THE DESIGN OF A DIDACTIC GAME (CIP-v.01-THD) FOR CRITICAL INFRASTRUCTURE SECURITY MANAGEMENT

Dorel BADEA*
Cezar VASILESCU**
Marian COMAN*

*"Nicolae Bălcescu" Land Forces Academy, Sibiu, România
**The Regional Department of Defense Resources Management Studies, Braşov, România

The motivation of addressing such a topic has as argument to ensure, educationally speaking, the best connection to the real aspects of critical infrastructure issues. We considered that there are postgraduate training programs at national level, which must implement case studies, in view of achieving the purposes resulting from the curriculum, as close to reality, by replicating some sensitive aspects of the relevant decision, which meet the training needs of students, in accordance with occupational standards. Being a complex area, the challenge is to best select the most relevant aspects to be played in terms of teaching, in a manner beneficial to the finality of integrating the system, technical and operational perspectives.

Key words: *critical infrastructure, security, education, game*

1. GENERAL CONSIDERATIONS

While exploring reality differently, at least two examples of best practices can be mentioned that were the inspiration in the field of security and defense in this case, made in prestigious educational institutions.

Internationally, the USA, at the Naval Postgraduate School, there is CyberCIEGE game [1] that includes tutorial movies illustrating information assurance concepts explored by the game, from one simple training sequence (How do you know if the system is secure?) to a complex end (Deciding who we are willing to communicate with, and the protection we want for that communication).

At national level, at the Regional Department of Defense Resources Management Studies (DRESMARA) there is an application of Defense Planning and Defense Resources Management - The Republic of AMRA, by which the translation of theoretical concepts is achieved,

from strategic to operational level, starting from a specific situation given by the regional security environment, for hypothetical states. For a substantial framing of this topic, a broader concept should be considered, that of serious games, explained since 1970 by studies conducted by Abt, C.C. [3], a precursor of the domain, as follows: "*These games have an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement. This does not mean that serious games are not, or should not be, entertaining." We can define game in a more conventional way as follows: a game is a context of rules where a group of rivals try to achieve their goals. We are interested in serious games because they are fun and have an explicit educational purpose which has been planned carefully*". For the 21st century, according to IT technologies, the simulation part is increasingly associated to the concept (fig. 1), achieved using the dedicated software. The classical, non-computerized component is approached in this paper, insisting on the transfer of expertise in the field concerned.

Fig. no. 1. *Content of the serious games concept* [4]

2. THE SOLUTION PROPOSED

The game is intended to be applied to laboratory and workshop activities for subjects in the area of critical infrastructure (CI abbreviation will be used). Two teams of 5-6 students are formed, whom are distributed a worksheet (Table 1) with the initial situation (the same) of the level to ensure the protection of critical infrastructure (ps% abbreviation will be used), based on the assumption that a 100% level of assurance cannot actually be achieved.

Table 1. *Initial situation regarding critical infrastructure security*

IC	Transports (T)	Energy (E)	Communications and IT (C)	Health (H)	Water supply (W)	Chemical industry (Z)
ps%	90	92	93	90	91	92

Presentation of the initial scenario (**step 1**) can be done using a written format or through a report distributed via a video or combined display to achieve a high degree of awareness of the situation, depending on the level of training, professional experience, expertise in the field, etc. (fig. 2).

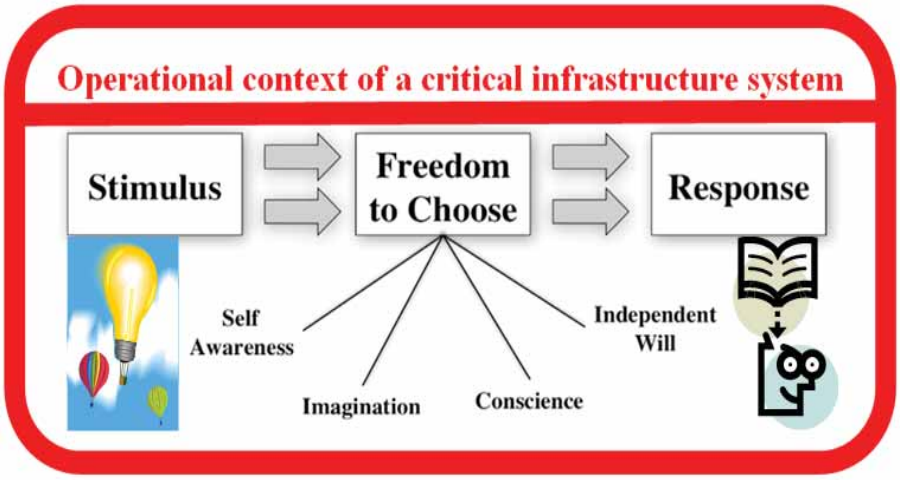

Fig. no. 2. *The general approach to a critical infrastructure situation* (adaptation after [5])

Such an example of content may be as follows.

Theodoria region is located in the central part of the XLand state, constituting a national development engine. With an area of approximately 1,500 square kilometers and a relief mostly piedmont, crossed by two rivers with an average flow rate on which a local hydroelectric power station was established (at the confluence), the region is crossed by a railway line and a national road connecting three urban settlements. In the regional development strategy for the period 2015-2025, the merging of certain rural settlements is provided, to become neighborhoods of major existing cities, in a general framework of strengthening the economic, social and political independence to neighboring countries characterized by fragile security environment. This would also strengthen efforts to redevelop flood embankments given some physical and climatic events occurred in the last two years, especially during mid-spring. Moreover, it is intended to start modernization projects of the water supply plant and Chemical XSA factory within the area, both being constructed 40 years ago, as an integrated system, given the need for water flow cooling of special equipment of the factory. Currently, representative for the region are the public radio and a large private television specialized in news and political-military analyses, the regional hospital and services in the area of alternative energy and IT, the solutions provided by the latter on a contractual basis to the local authorities and the Committee for emergencies being a real success, recognized for the performance.

To create an image with a better perception of the initial situation, a map was carried out, using ArcGIS environment (fig. 3).

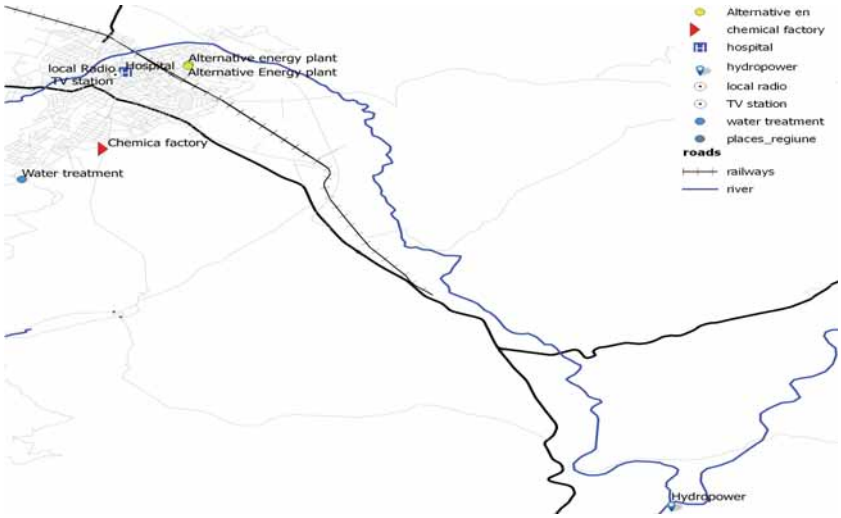

Fig. no. 3. *Modeling of initial core elements through ArcGis software*

After disclosing the scenario, the two teams will be assigned the necessary time (approximately 30 minutes) to establish responsibilities and the preliminary analysis, focusing on highlighting interdependencies of identified critical assets. Depending on the complexity sought to be replicated, teams will be formed (training targets), the optimal solution to this situation being to have one responsible for each critical infrastructure sector (see table 1) and a general manager of security. Students are free to take roles within the team and will carry out the activities in different rooms, the instructor monitoring the activity.

Further on (**step 2**) it is announced, based on the history of previous risk events specific to the region and the given current context, the possibility of the occurrence in the future of threats. For example, we chose this: flooding due to heavy rainfall regime caused by a major storm, code red for a day (36%); escalation of conflicts on the southern border with the use of cyber-attacks against the administrative center of the region (30%); a storage facility explosion of liquid ammonia from the chemical plant (34%). These are the three events that will be considered, in random order, explaining the specific context of the event. Teams have 15 minutes after announcing a preliminary analysis of possible situations to take action (what if) on the structure of infrastructures, given the existing level of security.

Subsequently, it is explainable that they have at their disposal a credit of 20 useful (values of the

measures that will need to be applied after the manifestation of each threat, to increase security of managed infrastructures), gradually (no more than 7 for each stage) and not more than 4 for a critical infrastructure. Security arrangements must be applied to each stage at least for three infrastructures.

It is shown that the exercise's score will be calculated according to the level of performance achieved in securing critical infrastructure by the formula:

$$\mathbf{PS} = \mathbf{T} * 0{,}08 + \mathbf{E} * 0{,}20 + \mathbf{C} * 0{,}35 + \mathbf{H} * 0{,}15 + \mathbf{W} * 0{,}12 + \mathbf{Z} * 0{,}10$$

wherein the values of T, E, C, H, W and Z are those in the worksheet at the end of round three. On equal scores of the two teams, the tie-break criterion will be the score achieved at the end for C.

There is, from **step 3 (45 minutes)**, the introduction of threats. For the first round, threat number three will be replicated, as follows: on April 5th, 2017, at 12.12 there was an explosion in a tank for storing liquefied ammonia from the chemical plant, following the execution of maintenance operations without full compliance with standard operating procedures and due to overload. According to preliminary data provided by the radio station, 30 people died and over 175 were seriously intoxicated and an area of 2.5 km^2 was contaminated. The committee for emergency situations called for the mobile team of volunteers to supplement the efforts of the medical team and for the local transport administration to replace reconstruction efforts after the event, by providing means of transportation, and it warned about the consumption of water for the population. The teams have received the first incident, analysed it and took the necessary actions (15 minutes) to increase the security of critical infrastructure (Table 2), based on all data provided in the three stages and the perception of events.

Table 2. *Situation regarding critical infrastructures security after the first incident*

IC	Transports (T)	Energy (E)	Communications and IT (C)	Health (H)	Water supply (W)	Chemical industry (Z)
Team *I*						
ps% 1	90	92	93	90+2	91+2	92+3
Team *II*						
ps% 1	90+1	92	93	90+1	91+1	92+4

For the second round of stage number three, teams are put before the following situation. Heavy rain which brought up to 90 liters per square meter caused a flood in central region, the hydroelectric energy station operating on emergency procedure due to the alarming increase level in the water storage tank. Amid the rain storm and lightning, the north wing of the hospital was caught by fire that forced the relocation of patients in other areas of the hospital unit. Adverse weather conditions caused the collapse of the three pillars of electricity, public radio station, water treatment and 568 households remained without power for four hours. In a short time, firefighters, aided by the engineer battalion in the region have put in place several motor pumps and a machine to help strengthen a dike. The intervention with special vehicles for firefighting and first aid to flood victims was hampered by the mostly impracticable state of the county road. Measures implemented by both teams led to the situation presented in Table 3.

Table 3. *Situation regarding critical infrastructures security after the second scenario*

IC	Transports (T)	Energy (E)	Communications and IT (C)	Health (H)	Water supply (W)	Chemical industry (Z)
Team *I*						
ps% 1	90	92	93	90+2	91+2	92+3
ps% 2	90+1	92+2	93+2	92+1	93+1	95
Team *II*						
ps% 1	90+1	92	93	90+1	91+1	92+4
ps% 2	91	92+3	93+3	91	92+1	96

For the second round of stage three, teams are faced with the scenario of a cyber-attack. Given the deterioration of external security environment, intended to attract in Theodoria conflict region, on the weekend preceding the National Day celebration, through intensive and extensive information actions, websites of central government of the private television were affected, their networks being temporarily taken out of service. The television's servers were blocked and as for the electricity supplier, the automated management systems of semi-active redundant operation have stopped working. At the regional hospital administrative activities that required the use of the computer networks were now made on paper and C4 network with the emergency committee is inoperative. Critical infrastructure security measures operated by the two teams led to the situation presented in Table 4.

Table 4. *Situation regarding critical infrastructures security after the third scenario*

IC	Transports (T)	Energy (E)	Communications and IT (C)	Health (H)	Water supply (W)	Chemical industry (Z)
Team *I*						
ps% 1	90	92	93	90+2	91+2	92+3
ps% 2	90+1	92+2	93+2	92+1	93+1	95
ps% 3	91	94+1	95+4	93+1	94	95
Team *II*						
ps% 1	90+1	92	93	90+1	91+1	92+4
ps% 2	91	92+3	93+3	91	92+1	96
ps% 3	91	95+1	96+4	91+1	93	96

Applying the calculation relationship of the final security level, we obtain:

$$PS\,I = 91 * 0{,}08 + 95 * 0{,}20 + 99 * 0{,}35 + 94 * 0{,}15 + 94 * 0{,}12 + 95 * 0{,}10 = 95{,}81$$

$$PS\,II = 91 * 0{,}08 + 96 * 0{,}20 + 100 * 0{,}35 + 92 * 0{,}15 + 93 * 0{,}12 + 96 * 0{,}10 = 96{,}04$$

Hence it results that the team won.

In **step 4 (10 minutes)** the reunion of the two groups in a common room, displaying the game tables and the debriefing takes place. The general manager of security at every team will be the one to briefly present, the mode of action and the justification of the measures taken.

3. REAL PROSPECTS ENVISAGED FOR APPLICATION

In the *National Defence Strategy for the years 2015/2019*, critical infrastructures are mentioned in the "*expanded concept of national security, based on constitutional democracy and mutual respect between citizens and the state, aimed at interests converging towards national security, manifested in the following areas: defence (as understood in double normative quality, national defence and collective defence), public order, intelligence, counterintelligence and security, education, health, economy, energy, finance, environment, critical infrastructure*". [6] At the same time, one of the national security objectives, from the internal perspective, aims at strengthening security and protection of critical infrastructure: energy, transport and cyber and food security as well as the environment. In addition, for the course of action - the dimension of intelligence, counterintelligence and security, identifying and reporting deficiencies in the optimal functioning of critical infrastructure is also aimed.

The Guide of National Defence Strategy of the country for the period 2015/2019 [7] defines critical infrastructure as: devices, networks, services, systems of material goods (energy, transport, communications and information technology, supply with utilities) of strategic interest and/ or public utility, whose destruction, non-operation, damage or disruption could have major negative effects on national or regional level, on the health and safety of citizens, the environment, economy and operation of state institutions.

The models and simulations on critical infrastructure security can be used to understand these infrastructure systems, their interrelationships, their vulnerabilities and the impact of spreading consequences in interdependent infrastructure systems, based on incidents in emergency situations.

For this paper the essence of the concept of modeling was taken into consideration, as a process that produces a model, which is a representation of the construction and operating mode of a certain system of which we are interested. As a defining element, a model should be essential for the real system, should include as many of its important characteristics and should not very complex so that it is not understood and so that it cannot be experienced by rules, players and resources.

4. CONCLUSIONS

In terms of elements of originality and novelty, the paper contains, at least at national level, the focus on educational aspects of critical infrastructures' security, since there are three military educational institutions ("Nicolae Bălcescu" Land Forces Academy, "Carol I" National Defense University and "Mihai Viteazul" National Intelligence Academy, which have in their educational offer programs dedicated to this issue. Previous research is therefore continued [8] coordinated by the author, in which general aspects of education and training in the field of critical infrastructure security were addressed.

This version of the educational game will be improved after comments from teachers and instructors who will carry out teaching activities. A proactive character may be considered, since a reactive component can be noticed in the current design. Moreover, in determining the final result (the winning team), it would be desirable to find a way to emphasize the final exposure of solutions experienced during the exercise.

Not at the least, corresponding to the required development level of this teaching game, it could be used Joint Exercise Management Module,

a planner tool for structuring military exercise and defining action timing, extensively used for training in simulation of all kind of crisis management scenarios at NATO level.

REFERENCES

[1] http://my.nps.edu/web/cisr/movies, accessed on 03.03.2017;

[2] Constantinescu, M., *The Republic of AMRA - an application of Defense Planning and Defence Resources management,* institutional internal course, Regional Department of Defense Resources Management Studies, Braşov;

[3] Abt, C. C., *Serious Games*, Viking Press, 1970, p.9;

[4]http://www.leandroadeodato.com/serious-games/, accessed on 18.03.2017;

[5]https://www.linkedin.com/pulse/3-building-blocks-entrepreneurial-decision-making-daniel-martin, accessed on 20.03.2017;

[6]http://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf, Strategia națională de apărare a țării pentru perioada 2015-2019, *O Românie puternică în Europa şi în lume*, Administrația Prezidențială, Bucureşti, 2015, p. 5, accessed on 23.03.2017;

[7]http://www.presidency.ro/files/userfiles/Ghid_SNApT_2015-2019_AP.pdf, Ghidul Strategiei Naționale de apărare a țării pentru perioada 2015-2019, Bucureşti, 2015, accessed 23.03.2017;

[8] Badea, D., O.M.C. Bucovetchi, R. Oancea, M. Coman, *Educational approaches (infragaming concept based) of the civil emergencies management caused by incidents related to critical infrastructures*, pp. 360-366, 5th International Management Conference "From Management of Crisis to Management in a Time of Crisis" 22nd-24th September 2016, Cluj-Napoca, **ISI** proceeding.