The 14th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 7th-8th 2019

CONCEPTUALIZATION OF A KNOWLEDGE MANAGEMENT FRAMEWORK DEDICATED TO THE SECURITY OF CRITICAL INFRASTRUCTURES

LTC, assoc. prof. eng. Dorel BADEA, PhD*

* "Nicolae Bălcescu" Land Forces Academy of Sibiu

Abstract:
The analysis of the proposed topic of the article had as working assumptions two tendencies with opposite directions from the point of view of the contribution to the sustainable development of the present society, namely, the exponential, quantitative and qualitative increase of the dimension of knowledge, as a process that favored in time the social transformation, respectively, the multiplication of the types of threats and the ways of their manifestation that ultimately affect the social balance. The activity segment chosen in this context for investigation is that of critical infrastructures (CI), a relatively recent field set from the point of view of knowledge management (KM) challenges and, at the same time, very sensitive to the desired state for the functionality of nowadays globalized society. The way of approaching the aspects specific to the stated topic is interdisciplinary, at the micro (operator and/or IC holder) but also macro (national and/or European IC system) level, the opportunities to identify possible solutions (4D structured - define, design, develop, deliver), being highlighted by the use of methodological tools of conceptual modeling, applied in the spectrum determined by the coordinates as is and are to be.

Key words: critical infrastructures, security, knowledge, modeling

1. Security of critical infrastructures - certainties and challenges

Critical Infrastructure Security (CIS) is a topic that is increasingly more present at the center of the concerns of government decision-makers, managers in the private environment who work in critical infrastructure systems and not least, the academic environment, as a provider of specific educational programs. All these stakeholders want to find optimal solutions to ensure the continuity of activities endangered by increasingly diverse threats, of which the most current is the cyber spectrum. 5G technologies like knowledge increase the possibilities of social reality in a comprehensive manner, but, at the same time, make individuals and organizations vulnerable. Constraints in terms of time, quality, resources of developing sustainable solutions for problems on the public agenda are combined with those of risk assessment, security measures, incident reporting, in an information overloaded framework, asserting that we live in an exponential time. The need to investigate the influence of activity within space systems on other common systems and, to a greater extent, on critical infrastructure systems [1], [2] is increasingly felt. Solutions containing metaconcepts are required and are discussed in the literature [3], an example in this respect being the governing and resilience. More and more standards that regulate the unitary approach of some major fields of activity and interest are produced within the profile organizations, of which we can highlight those regarding risk management and information security, which are, in fact, tools that facilitate the uniform management of complexity.

CONCEPTUALIZATION OF A KNOWLEDGE MANAGEMENT FRAMEWORK DEDICATED TO THE SECURITY OF CRITICAL INFRASTRUCTURES

In order to organize and structure the analysis of the factors that contribute to the determination of a satisfactory level of security of the critical infrastructures (reduction of the level of vulnerability) as well as of some interdependencies between these factors, the mind mapping method was used with the help of a dedicated software product available online [4]. The incidence and influence of these factors (figure 1) within the organizations holding critical infrastructures is different depending on the sector of activity (transport, energy, chemical, etc.), the size of the organization and the national or international scale (holding national and / or European critical infrastructures), the type of financing (public or private).

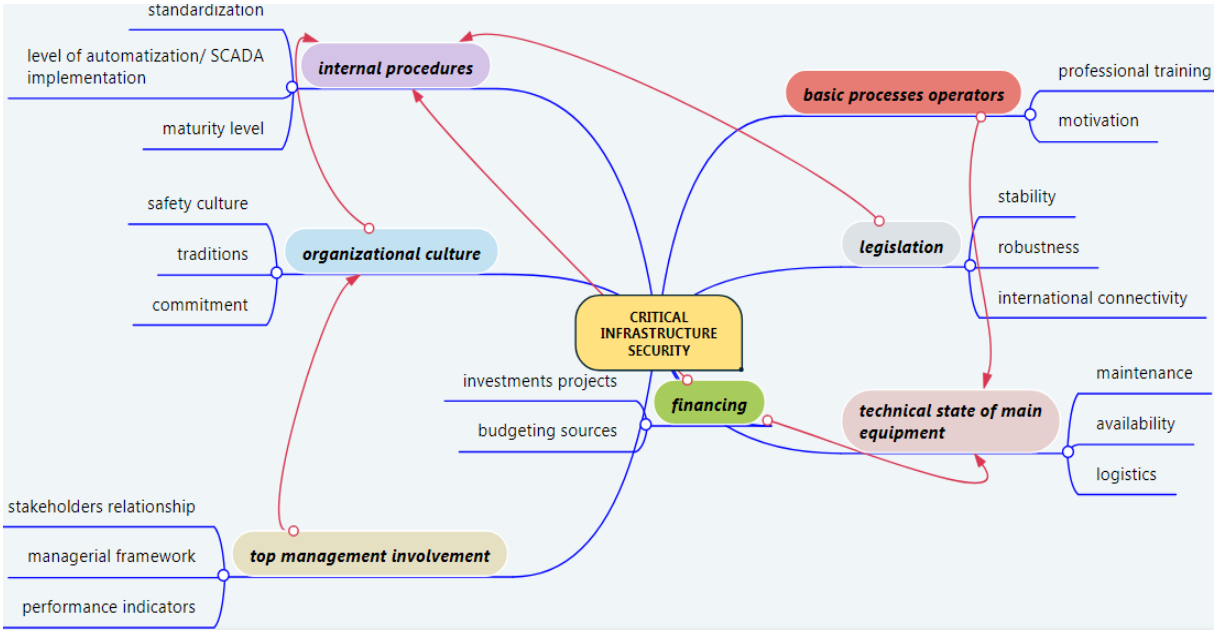

Fig.1 The relationship between CIS analysis factors

2.Modeling the processes of governance of critical infrastructure systems using the Zachman architectural framework

Starting from the differentiations (provided by the meaning, context and structure) between the data, information and knowledge and considering the objective of conceptually modeling a knowledge management framework dedicated to the security of critical infrastructures (especially the analysis of the required requirements), the Zachman model was chosen, used mainly for information systems in the business environment and in industry, also knowing the fact that [5], related to this situation, the focus is on the fact that all the aspects characteristic of an enterprise must be well realized and organized. The exploratory research undertaken is meant to clarify, define and identify the fundamental correlations that are manifested within the proposed theme and will allow, in the alternative, a deeper understanding of the concepts and the essence of the phenomena and processes envisaged, finally contributing to the awareness of the specialists with topical notions and approaches. The exploration of the opinions, reasons, attitudes and values that influence the understanding of the behaviors and decision processes specific to change management is carried out within Enterprise architecture (EA), a practice and emerging field intended to improve the management and functioning of complex enterprises and their information systems [6].

CONCEPTUALIZATION OF A KNOWLEDGE MANAGEMENT FRAMEWORK DEDICATED TO THE SECURITY OF CRITICAL INFRASTRUCTURES

For the particularization of the Zachman model in the case of critical infrastructure security, a simplified working tool was used in comparison with dedicated applications [7], the idea being to create an integrated big picture, necessary to understand the governance of the CI system from a managerial point of view (table 1).

Abstractions > \/ Perspectives	Data / What	Function / How	Network / Where	People / Who	Time / When	Motivation / Why
Scope / SMEs from presidential administration	the list of national security values and missions	establishing the essential processes for ensuring national security	headquarters of central institutions in the national defense , public order and national security system	national authorities at strategic level	deadlines for issuing / revising national defense planning documents	ensuring a sustainable development framework in national and regional context
Enterprise Model / integrated management of CI at government authority level	semantic model of the requirements for the management of CI interdependencies	setting the general framework for ensuring the effectiveness of policies in the field of CIS	the national coordination center of the CIS	inter-ministerial committees with responsibilities regarding the CIS	after approval of the budget / the budget constraints	implementation of proposed government security policies
System Model / domain leader (sector) of CI	interoperability requirements in the field of CI, critical values	defining the specific framework for achieving CIS management	areas of national or European importance in terms of criticality	operational or risk managers at the level of public-private partnership	agreed deadlines for reviewing or approving the security plans of CI operators	facilitating the implementation of governance initiatives and business continuity
Tech Constrained Model / holders / administrators (public / private) of CI	essential security requirements for the equipment used within the CI	updating the CI holder's security plan	CI location	organizational chart	periodicity of testing the viability of risk management plans in the framework of integrated training exercises	optimization of organizational performance in terms of cost and effectiveness of providing critical service
Detailed Representations / operators of systems / installations subcomponent of CI	requirements for reliability of measuring and control equipment and tools	use of specialized systems / SCADA; operationalization of active / passive / semi-active redundancy variants	the space of arrangement of the IT subassemblies	working shifts based on factors specific to human-machine interfaces	according to the specifications of the major equipment maintenance plan	role awareness within the organization that holds the CI
Functioning Enterprise / beneficiaries of the services of the CI systems	receiving the deliverables of the CI systems at the required functionality parameters	understanding the criticality of the provided service	the network / channel for providing the critical service	supervisory authorities of the quality of critical products / services provided to consumers	the need to have provided the critical service continuously or discontinuously	the utility of the CI system's deliverables in ensuring daily activities

Table 1 Zachman model (version) for CIS analysis

3.KM- a business driver for CIS implementation

The above table provides a comprehensive picture for identifying locations generating specific KM processes, the importance of these processes being emphasized at EU level in a broader context given by disaster management, ever since 2017, as follows: "Better knowledge, stronger evidence and a greater focus on transformative processes and innovation are essential to improve our understanding of disaster risk, to build resilience and risk-informed approaches to policy-making, and to contribute to smart, sustainable and inclusive growth." [8]. The approach used to define the concept of Knowledge Management (KM) with the meaning [9] of a study discipline that promotes an integrated approach for identifying, capturing, evaluating, retrieving and sharing all of an organization's information assets (may be included database, documents, policies, procedures and previously uncaptured expertise and experience in individual workers).

The main problem for the current situation in many critical infrastructures is the existence of data management systems and less information, which does not lead to knowledge, examples of good practices belonging to the private environment and IT industries (figure 2). The effects are as expected, thus diminishing the possibility of achieving integrated emergency management systems. Given that, generically, a KM framework contains hardware, software, people, and organization, environment around it, the challenge that appears so imminent at the level of governmental CIS management authority is setting up an integrative KM framework that should encompass at least one of the following elements: establishing the content of a minimum package of updated information necessary to be provided at any time in crisis situations by the CI holder to various stakeholders (as they were described in table 1); the creation of a CIS management software product with a common component regardless of the CI type and the level of decision hierarchy but also with a specific component of each CI, which can be interoperable both horizontally and vertically in terms of supporting the decision-making process; a coherent subsystem (in connection with the one proposed above) to generate lessons learned based on the problematic situations that have appeared in the organizations holding CI; regularly conducting interdisciplinary training sessions and integrative exercises with a robust practical component; KM structure.

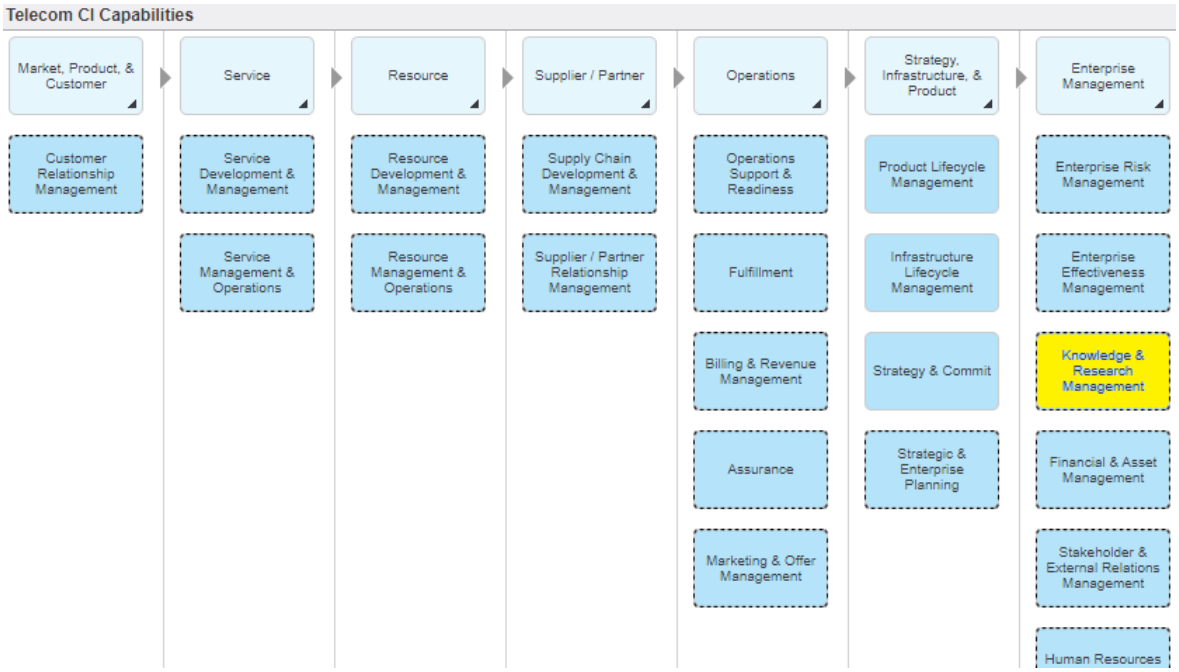

Fig. 2 The place of a KM department within an IT CI [generated using 10]

4. Conclusions

The need to find the optimal mix on knowledge management within complex systems is not new, the means of implementing it creating this perception. It has evolved in the same trend as the changes in business intelligence processes. The statement is also valid in the case of CI systems that are becoming increasingly dependent on the electrical and IT components, the desire to create robust, threat-resistant structures, further emphasizing the importance of the enterprise architecture approach and, subsequently, of the Zachman model. Under these circumstances, the words of Hansen W. [11] are expressive, who, as a visionary, emphasized almost thirty years ago that when people understand the vision and larger tasks of their enterprise, and are given the right information, resources and responsibilities, they will do the right things. It can be argued that the restructuring of some CI systems based on specific concepts of top-down or incremental architectural development models and of technological enhancing factors (exploding complexity of technology, proliferation of technology) is at the same time a rsolid premise of creating an appropriate KM framework for CIS.

References:

[1] Georgescu, A., Bucovetchi, O., Tatar, U., *Space Systems as Critical Infrastructures*, in *FAIMA Business & Management Journal*, vol.6 (1), 2018, pp. 24-34.
[2] Gheorghe, A. V., Georgescu, A., Bucovețchi, O., Lazăr, M., Scarlat, C., *New Dimensions for a Challenging Security Environment: Growing Exposure to Critical Space Infrastructure Disruption Risk*, in *International Journal of Disaster Risk Science*, Beijing Normal University Press, vol. 9(4), 2018, pp. 555-560.
[3] Pulfer, R., Bucovetchi, O.M.C., Gheorghe, A.V., *The Governance Risk and Compliance (GRC) Model within a Dynamic Business Environment*, in *Proceedings of 26th IBIMA Conference*, Madrid, 11-12 November 2015, pp. 2651-2658.
[4] https://www.mindmeister.com, accessed 09.10.2019
[5] http://www.ia.ase.ro/Sie/SIE-4-2013.pdf, accessed 15.10.2019
[6] Lapalme, J., Gerber, A., Van der Merwe, A., Zachman, J., De Vries, M., Hinkelmann, K., *Exploring the future of Enterprise Architecture: A Zachman Perspective* in *Computers in Industry*, Volume 79, June 2016, pp. 103-113.
[7] https://www.visual-paradigm.com , accessed 16.10.2019
[8] Poljanšek, K., Marin Ferrer, M., De Groeve, T., Clark, I., (Eds.), *Science for disaster risk management 2017: knowing better and losing less*, EUR 28034 EN, Publications Office of the European Union, Luxembourg, 2017, p.10.
[9] Duhon, B., *It's all in our heads* in *Inform*, Vol. 12, No. 8, September, 1998, pp. 8-13.
[10] https://ams001.blueworkslive.com/scr/processes/1000069c4d9359b#map, accessed 17.10.2019
[11] Hansen, W.C., *The Integrated Enterprise*. In *Foundations of World-C/ass Manufacturing Systems: Symposium Papers*, National Academy of Engineering, 2101 Consortium Ave, N.W. Washington, DC, 1991.