Development of an integrated methodology for the identification and classification of critical infrastructures at local level and associated risk assessment

Andrei Radovici, Liviu Muntean, Alexandru Ozunu

Faculty of Environmental Science and Engineering, Babeş-Bolyai University from Cluj-Napoca, Cluj-Napoca, Romania. Corresponding author: A. Radovici, radovici_andrei@yahoo.com

Abstract. The purpose of this paper is to lay the foundations of a methodology for the identification, classification and management of critical infrastructures to a much narrower range than they were previously defined in the literature and legislation. Still, the proposed methodology can be applied to all levels of administrative organization. These actions can help local decision makers, to jointly develop actions and strategies to support sustainable development and to improve the general level of security. In order to achieve these objectives, the critical infrastructures will be identified deductively, starting from the sectors of activity present in the studied area and classified on the basis of their dependence. In the final phase of the management process it is required to elaborate risk assessment for the critical infrastructures previously classified, in order to maximize the benefits/cost ratio.
Key Words: critical infrastructure, risk assessment, dependency, classification matrix.

Introduction. In the actual context of a dynamic society that constantly restructures its activities, some specific risks can arise through all sectors of activity. Potential actions on key issues in society may generate major effects on its operational capacity. In this case, the management of these situations by the authorities is a delicate and complex process, of which success is conditioned by various factors.

Society, just like a system, is developing on the basis of relations between the sectors and components. Those elements which are characterized as the most sensitive components of a system, in the context of human society, are entitled as critical infrastructures (CI). In a broader sense, it is acceptable to consider CI as the backbone of a system. With the increase of the system complexity it is recognizable that a series of new elements are characterized by a strong susceptibility to be influenced by voluntary or involuntary actions that tend to destabilize the system. In this context we can appreciate that CI will always have a high degree of vulnerability because they are usually the first target when external or internal agents are seeking to destabilize or even destroy a system or process (Alexandrescu & Văduva 2006).

The trend of increasing the risk associated with vital objectives of states or international organizations has imposed the need to develop the concept of CI. Over the last few years, a number of documents concerned with CI protection have offered general definitions for critical infrastructures and have provided short lists of which infrastructures should be included. None of these lists or definitions would be considered definitive, but it is important to mention the “Executive Order 13010”, issued by the President of United States in 1996, in which the CI are defined as “… so vital to society that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States”. The criteria for determining what might be a critical infrastructure, and which infrastructures thus qualify, have expanded over time (Moteff et al 2003). As mentioned above, CI were originally considered to be those whose prolonged disruptions could cause significant military and economic dislocation (Moteff et al 2003), but recent events like natural disasters and countless anthropic hazards have conducted to the development of terminology in such a manner that the concept will cover many more areas than it was initially projected.

To develop an integrated methodology for identification, prioritization and management of CI at local level, this study proposes to combine and adapt certain methods found in the literature. One of the main objectives of this methodology is to provide outputs that can be easily used by the decision makers, specialized or not, involved in the process of critical infrastructure management.

Methodology description. The current study is focused on three major topics related with CI management: identification, classification and risk management. These topics are also the three major steps to be followed in the presented methodology.

Identification. Because the current study proposes a more specific approach to CI, on an area much narrower that they were initially defined, the phase of identification may prove challenging because of the lack of existence of a method that takes into account only objective factors. Thus, we can say that this process is rather subjective, strongly influenced by the experience of conducting the study and the availability of information. In order to improve the accuracy of the study outputs, it is suggested that the identification of CI should be done in the spirit of the following definition (CIP Strategy 2009): "Critical infrastructures (CI) are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences". It should be noted that, in the present study, unlike the above definition, the effects of "failure" or "degradation" of CI are prone to affect the society and economy locally, only in exceptional cases their impact extends to higher levels of territorial organization. In practice, it is more convenient to identify the activity sectors present in the studied area and then to deductively identify the representative CI for those sectors.

Classification. In order to facilitate the decision making process and to develop local policies more effective, it is not enough only to identify CI, they also have to be classified on the basis of a predetermined criteria. This principle of classification may consist in the dependency or interdependency between at least two CI. The logic to do so, is based on the fact that failure or malfunction of one infrastructure will impact the functionality of the infrastructure dependent on it (Rinaldi et al 2001). If this process will continue to other infrastructures, the effect of "waterfall" is created and the process will conduct to the entire system failure. Considering this, the decision-makers should concentrate their resources to that CI of which many other CI are dependent.

To highlight the dependency relationships between CI and carry out a classification of them, the methodology is recommending using a modified version of the dependency matrix (Dunn & Wigert 2004), as seen in the Figure 1 (sectors identified in Cluj-Napoca Municipality). The scores of dependency between various critical infrastructures are made with ratings from 1 to 3, as follows: 1 - minor dependency; 2 - medium dependency; 3 - major dependency.

	Energy	IT	Finance	Public Health	Alimentation	Water	Urban security	Public Authorities	Transport	Industry	Education	Trade	Culture	Waste	Overall score
Energy															
IT															
Finance															
Public Health															
Alimentation															
Water															
Urban security															
Public Authorities															
Transport															
Industry															
Education															
Trade															
Culture															
Waste															

Figure 1. CI dependency matrix.

For a better understanding on how the dependency between various CI can be evaluated and on how to actually classify CI based on the overall score, Figure 2 must be consulted.

	Electricity distribution network	Natural gas distribution network	Phone network	Internet network	Financial network	Directorate for Local Taxes	Medical institustions	University of Medicine and Pharmac	Hipermarkets	Food Market	Water supply network	Wastewater discharge network	Police	Firefighters	Town Hall	Local Council	Public roads	Public transportation network	Industrial parks	Universities	Schools	Comercial centers	Green areas	Waste disposal system	Overall score
Electricity distribution network		2	3	3	3	3	3	3	3	1	2	3	3	3	3	3	1	3	3	3	3	3	1	1	**59**
Natural gas distribution network	2		0	0	1	1	3	2	1	0	0	0	2	2	2	2	0	0	3	2	2	3	0	0	**28**
Phone network	1	1		3	3	2	2	1	1	0	1	1	3	3	2	2	0	0	2	1	1	1	0	0	**31**
Internet network	1	1	2		3	2	1	3	3	0	0	0	3	1	1	1	0	0	3	3	3	1	0	0	**32**
Financial network	2	2	2	2		3	2	1	3	0	1	1	1	1	1	1	0	0	3	2	1	3	0	1	**33**
Directorate for Local Taxes	1	1	0	0	0		2	1	1	3	1	1	3	3	3	3	3	3	2	1	2	1	3	2	**40**
Medical institustions	0	0	0	0	0	0		3	0	0	0	3	0	0	0	0	0	1	0	2	2	0	0	3	**14**
University of Medicine and Pharmacy	0	0	0	0	0	0	3		0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	**7**
Hipermarkets	1	0	0	0	2	0	0	0		0	0	1	0	0	0	0	2	3	0	0	0	3	0	1	**13**
Food Market	0	0	0	0	0	0	1	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	1	**2**
Water supply network	1	1	1	1	3	3	3	3	3	3		3	3	3	3	3	2	0	3	3	3	3	1	0	**52**
Wastewater discharge network	0	0	0	0	3	3	3	3	3	3	3		3	3	3	3	2	0	3	3	3	3	3	3	**53**
Police	3	3	2	2	3	2	3	2	3	3	2	2		2	2	2	3	3	3	2	2	3	3	2	**57**
Firefighters	1	1	1	1	1	1	1	1	1	1	0	0	1		1	1	1	1	1	1	1	1	1	1	**21**
Town Hall	2	2	1	1	1	2	1	1	1	2	2	2	2	2		3	3	3	3	2	2	1	3	2	**44**
Local Council	2	2	1	1	1	2	1	1	1	2	2	2	2	2	3		3	3	3	2	2	1	3	2	**44**
Public roads	3	3	3	2	3	2	3	1	3	3	3	3	3	3	3	3		3	3	3	3	3	3	3	**65**
Public transportation network	1	0	0	0	1	0	0	0	2	2	0	0	0	0	1	1	3		3	3	3	2	1	0	**23**
Industrial parks	3	3	0	0	2	3	2	0	0	0	3	3	0	0	1	1	3	0		2	0	0	0	2	**28**
Universities	0	0	2	2	2	1	2	2	2	1	0	0	1	0	1	1	2	3	1		3	2	1	1	**30**
Schools	0	0	0	0	0	0	0	2	1	1	0	0	2	0	1	1	1	2	0	3		1	1	0	**16**
Comercial centers	0	0	0	0	2	2	1	1	3	1	0	1	0	0	1	1	2	2	2	1	1		0	1	**22**
Green areas	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0		1	**5**
Waste disposal system	2	2	2	2	3	2	3	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3	3		**63**

Figure 1. Dependency matrix for Critical Infrastructures of Cluj-Napoca Municpality.

The final score is obtained by the sum of all ratings for each CI. The classification has been done in descending order of marks obtained and CI with the highest score are the most important (Table 1).

Table 1

Classification of Critical Infrastructures based on dependency overall score

Name of Critical Infrastructure	*Overall score*
Public roads	65
Waste disposal system	63
Electricity distribution network	59
Police	57
Wastewater discharge network	53
Water supply network	52
Town Hall	44
Local Council	44
Directorate for Local Taxes	40
Financial network	33
Internet network	32

Phone network	31
Universities	30
Natural gas distribution network	28
Industrial parks	28
Public transportation network	23
Comercial centers	22
Firefighters	21
Schools	16
Medical institustions	14
Hipermarkets	13
University of Medicine and Pharmacy	7
Green areas	5
Food Market	2

The entire process of classification might be subjective if the evaluator doesn't have access to information relevant for relations between different elements of CI. To improve this aspect of subjectivity, it is recommended that the study to be developed by a team of evaluators from different fields of activity. Another important factor, which may contribute to the level of subjectivity in the study, is the experience of the assessor.

Risk assessment. To assess the risk associated with CI, a method developed by Federal Emergency Management Agency in 2005 will be adjusted to fit the study specificity. The method was originally intended to be a guide on how to mitigate potential terrorist attacks against buildings (FEMA 2005), but the relative simplicity of the method would recommend its usage in risk assessments related to CI. For the risk assessment process to be a functional one, FEMA suggests a study in five steps (FEMA 2005), as showed in Figure 3.

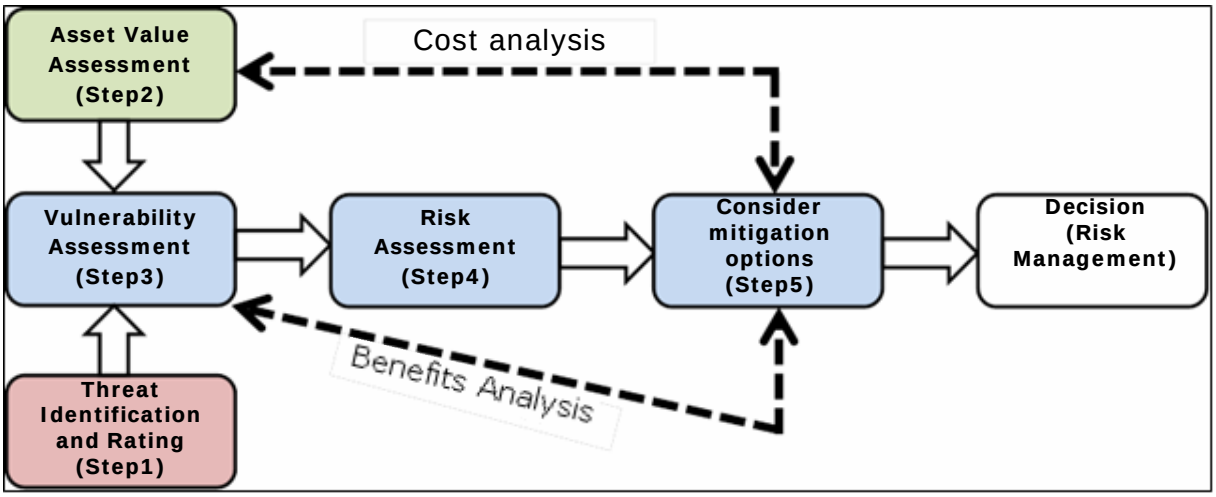

Figure 3. Risk assessment process model (FEMA 2005).

This method is considering the risk as a product of three factors: threats or likelihood of a threat, assets value or consequnces and the vulnerability of CI. Each of this components is rated with marks from 1 to 10 as explained in Tables 2-4.

Once the numeric value was set for each of the elements described above, the study will have to continue on calculating the value of the risk by multiplying the three values. Once calculated, the value of this risk translates into a matrix, whose characteristics are determined by the value of threats on the vertical axis and the value of vulnerability on the horizontal axis. Since there are ten numeric classes which set the value of the consequences, it is normally to have ten different types of risk matrices. Figure 4 provides a better understanding of how risk matrix changes depending on the value of the consequences. For a better visual representation three color codes have been used, their significance being indicated in Table 5. The thresholds limits are set

acordingly to FEMA recomandations, but they can vary based on different criteria set by the evaluators or the decision makers, wich may consider different levels of risk as acceptable or not.

Table 2

Threat rating scale (FEMA 2005)

	Threat rating
10	The likelihood of a threat, weapon, and tactic being used against the site, network, buildings or assets is imminent. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
8-9	The likelihood of a threat, weapon, and tactic being used against site, network, buildings or assets is expected. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
7	The likelihood of a threat, weapon, and tactic being used against the site, network, buildings or assets is probable. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
5-6	The likelihood of a threat, weapon, and tactic being used against the site, network, buildings or assets is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is not verified.
4	The likelihood of a threat, weapon, and tactic being used in the region is probable. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is not likely.
2-3	The likelihood of a threat, weapon, and tactic being used in the region is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat exists, but is not likely.
1	The likelihood of a threat, weapon, and tactic being used in the region or site, network, buildings or assets is very negligible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is non-existent or extremely unlikely.

Table 3

Asset value scale (FEMA 2005)

	Asset value
10	Loss or damage of the CI's assets would have exceptionally grave consequences, such as extensive loss of life, widespread severe injuries, or total loss of primary services, core processes, and functions.
8-9	Loss or damage of the CI's assets would have grave consequences, such as loss of life, severe injuries, loss of primary services, or major loss of core processes and functions for an extended period of time.
7	Loss or damage of the CI's assets would have serious consequences, such as serious injuries or impairment of core processes and functions for an extended period of time.
5-6	Loss or damage of the CI's assets would have moderate to serious consequences, such as injuries or impairment of core functions and processes.
4	Loss or damage of the CI's assets would have moderate consequences, such as minor injuries or minor impairment of core functions and processes
2-3	Loss or damage of the CI's assets would have minor consequences or impact, such as a slight impact on core functions and processes for a short period of time.
1	Loss or damage of the CI's assets would have negligible consequences or impact.

Table 4

Vulnerability rating scale (FEMA 2005)

	Vulnerability rating
10	One or more major weaknesses have been identified that make the asset extremely susceptible to an aggressor or hazard. The CI lacks redundancies/ physical protection and the entire CI would be only functional again after a very long period of time after the event.
8-9	One or more major weaknesses have been identified that make the asset highly susceptible to an aggressor or hazard. The CI has poor redundancies/ physical protection and most parts of the CI would be only functional again after a long period of time after the event.
7	An important weakness has been identified that makes the asset very susceptible to an aggressor or hazard. The CI has inadequate redundancies/ physical protection and most critical functions would be only operational again after a long period of time after the event.
5-6	A weakness has been identified that makes the asset fairly susceptible to an aggressor or hazard. The CI has insufficient redundancies/physical protection and most part of the building would be only functional again after a considerable period of time after the event.
4	A weakness has been identified that makes the asset somewhat susceptible to an aggressor or hazard. The CI has incorporated a fair level of redundancies/physical protection and most critical functions would be only operational again after a considerable period of time after the attack.
2-3	A minor weakness has been identified that slightly increases the susceptibility of the asset to an aggressor or hazard. The CI has incorporated a good level of redundancies/physical protection and the CI would be operational within a short period of time after an attack.
1	No weaknesses exist. The CI has incorporated excellent redundancies/physical protection and the building would be operational immediately after an attack.

Threats \ Vulnerability	1	2	3	4	5	6	7	8	9	10
1	5	10	15	20	25	30	35	40	45	50
2	10	20	30	40	50	60	70	80	90	100
3	15	30	45	60	75	90	105	120	135	150
4	20	40	60	80	100	120	140	160	180	200
5	25	50	75	100	125	150	175	200	225	250
6	30	60	90	120	150	180	210	240	270	300
7	35	70	105	140	175	210	245	280	315	350
8	40	80	120	160	200	240	280	320	360	400
9	45	90	135	180	225	270	315	360	405	450
10	50	100	150	200	250	300	350	400	450	500

Threats \ Vulnerability	1	2	3	4	5	6	7	8	9	10
1	10	20	30	40	50	60	70	80	90	100
2	20	40	60	80	100	120	140	160	180	200
3	30	60	90	120	150	180	210	240	270	300
4	40	80	120	160	200	240	280	320	360	400
5	50	100	150	200	250	300	350	400	450	500
6	60	120	180	240	300	360	420	480	540	600
7	70	140	210	280	350	420	490	560	630	700
8	80	160	240	320	400	480	560	640	720	800
9	90	180	270	360	450	540	630	720	810	900
10	100	200	300	400	500	600	700	800	900	1000

Figure 4. Risk matrices based on the value of consequences of 5 and 10.

Table 5

Risk value scale

Low risk	*Medium risk*	*High risk*
1-60	61-175	≥176

Conclusions. Developing a methodology for the identification and classification of CI is a challenge especially through the complexity of the topic, but this study has revealed one possible way on how these difficulties can be managed. The purposed methodology might be a reliable instrument to assist public authorities in the process of CI management; it is simple enough not to burden the procedure of planning and decision-making and is also quite consistent for the results to be satisfactory. This methodology should be improved in other papers in order to resolve some issues generated by the possibility to have some erroneous results generated by subjectivity.

References

Alexandrescu G., Văduva G., 2006 [Critical infrastructures: dangers, threats, protection systems]. „Carol I" National Univeristy of Defense Publishing House, Bucharest, pp. 29-35. [in Romanian]

Clinton W., 1996 Executive order EO 13010 for Critical Infrastructure Protection. Washington D.C.

Dunn M., Wigert I., 2004 International CIIP Handbook 2004: an inventory and analysis of protection policies in fourteen countries. Swiss Federal Institute of Technology. Zurich, 405 pp.

Federal Emergency Management Agency (FEMA), 2005 Risk assessment - a how-to guide to mitigate potential terrorist attacks against buidings.

Federal Ministry of the Interior, 2009 National Strategy for Critical Infrastructure Protection (CIP Strategy). Berlin, 18 pp.

Moteff J., Copeland C., Fischer J., 2003 Critical Infrastructures: what makes an infrastructure critical? Report for Congress. The Library of Congress. Washington, D.C., 20 pp.

Rinaldi S. M., Peerenboom J. P., Kelly T. K., 2001 Identifying, understanding and analyzing: critical infrastructure interdependencies. IEEE Control Systems Magazine, pp. 11-25.

Received: 03 August 2015. Accepted: 20 December 2015. Published online: 30 December 2015.
Authors:
Andrei Radovici, Babes-Bolyai University, Faculty of Environmental Science and Engineering, Fântânele str., no. 30, 400327 Cluj-Napoca, Romania, e-mail: radovici_andrei@yahoo.com
Liviu Muntean, Babes-Bolyai University, Faculty of Environmental Science and Engineering, Fântânele str., no. 30, 400327 Cluj-Napoca, Romania, e-mail: liviu.muntean@ubbcluj.ro
Alexandru Ozunu, Babes-Bolyai University, Faculty of Environmental Science and Engineering, Fântânele str., no. 30, 400327 Cluj-Napoca, Romania, e-mail: alexandru.ozunu@ubbcluj.ro

How to cite this article:
Radovici A., Munteanu L., Ozunu A., 2015 Development of an integrated methodology for the identification and classification of critical infrastructures at local level and associated risk assessment. Ecoterra 12(4):75-81.