VULNERABILITIES OF CRITICAL INFRASTRUCTURE WITH MILITARY FACETS

Florentina IUGAN, PhD candidate*

Abstract: *The considerable restructuring of the defence systems is a global feature of the current international security environment, with consequences in increasing the complexity of the military dimension of the critical infrastructure protection activities. The trends toward an integrated management of the national defence and security target the guidelines set up by the NATO and EU and require the assertion of an integrated risk management which should comprise new threats, as terrorism is. The cities are the main targets for terrorists because of their multiple critical infrastructures. The increasing of public safety and security within the city has become a must-have of the incoming concepts of planning, like the safe city or the military urbanism.*

Keywords: *critical infrastructure; risk management; defence system; safe city; military urbanism.*

One of the main trends that induce a major increasing of the cities' vulnerability is the on-going fast urbanisation, expressed by the densification of the compact urban zones and the out-of-control urban sprawl in the metropolitan territory, with consequences over a higher aggregation of the people, economic investments and public services within areas with the highest level of risk. Accordingly, *the cities are the main targets for the terrorists because of their multiple critical infrastructures.* The ideal city has not been established yet but the initiatives for its creation have had as outcomes in time the dismantling of its physical boundaries (the walls of the medieval fortress) and the sprawl in the territory by the setting up of city-region systems (by suburbanization). The current approach of the city development focuses more on the inner function of the city, in terms of urban policies targeting the bettering of the quality of life of the citizens, and less on the outer threats that emerge in the global environment and whose appearances are more and more similar in the most world cities. One of these emerging threats is the terrorism and it has been enhanced by the terrorist attacks from 9/11 in USA. Even if the present approaches on sustainable and integrated urban development promise to solve certain economic, social or environmental problems, a broader awareness on the public safety and security has become outstanding in the last years. It focuses not only on the every citizen's life but also on the high-density built areas and on the infrastructures that are critical for the daily city operations and the connection between the city and its surrounding territory.

Although the concept of *vulnerability*, associated to the infrastructure, has been initially defined within the legal framework on emergencies, it has been recently resized by reference to the issues of the critical infrastructures and consequently redefined in accordance with the attributes of their protection, together with the terms of *threat* and *risk*[1]. The argument for redefining vulnerability occurs from the fact that the purpose to destroy a system targets firstly the critical infrastructures. In brief, any vulnerability of a critical infrastructure is tailored by the proportion between the expectation of the occurrence of a real threat over its optimal use and the estimated consequences. Hence, the vulnerabilities must be always assessed with direct and mutual reference to the threats. Consequently, the risk of a critical infrastructure emerges from the potentiality of vulnerabilities and threats, as evaluated in terms of probability and impact of the happening of the threats enhanced by

**"Carol I" National Defence University*
f.iugan@insiteuro.eu.

[1] In Romania, they are defined in the *National Strategy on Critical Infrastructure Protection*, approved by the Government's Decision no. nr. 718/2011.

vulnerabilities[2]. The vulnerabilities of a critical infrastructure may be generated by its physical (constructions, facilities or their components) human (staff, visitors, etc.) or informational (IT systems) aggregates. Moreover, the vulnerabilities may occur either within one or several stages of the critical infrastructure life cycle (design, build, operate, management, refurbishment, etc.) and they must be assessed every time with reference to the susceptibility of optimal use capacity to get out-of-service or destroyed, partially or completely, by at least a threat.

For the purpose of taking measures for the critical infrastructure protection, the assessment of the individual and systemic vulnerabilities is an elementary issue[3]. In the case of man-made threats, as terrorism is, an exclusive focus on the vulnerabilities, even if it is essential in terms of cost-benefit analysis, may suppose that the terrorist will always find the same infrastructure as main target. The pitfall is to use the same methods for reducing the vulnerabilities, while new risk scenarios generated by unconventional approaches of the terrorist goals might be skipped. In this respect, the assessment of the critical infrastructure vulnerabilities must rely firstly on the enemy's ability to collect data and to use them in order to find the weaknesses. Nowadays, most of the public sources of information (open data) provide adequate, relevant, and complete data that might be used anytime for an attack against the critical infrastructure systems.

Several vulnerabilities are common to all the critical infrastructures and others are specific for each of them. The common vulnerabilities are generated by the common supply of all the critical infrastructures with electricity and information & communication technologies (ICT), as long as they are designed and built on the basis of IT software or they are controlled and monitored by ICT. Furthermore, the operation of the critical infrastructures depends on the traditional threats, like the breaks of the physical components, occurred by accident or with purpose, and also on the new virtual threats, like DDOS or malicious actions, leak of critical data by espionage or hacktivism, etc., that are facilitated mostly by the strengthening of the systemic interdependencies at the global level. This is the reason for which the critical infrastructure vulnerabilities have to be re-assessed by taking into consideration the double exposure to threats and dangers, which gathers both the physical and virtual elements of each critical infrastructure.

A particular feature with regard to the strength of the systemic interdependences of the critical infrastructures occurs in the case of the EU, from the spatial-territorial interconnectivity of the technical infrastructures of each country into *European critical infrastructures (ECI)*. The provisions for ECI require joint critical infrastructures for at least two countries, hence overpassing the State borders, and appoint the assumption of a higher level of interdependence of the critical infrastructures in the EU countries, respectively a higher level of ICE's vulnerability. Moreover, by the future enlargement of the EU, when new countries will join EU, the number of ICEs will increase and consequently their vulnerability will increase as well. In addition, the critical infrastructures are networked, in every country and in the EU territory too, which implies that the increasing of the vulnerability of critical infrastructures within a country may lead to the increasing of the vulnerability of all critical infrastructures within the region or the network, and their resistance against threats and dangers may increase accordingly, with synergistic effects. The conclusion is that *the critical infrastructure vulnerabilities increase and change as their interdependence and integrality reach upper levels*[4]. Because of the higher dependence on the services provided by the critical infrastructure, the society has become quite vulnerable to the threats and dangers that menace it. Hence, the vulnerability rose up not only because of the outer threats and risks but also due the interdependences among various infrastructures within the relevant systems, and this context enables the disturbances to cause overwhelming damages for the national economy.

The spatial-territorial integration of the critical infrastructure systems, mainly in the EU, requires the interconnectivity of the national strategic infrastructures, with further consequences in every country over the adjustment of the national defence system and the urban and territorial planning system. In Romania, the national defence system consists

[2] Iulian, Diculescu-Blebea; Ionel, Nițu, "Security risk analysis and management in the Romanian Inteligence Service", Revista Studia Securitatis*,* nr. 2, Ed. ULSB, Sibiu, 2012.

[3] SRI, *Protecția infrastructurilor critice*, Ed. SRI, București, 2010, p. 11.

[4] Grigore Alexandrescu, Gheorghe Văduva, *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*, Ed. UNAp, București, 2006, pp. 17-23.

of the leadership, the armed forces, the resources and the *territorial infrastructure*[5]. By grouping the components up to their criticality, the national defence system comprises common, special and critical infrastructures. The special infrastructures are performance infrastructure with military specification, holding an important role in the proper function of the military systems by ensuring a higher capacity for operations. The critical infrastructures comprise certain elements, subsystems and functional and operational systems, civil and military as well, which are indispensable to the actional and operational performance and the competitiveness, and to the operational stability, safe use and security of the defence force planning too, not only in peacetime but mainly during wartime, by transposing their main subsystems into capabilities and by ensuring performant operation of the other action, management and logistics elements and subsystems as well, in various situations. The *military critical infrastructures* consist of: military communication networks at strategic and tactical levels; equipment of military airparks and harbours, military units and other locations; networks, pipes, storages and supply systems (fuels, ammunition, food and other primary resources;) military roads, railways and navy transportation infrastructures; storage networks; arsenals; computer networks; IT systems[6].

The material resources for defence are included in the strategic infrastructure, made of physical infrastructure networks that are specialized, efficient and compatible with the European infrastructures, and their development targets the provision of enhanced facilities and capabilities.[7] The *territorial infrastructure* consists of the body of works and territorial planning that are in use for the national defence and comprises all the constructions, works, objectives and amenities which permanently hold or might get, by conversion/adjustment, an use in war or crises, in terms of enhancing the specifications and strengths provided by the natural geographic elements and the catalysis of the maximal capitalization of all the involved forces, and the preservation at optimal parameters of the effectiveness of the national defence system.

As basic and constitutional responsibility, *the preparedness of the national economy and territory for defence* is a component of the national security[8], and is in progress in peacetime and targets to meet the strategic and operative needs of the national defence system forces, by achieving certain objectives that will be exclusively used for defence and by identifying and registering the territorial infrastructure for defence, together with the protection of people and goods too.[9] In the scope of maintaining the territorial infrastructure in proper condition in peacetime, during crises or wartime, it is required the up-grading of the infrastructure by the following: rehabilitation and modernization of the civil and military infrastructures, for keeping their parameters at optimal level; rehabilitation, modernization and further development of the transportation infrastructures, inclusively aerial and maritime transportation; building a modern, viable and safe communication infrastructure, and integrate it into the European communication system; development of the energy transportation system; promotion of the ecological transportation technologies; preparation, modernization and development of the infrastructure amenities supplied by NATO for HNS[10]; promotion of infrastructure projects funded by NATO. It is worth to notice that in all these provisions regarding the preparedness of the Romanian territory for defence there is a special attention paid to at least three national critical infrastructure sectors[11]: *energy, transportation and ICT*, where the former two sectors belong to ECIs too, according to 2008/114/CE Directive.

The implementation of infrastructure projects requires identification and supply of resources from national or international sources, on the basis of program and project development and with the involvement of the institutional bodies with responsibilities in the realm of defence. The existing legislation stipulates obligations of the governmental authorities in drawing up the program on public works and territorial planning for the situations of conscription and war, and obligations of the local government authorities and business sector for obtaining the permit issued by

[5] Romanian Law on National Defence no. 45/1994, art. 6.

[6] Grigore Alexandrescu, Gheorghe Văduva, *op. cit*., p. 27.

[7] *National Defence Strategy*, art. 4.2.

[8] Law no. 477/2003 regarding the preparedness of the national economy and territory for defence.

[9] Government's Decision no. 370/2004 for the approval of the Methodological norms for the application of Law no. 477/2003, art. 51-53.

[10] *Host Nation Support* is the civil and military assistance provided by an HN to the forces located in or transiting through that HN's territory.

[11] As they are appointed in the Government's Ordinance no. 98/2010 regarding the identification, appointment and protection of critical infrastructure protection.

the General Headquarters (SMG) for building new investments or for the development of the existing ones, in the scope of framing them within the national defence system infrastructure[12]. As a conclusion, the territory defence planning is strongly related to the territorial infrastructure, respectively to the elements of the urban and territorial planning, and the national defence system infrastructure relies on the provisions and regulations stipulated in the urban and territorial planning documents, which are subject to the approval by SMG as well.

The major reform of the defence systems within the last two decades is a global feature of the international security environment, highlighted by the post-World Wars transition towards the 4th and 5th generation of modern wars, as the hybrid war is nowadays. The reform has consequences over the increasing complexity of the military dimension of the critical infrastructure protection activities, and this raises up a broad interest for the military facets of the critical infrastructure vulnerabilities. At the strategic level, these changes are underlied by the NATO' policies and supported at the regional and national levels by specific programs. NATO's concern for the critical infrastructure protection has started in 2001 and has been reconfirmed in 2007 by the *Report on the Protection of Critical Infrastructures*[13]. In 2003, the *Senior Civil Emergency Planning Committee (SCEPC)* enacted *Concept Paper on Critical Infrastructure Protection*, with the aim to support the development of tools to be used in the preparation and management of the consequences of nuclear accidents or natural disasters over the critical infrastructures. NATO' activities in this scope are comprised in the *Civil Emergency Planning Action Plan* that focuses on the nuclear terrorism risk as well. Another pillar of NATO' policy is the *Programme of Work on Defence against Terrorism*, enacted in 2004, which targets the promotion of the latest technologies for the protection of military assets and armed forces. The critical infrastructure protection is one out of the ten priorities set by this Program. The proposed activities target the use of military know-how, technologies and capabilities for strengthening the protection of strategic locations on the territories of the allied countries, inclusively airports, nuclear plants, communication networks, etc., and within the combat zones too.

NATO's focus on the new security risks is also expressed in the *New Strategic Concept* (2010), where the cyber-attacks are considered as a threat to the national and international security; the *Cyber Defence Concept and the Action Plan* (2011); the *Enhanced NATO Policy on Cyber Defence* (2014), and the topic of cybersecurity is currently debated by several working groups and committees within NATO, with a stronger role since 2013 regarding the improvement of the cyber defence governance within NATO.

Another involvement of NATO in the realm of critical infrastructure protection occurs from the *Smart Defence* initiative[14], that supports the promotion of infrastructure projects funded by NATO, with priority for critical infrastructure protection like: transportation infrastructure, utilities infrastructure (inclusively energy), ICT infrastructure and public services and facilities infrastructure (inclusively health), which are needed for HNS as well.

A distinct issue rises from the European dynamic supported by the *European Security and Defence Policy* regarding the building of joint political and military bodies[15] with the aim to implement the concept of European *common defence* which includes the crisis management with the help of civil and military means able to allow EU to accomplish a common effort towards the common defence and security, within a broader vision, in complementary with NATO's policies. The subsequent objectives of these approaches target that each country should develop an optimal defence capacity, adequate for providing an efficient response to the challenges

[12] In accordance with the Government's Decisio no. 62/1996 regarding the approval of the List of investment and development objectives, and the criteria for the implementing these ones, for which the General Headquarters' permit is compulsory, and with the Common Order of MLPAT, MI, MApN, SRI no. 34/N/3422/M.30/4221/1995 for the approval of the Specifications regarding the approval of the urban and territorial documentations and of the technical documentation for construction permitting.

[13] NATO Parliamentary Assembly, *162 CDS 07 E REV 1 – The Protection of Critical Infrastructures.*

[14] The concept of Smart Defence was introduced by the NATO Secretary General, Anders Fogh Rasmussen, at the Munich Security Conference in 2011, as a concept that encourages Allies to cooperate in developing, acquiring and maintaining military capabilities to meet current security problems in accordance with the new NATO strategic concept. Therefore, Smart Defence means pooling and sharing capabilities, setting priorities and coordinating efforts better.

[15] Political and Security Committee (PSC), EU Military Committee (EUMC) and EU General Headquarters, and the forces: Rapid Reaction Force operated by the EU (EUFOR), EUROCORP, EUROFOR and EUROMARFOR.

of the current security environment, on the basis of the principles of political dialogue, cooperation and partnership, and in accordance with the specific policies of NATO and EU.

In the case of Romania, the programmatic documents in the realm of national defence, among which are the *National Defence Strategy* (2010) and the *Army Transformation Strategy* (2007), target the aim of ensuring the national defence by the development of an optimal defence capacity and the modernization of the military infrastructure, the betterment of the methods and practice of defence resources management, the improvement of the efficiency of the planning, programming, budgeting and evaluation system, the decreasing of the armed forces capacities, and the progress of transition from the threats-based planning to capabilities-based planning. Hence, the defence planning requires an integrated management of the defence resources, adjusted to the actions allocated to the objectives regarding the transformation of the country's defence capacity, which include: the development of infrastructure elements able to provide proper capacities of dislocation, deployment and training for the national forces and NATO forces; building an integrated anti-missile defence system, based on capacities of missile detection and interception; the restructuring, streamlining and capitalizing of the national defence industry. The relationship security – prosperity – identity from the security matrix, as it is defined in *National Defence Strategy,* underlies the need for approaching the human and territorial security by an integrated manner of the convergence of the defence planning and the urban and territorial planning. As a consequence, from the components and the guiding priorities of the integrated planning, it occurs that a particular attention is paid to the betterment of the defence resources system management. In this respect, a consistent contribution might be provided by the adjustment of the urban and territorial planning' activities to the needs of the defence resources, by streamlining the assignment of compulsory resources for the highest importance assets for the national defence and the proper function and stability of the society and economy, as the critical infrastructures are. The opportunity of taking into consideration these ongoing contributions is supported by the agreed participation in the fight against terrorism as well, as a priority of the national defence policy. In order to increase the efficiency of the defence resources management, a high interest topic that is raised nowadays is the *development of double-use industries* (civil and military uses), by transferring technology and military research&development experience, and by the physical transfer of equipment and staff from military units to civil companies. This trend of transfer from the military realm to civil industries is supported by the increasing need of facing the mutations occurred lately in the security environment, which consists in the flourishing of enemies who threat both the military assets and the civil infrastructures, able to take action in peacetime and in crisis and wartime as well. Furthermore, the reconversion of military assets (like military roads, military units, etc.) into civil assets requires the amendment of the operation conditions in the civil scope up to the technical and military parameters from which those assets originate. As a consequence, the up-dating of the activities that target to enhance the critical infrastructure protection should primary focus on the adjustment of the military infrastructure protection to the scope and particularities of the civil critical infrastructures and should encompass the import of specific military elements (for design, build, control, etc.) into the action plans for civil critical infrastructure protection.

An additional challenge is generated by the status of ownership of the critical infrastructure systems. The State is in charge with the national security, and its involvement within the economic and social environment is basic from the security perspective. Nevertheless, in a large number of countries, whole critical infrastructure systems were privatized. Consequently, these infrastructures are currently owned by private companies that also hold the responsibility of protecting them. Therefore, in every country, the critical infrastructure protection activities are provided by several agents, from both the public sector (authorities from the central government and the local government, public agencies) and the private sector (business companies, as owners and/or operators of the critical infrastructures). However, the multiplication of the warnings regarding the terrorist threat, which target mainly the critical infrastructures, and the stepping up of the awareness of the potential devastating consequences of the natural disasters, force more and more the governments to review and amend the policies on the protection of people and critical infrastructures. In most of the cases, this trend emphasizes two dimensions for the coordination of the critical infrastructure protection activities: horizontal coordination (inter-ministries) and vertical (local-county-central levels of authorities) of the responsible public bodies, and coordination between the public authorities and the private owners/operators of critical infrastructures, by supporting the development of public-private partnerships.

In line with the abovementioned matters, the current trends towards a military-civil and public-private integrated approach of the critical infrastructure protection, with the goal to streamline the subsequent activities, is framed by the policies on the *integrated security management*, which includes the development of national capacities for the management of national and international crises and emergencies as well, and should be based on an *integrated risk management*. These trends converge to the priorities set up by the *Romanian National Security Strategy* (2007) and the objectives of the *EU Internal Security Strategy: towards a European Security Model* (2010). Moreover, the proposals for implementing the concept of *urban regeneration* in Romania include the raising of the security level for citizens, by taking actions like the design of more attractive and less risky public open spaces.[16] Nevertheless, even if the new approach promoted by the European Commission in regard of the security objectives related to the risk management has already been implemented up to now in 11 countries (UK, Netherlands, Sweden, Denmark, France, etc.), by the approval of *safety and security national plans* which enclose criteria and complex scenarios on prevention and management of current risks, inclusively the risks generated by the terrorist threat, Romania still misses a similar national plan or strategy.[17]

The military forces generally play only a supportive role in the critical infrastructure protection, focusing mostly on the consequence management, which is after the occurrence of an emergency. However, certain countries authorise the use of military forces as additional patrolling forces which can join the police forces, in the stage of prevention and monitoring of the critical infrastructure conditions, as for example in the airports or the public transportation system, or for the safeguard of large public events, as sports or concerts in open spaces. These preventive actions are expected to deter any terrorist attack plan. For example, in February 2003, at London's Heathrow airport, when a strong military presence was deployed in response to intelligence reports suggesting that al-Qaeda terrorists might launch surface-to-air missile attacks at British or American airliners. Also, these types of actions are routinely taken in France, in the framework of the VIGIPIRATE Plan.[18]

The reconfiguration of the national defence and security systems, by approaching the critical infrastructure protection activities in an integrated manner, has a significant impact mainly at the spatial-territorial level by the restructuring of the territorial infrastructure, as referred to the principles of urban and territorial planning. This type of impact has lately occurred in terms of new concepts, like the *safe city* or the *military urbanism*.

The concept of *safe city* focuses on increasing the public safety and security within the city with the goal to reduce the urban criminality. There is no unique formal definition for the safe city, as the safe city is conceptualized as a sum of the main initiatives and projects designed for increasing the safety of its citizens. In certain approaches, the safe city is considered as the safety & security component of the *smart city*, being completely integrated within it. In other approaches, the safe city highlights the imperative of bettering the city by ensuring maximal security for most of its elements, mainly the components of the critical infrastructures, irresponsive to the implementation of distinct smart projects. The elements of the urban environment that require priority measures for their permanent protection are: the transportation system (roads, railways, etc.), the public open spaces (squares, green areas, etc.), the landmarks (mainly the governmental buildings) and the utilities (supply of water, energy and natural gas, telecommunications, etc.). For securing these elements, a spe-

[16] MDLPL, *Ghid informativ privind regenerarea urbană – principii și practici europene*, MDLPL, București, 2007, p. 25.

[17] European Commission, *Overview of natural and man-made disaster risks in the EU / SWD(2014) 134*. Available from: http://www.sos112.si/slo/tdocs/eu_risks_overview.pdf. Accessed: 20 March 2015.

[18] VIGIPIRATE is France's national security alert system. Until 2014 the system defined four levels of threats represented by five colors: white, yellow, orange, red, scarlet. The levels called for specific security measures, including increased police or police/military mixed patrols in subways, train stations and other vulnerable locations. In 2014 the levels were simplified to 'vigilance' and 'attack alert.

cial attention should be paid to their specific spatial and functional features, in addition to the dynamic elements (like the high mobility generated by the traffic flows) and the variables that arise from the assessment of the vulnerabilities and threats against them.

If considering the safe city as a component of the smart city, the main objective that targets the increasing of the safety and security lies in the extension of ICT use within most of the homeland security infrastructures and services and in the introduction of new standards and regulations for constructions, public equipment and facilities, with the aim to reduce the vulnerability of the urban areas to inner and outer threats against them.

The up-grading of a city up to a safe city will presume to take actions as the following: the permanent monitoring of the technical infrastructures (by using CCTV surveillance systems, environmental sensors, biometric sensors, wireless sensor networks in the public spaces and buildings, and setting up access and control points and control networks with wireless technology, software for activating the mechanisms by phone or internet, etc.); the use of integrated heterogeneous smart systems (*Cyber-Physical-Systems*[19]) like motion detection and video surveillance systems, communication resilient networks, integrated emergency response systems, inclusively early warning sensors for disasters, etc. Up to present, several initiatives of developing European safe cities have been implemented, most of them with financing support from the EU funds, as for example *Safe City*[20] or *FIREBALL*[21]. One of the well-known projects is *SAMURAI*[22], developed in 2008-2011 in UK, with the aim to develop and integrate an innovative surveillance system for robust monitoring of both inside and surrounding areas of a critical public infrastructure site, where people gather (airports, underground platforms, etc.). These systems comprise networked heterogeneous sensors which build multiple complementary sources of information, online adaptive behaviour monitoring system for real-time abnormal behaviour detection and triggering of context-aware alerts in assisting the prevention of crime and integrate fix-positioned CCTV video input with control room operator queries and mobile sensory input from patrolling staff.

Initiatives for securing the urban environment, mainly the public open spaces and the governmental buildings, have already been institutionalized in several European states. For example, the UK planning system has been up-graded in 2004 by the *DCLG Planning Policy Statement* entitled *Safer Places – The Planning System and Crime Prevention*, lately up-dated as *Crime Prevention through Urban Design and Planning (CPTED)* which approves a guide of norms and regulations on urban design and planning, that mainly targets to reduce the crime potential and to increase the feeling of safety of the local community. Hence, the urban planning system becomes an important agent in changing the criminal behaviour by modelling the urban environment in a way to deter out from crime and fear, since the early stage of design of the urban place. The guide synthetizes the features of a safe city to 7 key principles:

- Access and movement: Places with well-defined routes, spaces and entrances that provide for convenient movement without compromising security;
- Structure: Places that are structured so that different uses do not cause conflict;
- Surveillance: Places where all publicly accessible spaces are overlooked;
- Ownership: Places that promote a sense of ownership, respect, territorial responsibility and community;
- Physical protection: Places that include necessary, well-designed security features;
- Activity: Places where the level of human activity is appropriate to the location and creates a sense of safety at all times;
- Management and maintenance: Places that are designed with management and maintenance in mind, to discourage crime in the present and future, what attracts people to the public realm uphold its

[19] *Cyber-Physical-Systems* (CPS) is a system of collaborating computational elements controlling physical entities. Unlike more traditional embedded systems, a full-fledged CPS is typically designed as a network of interacting elements with physical input and output instead of as standalone devices.

[20]Available from: http://www.safecity- project.eu/index.php/mod.proyectos/mem.detalle/id.19/relcategoria./relmenu.3/chk.19353c5bb6e7dcf9f6f4b92d15674c81. Accessed: 15 March 2015.

[21] Available from: https://vimeo.com/fireball4smartcities. Accessed: 15 March 2015.

[22] *Suspicious and Abnormal Behaviour Monitoring using a Network of Cameras and Sensors for Situation Awareness Enhancement*. Available from: http://cordis.europa.eu/result/rcn/45790_en.html. Accessed: 15 March 2015.

attractiveness[23].

The crime prevention through environmental design has become a concept broadly spread in Europe, as it is implemented in other countries[24] and strongly supported with EU funds allocated for projects like *DESURBS – Designing Safer Urban Spaces* or *COST – Crime Prevention through Urban Design and Planning*. This kind of projects are framed within the regulations for urban safety and security set up since 2007 by the European Committee of Standardization in the Technical Report *Prevention of Crime by Urban Planning*.

As a conclusion, the implementation of this type of guides on urban design and planning proves a pro-active approach of the safe city development, from which all the construction or landscape projects should start on, and hereby replace the re-active approach which is intensively promoted nowadays through the addition of ICT in most of the public safety and security systems. The design and build of safe public spaces, buildings and infrastructures may be definitely achieved if security elements are comprised within them since the very beginning. Consequently, the later insertion of surveillance systems (as CCTV) remains only an option from the safety toolbox prepared for reducing the vulnerability to crime threats or crises.

Besides of the evidence that objectives that target the increasing of the homeland safety and security have become part of the most national defence and security strategies all over the world, by following the model of USA *Patriot Act*[25], through which the capacities of police forces and security agencies have been strongly developed in order to trace the terrorist activities since an incipient stage, there are some analysts who warn on the danger of over-securing the cities and the diversion of the urban development planning towards *military urbanism*.[26] This trend is justified from the perspective of oversupplying the urban environment with public safety actions and equipment. One of the arguments is provided by the use in the urban environment of military technologies and software, which were expressly designed for the battlefields and combat zones. Despite of their military origin, they are considered to be useful, either in peacetime or crises or emergencies, in the scope of increasing the public safety in the city. Examples of these types of technologies are the tracking and surveillance systems, like *Visibuilding, Combat Zones That See (CTS)*[27] or performant drones and radars, like *Multipath Exploitation Radar Program* (*MERP)*[28].

Another argument is supported by the latest mutations in the urban environment morphology through the rise of *enclave-spaces*, in a modern version of the historical defence structures. Examples of enclave-spaces are the residential gated communities, the leisure centres and tourist areas with exclusive character, refuges or immigrants' camps, prisons, military bases, airports, stadiums, mixed-use halls, and other types of constructions which address to accommodate masses of people.

As a conclusion, one of the main issues that must be taken into consideration in approaching the critical infrastructure protection, either civil or military, is the assessment of the common elements generated at the convergence of the realms of urban and territorial planning and of national defence and security, respectively the elements which are common to both the territorial infrastructure and the defence infrastructure. The perspectives of the ongoing fast technological development claim for digitalizing the city, mainly in its critical sectors, like transport, energy, health care or water supply, and target to enhance not only the efficiency of public services delivery but the security and the safety of the whole city as well. As the quality of urban design and planning is an urban security measure by itself, inclusively for the critical infrastructure located within the urban environment, it is worth paying attention to the imperative requirement of setting up an integrated risk management with focus on the critical infrastructure protection, by taking into consideration methods of urban design and

[23] The Royal Borough of Kensington and Chelsea, *Designing Out Crime*, 2008 [online]. Available from: http://www.rbkc.gov.uk/pdf/designingoutcrime_spd.pdf. Accessed: 15 March 2015.

[24] See *International CPTED Association*. Available from: http://www.cpted.net/. Accessed: 7 March 2015.

[25] *USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act)* is the main USA law on terrorism prevention. It was enacted in 2001 and completed in 2011by the PATRIOT Sunsets Extension Act.

[26] Stephen Graham, *Cities Under Siege: The New Military Urbanism*, Ed. Verso, London, 2010.

[27]*Combat Zones That See* is a project of the USA Defense Advanced Research Projects Agency (DARPA) whose goal is to "track everything that moves" in a city by linking up a massive network of surveillance cameras to a centralized computer system

[28] *Multipath Exploitation Radar Program* (orig.) is a project of the USA DARPA with extended capacities to reach of airborne sensor platforms beyond Line-of-Sight (LOS) limits by peering deep within the shadows of urban canyons.

territorial planning that could consistently contribute to reducing the vulnerabilities and consequently preventing the danger forecasts from the current threats against the critical infrastructures.

ACKNOWLEDGEMENTS

This paper has been financially supported within the project entitled "Horizon 2020 -Doctoral and Postdoctoral Studies: Promoting the National Interest through Excellence, Competitiveness and Responsibility in the Field of Romanian Fundamental and Applied Scientific Research", contract number ***POSDRU/159/1.5/S/140106. This project is co-financed by European Social Fund through Sectoral Operational Programme for Human Resources Development 2007-2013. Investing in people!***

BIBLIOGRAPHY

1. Alexandrescu, Grigore; Văduva, Gheorghe, *Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie*, Eitura UNAp, Bucureşti, 2006.
2. Diculescu-Blebea, Iulian; Nițu, Ionel, *"Security risk analysis and management in the Romanian Inteligence Service"*, Revista Studia Securitatis nr. 2, Eitura ULSB, Sibiu, 2012.
3. Graham, Stephen, *Cities Under Siege: The New Military Urbanism*, Eitura Verso, London, 2010.
4. Graham, Stephen, *Cities, War, and Terrorism: towards an urban geopolitics*, Eitura Blackwell Publishing, Oxford, 2004.
5. OECD, *Protection of Critical Infrastructure and the Role of Investment Policies Relating to National Security*, 2008 [online]. Available from: http://www.oecd.org/investment/investment-policy/40700392.pdf. Accessed: 10 March 2015.
6. Paraniac, Cornel; Geantă, Ioan, *Un atac terorist pentru viitorul Europei*, Ed. Centrului Tehnic-Editorial al Armatei, Bucureşti, 2008.
7. Scaleţchi, Florentin, *Securitatea comunitară şi terorismul*, Ed. Bren, Bucureşti, 2006.
8. Smedts, Bart, Critical Infrastructure Protection Policy in the EU: state of the art and evolution in the (near) future, *The Royal High Institute for Defence – Center for Security and Defence Studies Focus Paper*, nr. 15/2010 [online]. Available from: http://www.irsd.be/website/images/livres/focuspaper/FP15.pdf . Accessed: 15 March 2015
9. Serviciul Român de Informații, *Protecția infrastructurilor critice*, Eitura SRI, București, 2010.
10. The Royal Borough of Kensington and Chelsea, *Designing Out Crime*, 2008 [online]. Available from: http://www.rbkc.gov.uk/pdf/designingoutcrime_spd.pdf. Accessed: 15 March 2015.
11. Topor, Sorin, *O scurtă istorie a terorismului,* Eitura UNAp, Bucureşti, 2013.