International Journal of Management and Applied Science, ISSN: 2394-7926 Volume-8, Issue-3, Mar.-2022
http://iraj.in

FRAMEWORK FOR CRITICAL INFRASTRUCTURE SECURITY RATING

[1]DORAH CHAUKE, [2]FHUMULANI MPHADZHA

Council for Scientific and Industrial Research
E-mail: [1]dchauke2@csir.co.za,[2]fmphadzha@csir.co.za

Abstract - Proper functioning of a nation's economy and society requires that its critical infrastructure is safe and secure. The protection of critical infrastructure is becoming a growing concern to national governments, infrastructure managers and local authorities. Hence, the need to develop a framework for evaluating the safety of these critical infrastructures. Critical infrastructures are interconnected and therefore face a myriad of vulnerabilities and threats. A comprehension of these vulnerabilities is essential in developing a framework for evaluating security levels of critical infrastructures. In addition to evaluating how safe and secure the infrastructure is, a framework is essential in for identifying security gaps that need to be addressed. This paper proposes a framework for rating critical infrastructure's security level using weighted variables.

Keywords - Critical Infrastructure, Security Rating, Vulnerability Assessment

I. INTRODUCTION

Infrastructure is defined as any building, centre, establishment, facility, installation, pipeline, premises or systems needed for the functioning of society, the Government or enterprises of the Republic, and includes any energy production, transmission and distribution, food and water, transportation, telecommunications, health, and information systems [1][2]. Critical Infrastructure Protection (CIP) has become of increasing concern to national governments, infrastructure managers, and local authorities [3]. Therefore, there is a need for nations to develop frameworks for evaluating these infrastructures. Critical infrastructure represents mutually connected and mutually dependent systems from different sectors of a human system [3]. These interdependencies could trigger cascading effects in multiple critical infrastructures when one critical infrastructure is disrupted, damaged or destroyed [4]. Thus, the safety of each system ensures the safety of the overall critical infrastructure system[5]. Four types of interdependencies were identified i.e.: (i)physical;(ii)geographic;(iii)cyber; (iv) andlogical[4].

- A physical interdependency exists when a critical infrastructure requires resources or raw materials from other infrastructures.
- A geographic interdependency exists when multiple infrastructures share a close spatial proximity, and a problem in one critical infrastructure can reach the other critical infrastructures.
- A cyber interdependency is the result of a dependency on information and communications systems.
- A logical interdependency exists when systems, actions or decisions connecting an agent in one infrastructure to an agent in another infrastructureare not physical, geographic, or cyber in nature (e.g., bureaucratic or political decisions).

In contrast to the latter, due to an increase in transnational, and global dependencies in critical infrastructures, the European Union (EU) directive proposed five types of interdependencies: (1) physical, (2) information, (3) geospatial, (4) policy and process and (5) societal.

When examining the case of multiple infrastructures connected as a "system of systems," their interdependencies must be considered.

II. INTERDENDENCIES BETWEEN CRITICAL INFRASTRUCTURES

The connection of multiple critical infrastructures connected as a "system of systems," causes to their interdependencies with each other. Infrastructure interdependency is defined as a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlatedto the state of the other[6].

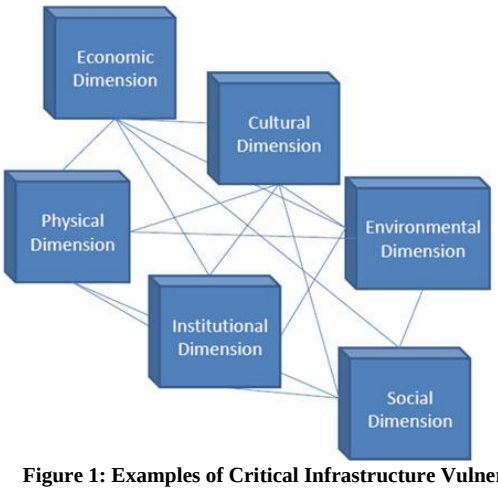

Figure 1: Examples of Critical Infrastructure Vulnerability Dependencies

Figure 1 above depicts critical infrastructure vulnerability dependencies. In addition to these, transnational and extra-sovereign dependencies that extend beyond the mandate of sovereign states exists[7]. This indicated that the scope of what needs to be protected and against what has increased.

- Social dimension: propensity for human wellbeing to be damaged by disruption to individual (mental and physical health) and collective (health, education services, etc.) social systems and their characteristics (e.g., gender, marginalization of social groups).
- Economic dimension: propensity for loss of economic value from damage to physical assets and/or disruption of productive capacity.
- Physical dimension: potential for damage to physical assets including built-up areas, infrastructure, and open spaces.
- Cultural dimension: potential for damage to intangible values including meanings placed on artefacts, customs, habitual practices and natural or urban landscapes.
- Environmental dimension: potential for damage to all ecological andbio-physical systems and their different functions. This includes particular ecosystem functions and environmental services but excludes cultural valuesthat might be attributed.
- Institutional vulnerability: potential for damage to governance systems, organizational form and function as well as guiding formal/legal and the complex dependencies between critical infrastructure types gives rise to vulnerabilities and threats for these infrastructures. For example, the electricity and communication networks are particularly vital for the smooth functioning of other infrastructures.

III. VULNERABILITIES AND THREATS FACING MODERINFRASTRUCTURE

In a hyper connected world, infrastructures are vulnerable to a myriad of threats. Critical Infrastructures in particular are vulnerable due to their interdependencies. Disruption in critical infrastructure can result in life-threatening and general debilitating consequences to the population, economy and government [8]. Vulnerabilities and threats to critical infrastructure have always existed, however, the impact in the 21st century has local, regional and cross border implications.

3.1. Cyber Security Threats

Industry 4.0 presents opportunities and challenges to Cyber security threats. Opportunities presented by Industry 4.0 allow for automation and improve operations. However, there are challenges which include such issuesas energy and power generation failures, online banking systems malfunction, transportation accidents, and hazardous material accidents. Interconnectivity and interdependencies increase vulnerabilities and risks in critical infrastructures.

3.2. Physical Security Threats

Critical infrastructures must be properly secured to avoid unauthorized access from either people or cars. Only authorized entities should be allowed access. Hence, the infrastructures should have effective access control mechanisms to deter physical security threats.

The above vulnerabilities and threats to modern infrastructures requires organizations and businesses to protect these infrastructures. In order to do this, an assessment of infrastructure security levels is essential. A closer look at infrastructure assessment models follows.

IV. INFRASTRUCTURE SECURITY ASSESSMENT MODELS

The military uses several decision-making support tools to assess the center of gravity (COG) to perform vulnerability assessments of operational areas. Vulnerability assessment is used to identify critical vulnerabilities of an adversary, then develops a coherent set of friendly actions to attack these vulnerabilities by means that may be lethal, nonlethal, or a combination of the two [9]. The COG in the military context is defined as a physical entity capable of accomplishing the organization's ends, such as a military unit [9]. The tools used in the military environment for vulnerability assessments include the mission, symbolism, history, accessibility, recognizability,population, and proximity (MSHARPP) model and the criticality, accessibility, recuperability, vulnerability, effect, and recognizability (CARVER) model.Additionally, the American Society of Civil Engineers (ASCE) developed an Infrastructure Rating Tool (IRT) based on Multi Criteria Decision Modeling (MCDM)[10]. These models are discussed below:

4.1. MISHARP Model

MSHARPP examines seven variables: mission, symbolism, history,accessibility, recognizability, population, and proximity[9]. It is a targetingtool geared toward assessing personnel vulnerabilities but can also be used for facilities, units, or other assets.

4.2. CARVER Model

Another assessment tool used by the military to assess criticality and vulnerability CARVER.

Model[9]. This model is used to assess enemy infrastructureusing a matrix that evaluates assets against a criteria list.

4.3. ASCE Infrastructure Rating Tool

The Infrastructure Rating Tool (IRT developed by ASCE is based on multiple criteria decision making [10]. Criteria used in this model are: Condition, Capacity, Operation and Maintenance, Funding, Future Need, Public Safety and Resilience. Models discussed above all use multiple criteria to rate infrastructure status. However, the MISHARP and CARVER models are suitable in assessing infrastructure security levels and hence, some criteria for these models will be used and adapted for the proposed model.

V. VARIABLES FOR RATING CRITICAL INFRASTRUCTURE SECURITY LEVEL

For the proposed security rating model, variables for rating critical infrastructure have to be decided upon. These variables were deduced from the MISHARP and the CARVER models. These variables are discussed below:

5.1. Criticality

Criticality can be defined asa relative measure of impacts of frequently occurring defects and failures[5]. The effects of defects and failures can furtherbe categorized into the following groups [11]:

- Critical: Risk is critical if a key term or major program milestonecannot be achieved
- Serious: Risk is serious if major slip in key milestone or critical path impacted
- Moderate: Risk is moderate if minor slip in key milestones and not able to meet need dates
- Minor: Risk is minor if additional resources are required but able to meet need dates
- Negligible: Risk is negligible if minimal or no impact.

5.2. Recoverability

Recoverability is the ability of an element to recover itsfunctions to its original state after the disruption has seized. Recoverability can be determined by the following factors [12]:

- Material resources: Refers to the availability of componentsrequired for the repair or replacement of damaged or destroyed parts of the element
- Financial resources: Refers to the availability of financial resources to finance the rapid recovery of the element.
- Human resources: Refers to the availability of human resources with the required level of qualifications.
- Recovery processes: Refers to the processes facilitating the rapid recovery

5.3. Accessibility

5.3.1. Physical Accessibility

Physical accessibility in this paper relates to security access. Security must prevent physical infrastructure misuse which can result in the misuse or harm of protected information and infrastructure [13].

Security system installed is influenced by the risk the infrastructure is exposed to. The nature of risks includes unauthorized access, fire etc [13].

5.3.2. Data Accessibility

Data access to any service should be limited to authorized and authenticated individuals [13]. Insecure authentication methods expose the systems to unauthorized access, which could result in data theft, service modifications, or a denial of service [13].

VI. PROPOSED MODEL

This section of the paper looks into a proposed Infrastructure Security Rating Model and corresponding application model. The model seeks to provide a quick assessment of the level of security for critical infrastructure. The model is explained below:

6.1. Infrastructure Security Rating Model

Table 1 represents the variables which influence the infrastructure security rating. The variables will be used to determine the level of security an infrastructure might require. A weighting score has been assigned to the variables. The variable with a higher weight ratingis assigned deemed important as it has greater influence on results. The variables with reference to scoring the framework are further explained below:

- Interdependency: Interdependency scoring is based on the impact infrastructuredisruption has on trade.A higher scoring is given if international trade will be impacted due to infrastructure disruption. The scoring will cascade down to lower levels and respective rating will be assigned.
- Vulnerability:Vulnerabilityscoring is based on the level of physicaland cyber security implemented withininfrastructure. If the infrastructure is viewed to be more vulnerable to organizedcrime, the security rating suggested is high since high security will be required to protect the infrastructure and the rating level cascades down depending onthe source of vulnerability

- Criticality: Criticality scoring is based on the impact risks haveon infrastructure. If the majority of risks on the infrastructure have greater impact and the possibility of occurring is high, then a high rating will be assigned. The rating method will cascade as the risk reduces.
- Recoverability:Recoverability scoring is based is on how quickly the infrastructure can return to full functionality after a disruption as well as financial implication of the downtime. The longer the downtime usually translates to higher financial implication. A higher rating is assigned if down time islonger, and the rating cascades down as downtime reduces.
- Accessibility: Accessibility scoring is grouped into physical and data accessibility. Physical accessibility focuses on rules ofentry that are in place. Dataaccessibility focuses on data protection.A higher rating is assigned if the level of security at entry is low. This implies that the infrastructure requires more security, and similarly easy accessibility to data with attract a higher score. The scoring cascades down as security measures increase.

Variables	Rating
Interdependency Weight = 0.3	
International trade disrupted	10
National trade disrupted	8
Provisional trade disrupted	6
Municipal trade disrupted	4
No dependency	1
Vulnerability Weight = 0.2	
Vulnerable to vandalization by organized crime	10
Vulnerable to Vandalization by community	8
Vulnerable to Natural disasters	6
Vulnerable to vandalization by wildlife	4
Invulnerable	1
Criticality Weight = 0.2	
Mostly Critical	10
Mostly Serious	8
Mostly Moderate	6
Mostly Minor	4
Mostly Negligible	1
Recoverability Weight = 0.1	
Infrastructure maintenanceor rebuild requiresat least 2Years	10
Infrastructure maintenance or rebuild requiresat least 1Year	8
Infrastructure maintenanceor rebuild requiresat least 6Months	6
Infrastructure maintenanceor rebuild requiresat least 1Month	4
Infrastructure maintenanceor rebuild requiresat least 2 Week	1
Financial ImplicationWeight = 0.1	
Infrastructure downtime more than 2 year	10
Infrastructure downtime more than 1 year	8
Infrastructure downtime more than 6 Month	6
Infrastructure downtime more than 1 Month	4
Infrastructure downtime more than 2 weeks	1
Physical Accessibility Weight = 0.05	
Free infrastructure entry	10
Moderate infrastructure security	8
Restricted infrastructure security	6
High infrastructure security	4
Maximum infrastructure security	1
Data Accessibility Weight = 0.05	
Data easily accessible	10
Data access restricted	8
Data is secret	6
Data is top secret	4
Intelligence data	1

Table 1: Infrastructure security Rating Model

Instructions:
1.Allocate arating for each variable based on infrastructure assessment.Onerating should be allocated per variable.
2.Multiply the rating with corresponding weight
3.Add all weighted ratings to obtain total score
4.Use the application model to check which classification does the total score correspond with.

6.2. Application Model

Table 2presents the application model for infrastructure rating and classification of critical infrastructure. The model obtains the rating score from table 1 and then classifies the infrastructure based on obtained rating score.

Rating Score	Security Classification	Security assessment	Security Rating
0-1	Category 1	High infrastructure security	Highest
2-3	Category 2	Good infrastructure security	High
4-5	Category 3	Acceptable infrastructure security	Moderate
6-7	Category 4	Poor infrastructure security	Low
8-10	Category 5	Inadequate infrastructure security	Lowest

Table 2: Infrastructure Security Application Model

VII. CONCLUSION AND FUTURE WORK

The proposed framework for rating critical infrastructure security can be used to evaluate how secure an infrastructure is. Based on outcomes from the rating, corrective measures or interventions to improve the rating can be done.

There is an opportunity to use the proposed framework in other entities besides infrastructures which is a potential future work.

REFERENCE

[1] B. Baker, R. J. Eagan, P. K. Falcone, J. M. Harris, G. V. Herrera, W. C. Hines, R. L. Hutchinson, A. K. Moonka, M. L. Swinson, E. K. Webb, T. D. Woodall and G. D. Wyss, "A Scalable Systems Approach for Critical Infrastructure Security," Sandi National Laboratories, California, 2002.

[2] South Africa, "Critical Infrastructure Protection Act 8 of 2019," Government Gazette No. 42866, vol. 653, pp. 1-59, 2019.

[3] Z. Dvorak , E. Sventekova, D. Rehak and Z. Cekerevac, "Assessment of Critical Infrastructure Elements in Transport," 10th International Scientific Conference Transbaltica 2017: Transportantion, Science and Technology, pp. 548-555, 2017.

[4] Alcaraz and S. Zeadally, "Critical Infrastructure Protection: Requirements and Challenges for the 21st Century," International Journal of Critical Infrastructure Protection, vol. 8, pp. 53-66, 2015.

[5] Prochazkova, "Critical Infrastructure Safety Management," Transactions of Transport Science, vol. 3, no. 4, pp. 157-168, 2010.

[6] T. Xu and A. J. Masys, "Critical Infrastructure Vulnerabilities: Embracing a Network Mindset," in Exploring the Security Landscape: Non-Traditional Security Challenges, Switzerland, Springer International Publishing , 2016, pp. 177-192.

[7] O. Fjader, "National Security in a Hyper-Connected World," in Exploring the Security Landscape: Non-Traditional Security Challenges, Switzerland, Springer International Publishing, 2016, pp. 31-58.

[8] W. Hurst, M. Merabti and P. Fergus, "A Survey of Critical Infrsatructure Security," in International Conference on Critical Infrastructure Protection, Heidelburg, 2014.

[9] C. M. Schnaubelt, E. V. Larson and M. E. Boyer, Vulnerability Assessment Method Pocket Guide: A Tool for Center of Gravity Analysis, Santa Monica, CA: RAND Corporation, 2014.

[10] A. Amekudzi, R. Shelton and T. R. Bricker, "Infrastructure Rating Tool: Using Decision Support Tools to Enhance ASCE Infrastructure Report Card Process.," Leadership and Management in Engineering, vol. 13, no. 2, pp. 79-82, 2013.

[11] Chen , H. Ni and N. Chen , "Some extensions on risk matrix approach," Elsevier, 2010.

[12] Rehak, P. Senovsky and S. Slivkova, "Resilience of Critical Infrastructure Elements and Its Main Factors," Faculty of Safety Engineering, VSB—Technical University of Ostrava, 2018.

[13] Atieh, "Assuring the Optimum Security Level for Network, Physical and Cloud Infrastructure," EGM- IT Infrastructure Operation, Etihad Etisalat – MOBILY, 2021.

★★★