ELEMENTS OF CRITICAL INFRASTRUCTURE RESILIENCE[1]

Darko Trifunovic*

Abstract

This Article points to key elements of Critical Infrastructure Resilience (CIR) and how they differ from Critical Infrastructure Protection (CIP). CIP is still very important and one of the key systems that the society relies upon to ensure the continuity of operation of CI. However, CIP cannot predict an adequate number of major threats that would allow to conduct the preparedness and response

[1] The article was presented at International Expert Forum, Zagreb Security Forum 2018 on Plenary Session by invitation.

* Dr. Darko Trifunović, Director of the Institute for National and International Security, professor at Faculty of Law, Administration and Security, Megatrend University, Belgrade. Dr Trifunovic was elected as guest professor at FUDAN University – Center of American Studies, Shanghai, China. Senior Research Fellow and lecturer at Faculty of Security Studies-University of Belgrade. He is Senior Adviser at the Research Institute for European and American Studies, Greece, Athens. He is a specialist in Security studies, Intelligence & Counter Intelligence studies as well as Counter-Terrorism, National and International Security studies. He is a former diplomat (First Secretary of the Foreign Service of Bosnia and Herzegovina at the United Nations). Dr. Trifunovic is the representative for Serbia and Montenegro of International Strategic Studies Association (ISSA); Defense & Foreign Affairs publications; and the Global Information System and he is member of the Advisory Board of the Institute of Transnational Studies, Munich, Germany. The Shanghai Center for International Studies appointed him as the first foreign expert for the Olympic Games (2008) security preparation in China. In 2010, he is engaged in World Expo Security preparation and is a Member. Dr Trifunovic is regular speaker at International Counter Terrorism Institute, Tel Aviv, Israel, and prof.dr Darko Trifunovic is one of the founding Members of the International Counter Terrorism Academic Community (ICTAC). He has published numbers of academic books papers and articles.

at the level which would ensure the sufficient operation of CI in all cases. In that sense CIR sets a new paradigm with a quality that reduces vulnerability, minimizes the consequences of threats, accelerates response and recovery, and facilitates adaptation to a disruptive event. Some selected concepts of CIR with examples are presented in the Article that should assist in further development and enhancement of resilience of subsystems and infrastructures as a whole, resulting in more secure CI.

Key words: critical infrastructure, protection, resilience, vulnerability, adaptability

Introduction

Critical Infrastructure Resilience (CIR) is the latest segment of activities and measures aiming to ensure the continuity of operation of critical infrastructures (CI). Combination of importance and vulnerability of CI was recognized as the serious issue in 90ties in the United States and various steps have been taken from that time till today to secure CI and its operation.

Critical Infrastructure Protection (CIP) is a concept that relates to the preparedness and response to serious incidents that involve the critical infrastructure of a region or nation. In Europe, the European Programme for Critical Infrastructure Protection (EPCIP) refers to the doctrine or specific programs created as a result of the European Commission's directive EU COM(2006) 786 which designates European critical infrastructure that, in case of fault, incident, or attack, could impact both the country where it is hosted and at least one other European Member State. Member states are obliged to adopt the 2006 directive into their national statutes[2].

However, it is very difficult to predict an adequate number of major threats that would allow conducting the preparedness

2 *Presidential Decision Directives – PDD*, The White House Washington, May 22, 1999, retrieved December 27, 2019. https://fas.org/irp/offdocs/pdd/pdd-63.htm

and response at the level which would ensure the sufficient operation of CI under any circumstances. Therefore, to cover for the unexpected in that domain, the Critical Infrastructure Resilience (CIR) concept has been developed. This review article presents the current situation in CIR field with selected examples.

Review of Critical Infrastructure Protection

Critical infrastructure (CI) involves elements that are fundamental to the normal operations of the human society. Resilience can be defined as the capacity to prevent, adapt, withstand and recover swiftly from both intentional and unintentional attacks. To achieve research objectives, a systematic review approach [Grant & Booth, 2009] can be used to identify and select related and relevant literature sources. This review technique can guarantee the quality and reliability of selected articles.

CIP approaches were analyzed based on obtained information obtained about them from bibliographic literatures: reports, articles, white papers and guideline to arrive at informed insights [DHS, 2013].

What seems new and perhaps not well reflected – at least directly in most of the critical infrastructure modeling and security approaches (tools, techniques, and methodologies) – is the concept of addressing 'resilience'. Most CIP approaches reviewed mainly focus on exploring concepts and phenomena related to security, reliability, dependability and risks in CIs. The first type of resilience that was added to the inoperability input-output modeling (IIM) is restorative resilience or the speed of recovery after a disruption, including this type of resilience changes the static IIM into a DIIM (Dynamic IIM) [Alcaraz & Zeadally, 2015].

A second type of economic resilience is "adaptive resilience" which refers to the change in the speed of recovery of a sector during the recovery period. One category of key assets comprises the diverse array of national monuments, symbols, and icons that represent our Nation's heritage, traditions and values, and political power. Identifying and prioritizing which assets of an infrastructure are most essential to its function, or pose the most significant danger to life and property if threatened or damaged, is necessary for developing an effective protection strategy.

The European Commission has taken the initiative to organize a network consisting of research and technology organizations within the European Union (EU) with capabilities in critical infrastructure protection. Preparatory studies and road mapping were carried out in 2009–2010 by the European Commission's Joint Research Centre on behalf of the Directorate-General for Home Affairs. The characteristics were planned on the basis of the priorities of the EU member state governments and critical infrastructure stakeholders, and in coherence with EU critical infrastructure protection policy in general. The network of laboratories is called the European Reference Network for Critical Infrastructure Protection (ERNCIP). It is intended to be a long-term, sustainable grouping with a light management structure based on existing European laboratories and facilities. Its main objectives are to agree on common test methodologies and standards, recommend security certification schemes, develop methods for laboratory accreditation, promote the exchange of good and best practices for critical infrastructure protection, and help the development of a single market in the EU for critical infrastructure protection related products and services [Lewis et al., 2013].

Selected concepts of Critical Infrastructure Resilience

Resilience in a critical infrastructure system can be viewed as a quality that reduces vulnerability, minimizes the consequences of threats, accelerates response and recovery, and facilitates adaptation to a disruptive event. Resilience is defined in Webster's Unabridged Dictionary as "the ability to bounce or spring back into shape, position, etc., after being pressed or stretched." Definitions vary slight, but they all link the concept of resilience to recovery after physical stress. The development and subsequent strengthening of the resilience of any set of critical infrastructure subsystems is a painstaking process in terms of design, time, and resources, and one that requires clearly defined initial as well as functional conditions. Defining such conditions can be understood as the overall concept of resilience for these subsystems in a critical infrastructure system [Ouyang, 2014].

The setting of the management process for protecting critical infrastructure elements, comprising the framework for strengthening resilience, can be regarded as the principal initial condition. Conversely, the fundamental functional condition is the unambiguous specification and perception of factors determining critical infrastructure resilience.

Designation of critical infrastructure elements is the initial sub-process of protection management. This sub-process hinges on the correct setting of criteria for designation of critical infrastructure elements on the European, national, and regional levels. In this phase of the process, it is equally important to consider the suitability of implementing an appropriate approach to element designation, which can be based on either the top-down or the bottom-up principle.

The fundamental functional condition for strengthening the resilience of critical infrastructure subsystems is the unambiguous specification and perception of factors that determine it. In this context, the resilience of a critical infrastructure system must be understood as a cyclic process of continual improvement of prevention, absorption, recovery, and adaptation.

The first phase of the critical infrastructure resilience cycle is prevention. Absorption is initiated if a subsystem is impaired due to a disruptive event, and is determined by the robustness of the critical infrastructure subsystem. The recovery phase starts after the effects of a disruptive event have worn off. This phase is characterized by recoverability, which is the capacity of a subsystem to recover its function to the original and/or required level of performance. The final phase of the critical infrastructure resilience cycle is adaptation, which is essentially the ability of an organization to adapt an operated subsystem to the potential recurrence of a disruptive event—i.e., to learn from previous disruptive events.

Critical infrastructure subsystem resilience can be understood as a condition formed by three types of factors: 1) Factors determining resilience (i.e., components and variables of technical and organizational resilience); 2) factors limiting resilience (i.e., statutory regulation of the operation of infrastructure or the level of available financial resources); and 3) factors affecting resilience (i.e., threats or resilience strengthening instruments).

- Factors Determining Robustness: Robustness is the ability of an element to absorb the impacts of a disruptive event. These impacts may be absorbed via the structural qualities of buildings or the technologies used (i.e., structural robustness) and/or via security measures (i.e., security robustness).

- Factors Determining Recoverability: Recoverability is the capacity of an element to recover its function to the original (required) level of performance after the effects of a disruptive

event have ended. With respect to critical infrastructure, recoverability is understood as reparability, in which case, only the damaged or destroyed components of an element are repaired or replaced.

- Factors Determining Adaptability: Adaptability is the ability of a critical infrastructure operator (i.e., an organization) to prepare an element for the recurring effects of a previous disruptive event. Adaptability is determined by the internal processes of an organization focused on creating optimal conditions for the strengthening of resilience.

Element resilience affects the dynamics of the performance of the services provided by an element in response to a disruptive event [Tague, 2005], [Twidale & Floyd, 2008].

Critical infrastructure system resilience is also defined as the ability to absorb, adapt to, and/or rapidly recover from a potentially disruptive event. In this context, it can be understood as a condition closely related to the performance function of individual subsystems. The strengthening of resilience is based on the continual enhancement of the level of factors which determine it [Denyer, 2017]. Sustained attention should be devoted to these factors in the areas of both technical resilience (i.e., robustness and recoverability) and organizational resilience (i.e., adaptability). At the same time, it is equally important also to reflection factors hindering resilience (i.e., statutory regulation of the infrastructure's operation or the availability of financial resources) and factors that affect it (i.e., threats or resilience strengthening instruments). These principles are usually acceptable across individual sectors of critical infrastructure.

However, in order to implement the evaluation system effectively, it is essential that this accord also manifests at deeper levels, such as the level of individual resilience factors, the action of which varies significantly in different critical infrastructure sectors [ISO 31000, 2018].

CIR activities and examples

In systems engineering, the goal of the architecting process is to reduce ambiguity and narrow the alternative solution space. In infrastructure systems, ambiguity exists in the functional and logical interrelationships that exist across system boundaries, and in the definition and application of resilience to these systems. Critical infrastructure is the set of

systems, networks and assets that provide vital services and capabilities to the served population. Critical infrastructure is characterized by the functions of the segments that comprise it and the interrelationships that exist across those segments [DHS - Critical infrastructure].

Critical infrastructure systems are vulnerable to disruptive events. Disruptive events result from natural or man-made disasters and other catastrophic events which degrade system performance with respect to a Key Performance Indicator (KPI). Critical Infrastructure Segments: Dams (Agriculture and Food & Defense Industrial Base), Water (Postal and Shipping & Critical Manufacturing), Energy (Banking and Finance & Nuclear Reactors, Materials and Waste), Communication (Transportation Systems & Healthcare and Public Health), Chemical (Government Facilities & Commercial Facilities), Emergency Services (National Monuments & Information Technology). Infrastructure segments that provide services which address the basic needs of the served population are those in which resilience is most important. This is similar to the individual satisfying Maslow's hierarchy of needs. "A Fuzzy Approach for Assessing Architecture Resilience"; Important functional, logical and operational interdependencies are often overlooked by existing modeling approaches [Kujawski, 2006], [Rinaldi et al., 2001]. The functional relationships and logical dependencies that are woven throughout these systems dictate how well each segment can perform, and the degree to which services are rendered for other infrastructure segments.

Fuzzy logic is approached in a two-step process:

1. Identify infrastructure segments where resilience is apriority architecture attribute using expert judgment for functional, logical and operational interdependencies in concert with inoperability input-output modeling (IIM), dynamic IIM, or other existing interdependency analysis methods.

2. Assess infrastructure architecture resilience using a fuzzy rule set tailored to the specific resilience metrics and characteristics most appropriate to the infrastructure architecture under consideration.

Several methods have been developed to forecast the impacts of a disruptive event using information about the system and interactions and interdependencies present

throughout the system. Using the results from the IIM, infrastructure segments can be prioritized based on the dependencies that exist across the infrastructure system. This methodology does not require any changes to the inoperability modeling methodology selected from among [Haimes et al., 2005], [Lian & Haimes, 2006] or [Kujawski, 2006].

"Application of the Fuzzy Architecture Assessment"; Alternative methods have been proposed to identify key infrastructure segments through the expected impacts resulting from a disruptive event [Haimes et al., 2005], [Lian & Haimes, 2006] or [Kujawski, 2006]. The results of these approaches are used to prioritize the identification of, and investment in, more resilient architecture alternatives that better support the services provided by these systems in the face of disruptive events. This approach requires the definition of resilience attributes and the mapping of fuzzy membership functions to each attribute. These attributes can be ascribed by operators and subject matter experts by clearly defining the relationships that exist across the infrastructure within the contexts of the performed functions. Resilience attributes of adaptability and redundancy are considered for the example architecture assessment [Jackson, 2007].

A fuzzy approach accommodates ambiguity in the assessment of key system attributes, and brings together different measurement scales to provide a combined outcome. For the architecture assessment, these differences are implemented by differentiating the fuzzy membership functions associated with the resilience attributes that are key to each infrastructure segment. IF adaptability is high AND robustness is moderate THEN resilience is high; IF adaptability is moderate AND robustness is moderate THEN resilience is low; IF adaptability is high AND robustness is high THEN resilience is high. For defuzzification, each satisfied antecedent block is evaluated and produces the membership for the resilience consequent. The degree of membership for each fuzzy resilience set is evaluated using the mean of maximum defuzzification rule [Muller, 2012].

As the interesting example of current CIR there is an article which review s the responses of four of the five Nordic countries to this challenge, namely Denmark, Finland, Norway and Sweden. The article analyzes their strategies and conceptual development, highlighting the common trends and

differences. In so doing, it argues that these countries have a better starting point for the task of making their critical infrastructure resilient than most of the EU. This is due to the fact that even before the resilience debate emerged, these countries had based their policies on securing vital societal functions rather than the individual infrastructures that support these functions. The article concludes that some kind of Nordic model can really be identified when it comes to approaches towards critical infrastructure resilience [Pursiainen, 2018].

It has been widely reported that industrial control systems underpinning critical infrastructures ranging from power plants to oil refineries are vulnerable to cyber attacks. A slew of counter measures have been proposed to secure these systems, but their adoption has been disappointingly slow according to many experts. Operators have been reluctant to spend large sums of money to protect against threats that have only rarely materialized as attacks. But many security countermeasures are dual-use, in that they help protect against service failures caused by hackers and by accidents. In many critical infrastructure sectors, accidents caused by equipment failures and nature occur regularly, and investments for detecting and possibly preventing accidents and attacks could be more easily justified than investments for detecting and preventing attacks alone [Papa et al., 2013].

Conclusions

In regard to Critical Infrastructure security and operation, there has been a shift in emphasis in recent years from protection to resilience. CIP remains in focus and still is one of the key systems that the society relies upon to ensure the continuity of operation of CI. One of the good examples is the European Reference Network for Critical Infrastructure Protection (ERNCIP) However, the shift in emphasis towards resilience reflects the acknowledgment that complete protection is impossible to achieve and that the level of efforts required organizing and maintaining the desired level of protection is not cost-effective in relation to risks and vulnerabilities.

CI systems are very different in their structures and ways of operation. Critical Infrastructure Protection (CIP) and Critical Infrastructure Resilience (CIR) activities are further complicated by CI interdependencies, cascade effects and similar factors. Therefore it is important to enhance efforts on

the global level in relation to CIP and CIR, with emphasize on the latter. Selected concepts of CIR with examples, as presented in this Article, should assist that goal.

References

Alcaraz, C., Zeadally, S., “Critical infrastructure protection: Requirements and challenges for the 21st century,” Int. J. Crit. Infrastruct. Prot., vol. 8, pp. 53–66, 2015.

Contini, S., Matuzas, V., Analysis of large fault trees based on functional decomposition,ReliabilityEngineering & SystemSafety,Vol.96,no.3,383-390

Denyer, D. Organizational Resilience: A Summary of Academic Evidence, Business Insights and New Thinking, 1st ed.; BSI and Cranfield School of Management: Cranfield, UK, 2017.

DHS - Department of Homeland Security, “NIPP 2013: Partnering for Critical Infrastructure Security and Resilience,” 2013.

DHS - Department of Homeland Security, Critical infrastructure, https://www.dhs.gov/cisa/critical-infrastructure-sectors

Grant, M. J., Booth, A. “A typology of reviews: an analysis of 14 review types and associated methodologies,” Health Info. Libr. J., vol. 26, pp. 91–108, 2009.

Haimes, Y. Y., Horowitz, B. M., Lambert, J. H., Santos, J. R., Lian, C., Crowther, K. G., Inoperability input-output model for interdependent infrastructure sectors. i: Theory and methodology, Journal of Infrastructure Systems 11 (2) (2005) 67–79.

ISO 31000. Risk Management–Guidelines; ISO: Geneva, Switzerland, 2018.

Jackson, S., System resilience: Capabilities, culture and infrastructure (2007).

Kujawski, E., Multi-period model for disruptive events in interdependent systems, Systems Engineering 9 (4) (2006) 281–295.

Lewis, A., Ward, D., Cyra, L., Kourti, N., European Reference Network for Critical Infrastructure Protection, International

journal of critical infrastructure protection 6 (2013) pp. 51–60

Lian, C., Haimes, Y.Y., Managing the risk of terrorism to inter dependent infrastructure systems through the dynamic inoperability inputoutput model, Systems Engineering 9 (3) (2006) 241–258.

Muller, G., Fuzzy architecture assessment for critical infrastructure resilience, Procedia Computer Science 12 (2012) pp. 367 – 372

Ouyang, M., "Review on modeling and simulation of interdependent critical infrastructure systems," Reliab. Eng. Syst. Saf., vol. 121, pp. 43–60, 2014.

Papa, S., Casper, W., Moore, T., Securing waste water facilities from accidental and intentional harm: A cost-benefit analysis, International journal of critical infrastructure protection 6 (2013) pp. 96–106

Pursiainen, C., Critical infrastructure resilience: A Nordic model in the making?, International Journal of Disaster Risk Reduction 27 (2018) pp. 632–641

Rinaldi, S., Peerenboom, J., Kelly, T., Identifying, understanding, and analyzing critical infrastructure interdependencies, Control Systems, IEEE 21 (6) (2001) 11 –25

Tague, N.R. Quality Toolbox, 2nd ed.; ASQ Quality Press: Milwaukee, WI, USA, 2005.

Twidale, M.B.; Floyd, I. Infrastructures from the bottom-up and the top-down: Can they meet in the middle? In Proceedings of the Tenth Anniversary Conference on Participatory Design (PDC '08); Indiana University Indianapolis: Bloomington, IN, USA, 2008; pp. 238–241.

Wikipedia - CIP; Critical infrastructure protection, https://en.wikipedia.org/wiki/Critical_infrastructure_protection