engineering (2013) at "Lucian Blaga" University of Sibiu. He collaborates with members of NATO Modeling and Simulation Group and his main areas of interest include operational planning and exercises and conceptual modeling of spatial critical infrastructures.

Assoc. Prof. **Olga Bucovețchi** received her BSc in Economic Engineering (2006) and PhD in Industrial Engineering (2014) from University Politehnica of Bucharest. Now she is assoc. prof. at University Politehnica of Bucharest. She is member of Association of Economist Managers and Engineers in Romania and Romanian Association for the Promotion of Critical infrastructure and Services Protection. While working at UPB she had several collaborations within national and international research projects related to risk management, critical infrastructure protection and business continuity.