Chapter 3

RISK-BASED CRITICALITY ANALYSIS

Marianthi Theoharidou, Panayiotis Kotzanikolaou and Dimitris Gritzalis

Abstract Critical infrastructure protection requires the evaluation of the criticality of infrastructures and the prioritization of critical assets. However, criticality analysis is not yet standardized. This paper examines the relation between risk and criticality. It analyzes the similarities and differences in terms of scope, aims, impact, threats and vulnerabilities; and proposes a generic risk-based criticality analysis methodology. The paper also presents a detailed list of impact criteria for assessing the criticality level of infrastructures. Emphasis is placed on impact types that are society-centric and/or sector-centric, unlike traditional risk analysis methodologies that mainly consider the organization-centric impact.

Keywords: Risk analysis, criticality, impact

1. Introduction

A critical infrastructure (CI) is a "service, facility or a group of services or facilities, the loss of which will have severe adverse effects on the physical, social, economic or environmental well-being or safety of the community" [6]. CIs incorporate material and information assets, networks, services and installations [4]. All CIs use information and communications technology (ICT) systems and depend strongly on these systems [3].

The importance of assessing the criticality of CIs, prioritizing them and implementing adequate security controls has been emphasized by the European Commission [8], U.S. Government [26] and other governments [6, 22]. Clearly, there is a close correlation between the protection of CIs and the mitigation of security risks faced by CIs. However, the "criticality" of a CI is a term that has not been formally defined. Unlike ICT risk analysis methodologies, criticality analysis methodologies are relatively obscure and *ad hoc* in nature. In fact, no specific standards exist for critical infrastructure protection itself, although certain security and safety standards are being used as auxiliary standards [3]. Standard CIP-002-1 (Critical Asset Identification) created by the North

American Electric Reliability Corporation [20] requires a risk-based assessment methodology to identify critical assets. However, it neither suggests a specific method nor provides detailed requirements for a suitable method. There is an urgent need to clarify how existing risk analysis methodologies can be properly utilized to assess, categorize, prioritize and protect CIs.

This paper compares risk and criticality in terms of their scope, aims, impact, threats and vulnerabilities to clarify how risk analysis methodologies can be applied to critical infrastructure protection. It defines "criticality analysis" as a special-purpose, society-centric risk analysis process applied to large-scale interdependent systems and infrastructures. The primary contributions of this paper are a generic risk-based criticality analysis methodology and a detailed list of impact criteria for assessing the criticality of infrastructures.

2. Criticality

The most common approach used to characterize an infrastructure as critical is to assess the impact level in the presence of security-related threats. Most methods focus on the consequences of an event, i.e., the "outcome of a situation or event expressed qualitatively or quantitatively as being a loss, injury, disadvantage or gain" [6]. Impact factors, or critical asset factors, are criteria used to prioritize assets and infrastructures. Impact is usually evaluated with respect to three primary characteristics [6–8, 17]: (i) scope or spatial distribution – the geographic area that could be affected by the loss or unavailability of a critical infrastructure; (ii) severity or intensity or magnitude – the consequences of the disruption or destruction of a particular critical infrastructure; and (iii) effects of time or temporal distribution – the point that the loss of an element could have a serious impact (immediate, one to two days, one week).

Intensity is usually analyzed using detailed qualitative and quantitative criteria. For example, the European Commission [7, 8] defines a minimum set of criteria that member states should consider in their critical infrastructure assessments: (i) public effect – population affected, loss of life, medical illness, serious injury, evacuation; (ii) economic effect – GDP effect, significance of economic loss and/or degradation of products or services; (iii) environmental effect – effect on the public and the surrounding environment; (iv) interdependency – interdependencies between critical infrastructure elements; (v) political effects – confidence in the government; and (vi) psychological effects – psychological effects on the population. These criteria are evaluated in terms of scope (local, regional, national and international) and time (during and after the incident).

Similarly, the U.S. National Infrastructure Protection Plan [26] lists criteria for evaluating consequences: (i) public health and safety – effect on human life and physical well-being; (ii) economic – direct and indirect economic losses; (iii) psychological – effect on public morale and confidence in economic and political institutions; and (iv) governance/mission – effect on the ability of the government or industry to maintain order, deliver essential services, ensure public health and safety, and carry out national security-related missions.

Table 1. Criticality approaches (impact factors).

Impact Criteria	**Approach**
Public Health and Safety	[7, 8, 17, 26]
Economic	[7, 8, 17, 22, 26]
Environment	[7, 8, 17]
Political/Governance/Mission	[7, 8, 17, 26]
Psychological/Social/Public Confidence	[7, 8, 17, 22, 26]
Interdependency	[7, 8, 13, 16, 22]
Complexity	[13]
Vulnerability	[13]
Market Environment	[13]
Concentration of People and Assets	[22]
Scope/Range	[7, 8, 17, 22]
Service Delivery/Recovery Time	[7, 8, 16, 17, 22]
National/Territorial Security	[17, 26]

Other proposed factors are [13]: (i) complexity; (ii) dependence on other infrastructures, by other infrastructures, by intra-infrastructure components and on information and communications technology; (iii) vulnerability, including external impact (natural hazards, construction mishap), technical/human failure, cyber attacks and terrorism; and (iv) market environment, especially the degree of liberalization, adequacy of control and speed of change.

The Canadian approach [22] is different in that the criteria are accompanied by impact scales: (i) concentration of people and assets; (ii) economic; (iii) critical infrastructure sector (international, national, provincial or regional); (iv) interdependency (physical, geographic or logical); (v) service delivery (acceptable downtime, availability of substitutes, time and cost required for recovery); (vi) public confidence (in the ability of a state to preserve public health and safety, and provide economic security and essential services).

The Dutch approach [16] uses the notion of "vitality." Indirect vitality is the degree to which other products and services contribute to the dependability of a product or service. Direct vitality is the contribution that a product or service delivers to society. The approach also engages backward and forward dependencies, the failure vs. recovery criterion (time required for minimum recovery and for full recovery) and the point of time when the major impact occurs. The Dutch risk assessment method for CIs [17] evaluates impact based on: (i) territorial security; (ii) physical safety; (iii) economic security; (iv) ecological security; (v) social and political stability; and (vi) social and psychological impact. All the criteria are evaluated in terms of range and duration.

Several terms are used in the literature to express the degree to which an infrastructure is critical. As discussed above, the principal terms are criticality [7, 8, 13, 22], vitality [16] and risk (impact or consequences) [17, 26]. Table 1 presents the impact criteria used by various approaches in the literature.

Interdependencies may be characterized as: (i) physical; (ii) cyber; (iii) geographic; and (iv) logical [23]. Another categorization of interdependencies is: (i) physical (e.g., a fallen tree causes a power outage); (ii) informational (e.g., loss of a SCADA system that monitors and controls the electrical power grid); (iii) geospatial (e.g., a flood damages key telecommunications assets); (iv) policy/procedural (e.g., a safety hazard in one subway station halts transportation throughout the subway system); and (v) societal (e.g., erosion of public confidence after the September 11, 2001 terrorist attacks) [21].

3. Security Risk and Criticality

Most of the criteria used to assess criticality are impact factors that are commonly used in risk analysis methodologies. Obviously, there is a correlation between the criticality level of a CI and the security impacts and associated security risk levels. We examine this correlation in order to define the criticality level of an infrastructure in relation to its risk level.

Criticality as a Subset of Risk. Several critical infrastructure protection impact criteria (e.g., health and safety, national security, financial loss, service loss and public confidence loss) are used in risk analysis methodologies. However, some of the more prominent risk analysis methodologies (e.g., CRAMM [9] and OCTAVE [2]) consider additional impact factors. These include competitive disadvantage (due to commercial and economic interests), legal or regulatory sanctions (due to law enforcement or non-compliance with legal or regulatory obligations), and system operation malfunctions (due to flawed management or business operations).

During a typical risk analysis, risk is assessed based on impact factors, threats and vulnerabilities. Thus, the criticality of the system is also evaluated (at least partially) as a side-effect. Indeed, the evaluated risks associated with the criticality-related impact factors include the criticality-related risks. Note that during risk analysis, some of the evaluated risks are based on impact types that are not associated with the criticality level of a system. In this sense, criticality can be considered to be a subset of the risk.

Risk as a Subset of Criticality. Certain criticality factors are not used as impact criteria in traditional risk analysis methodologies. Examples include scope, economic impact, environmental effects and dependency effects. As a result, a risk analysis conducted for a single organization (or multiple organizations in the same sector) does not evaluate risks associated with external impacts (e.g., social and/or sector-oriented consequences). For example, a criticality analysis may assess the societal impact of an incident that affects the banking sector. Such an impact may not be considered in a risk analysis conducted for an individual bank. In fact, if a risk analysis for an individual bank were to examine the impact of an event that affects the availability of the entire banking sector, it would result in a lower risk level compared with an event that only affects the availability of services at that particular bank. This

is because the bank in question would not lose its competitive disadvantage or face legal/regulatory consequences. Thus, certain criticality factors are not considered as typical risks, and risk can be viewed as a subset of criticality.

Risk vs. Criticality. Impact is the basic connecting element between risk and criticality. However, other issues should also be considered in order to clarify how risk analysis can be used when evaluating CIs.

- **Interdependency of CIs:** Risk analysis methods mainly focus on information systems, which they treat as isolated entities. Thus, they fail to capture the complexity of CI interconnections, cross-sector impacts, dependencies with other systems or CIs and cascading effects within a sector or across sectors. Therefore, the integration of key critical infrastructure protection models with risk analysis methodologies is important. Examples include critical infrastructure protection layers, the implications of dependencies between layers, and the multi-dimensional nature of the impact of an incident [1]. Approaches for interdependency identification, modeling, visualization and simulation should be embedded in risk analysis methodologies [5, 11, 19, 23, 24].

- **Impact Scope:** Risk analysis mainly evaluates internal impacts. However, criticality analysis also considers impacts external to the examined CI such as societal impacts, sector impacts and impacts to citizens that are not directly related to the examined CI (e.g., users, customers, candidate customers and contracted third parties). As a consequence, risk analysis only evaluates the factors that relate to internal impacts, while criticality analysis mainly focuses on the security risks related to external impacts (societal/sector-based impacts).

- **Impact Scale:** Since external and cascading impacts must be taken into account, the evaluated impacts tend to be higher than the internal impacts. New impact scales related to criticality factors must be defined and evaluated; these should differentiate between impact types as well as impact levels.

- **Objectives:** Although critical infrastructure protection objectives may appear to be similar to information assurance objectives (e.g., confidentiality, integrity and availability), achieving the objectives is much more complex for a CI. This is due to the global dimension of CIs, the complexity due to inter- and intra-dependencies, new threats, and dependability and survivability issues [3]. Also, attacks can be the result of structural threats (e.g., natural disasters, accidents, strikes, epidemics, technical failures, human error and supply shortages) or intentional attacks, which may be executed by actors ranging from disgruntled employees to terrorists and nation states. These issues are generally not considered in traditional risk analysis [4].

Table 2. Risk analysis vs. criticality analysis.

	Risk Analysis	**Criticality Analysis**
Aim	Organization	Society
Scope	Internal assets	Internal assets and interdependencies
Impact Type	Organization-centric	Society-centric
Threats	System	CI and interdependencies
Vulnerabilities	System	CI and interdependencies
Impact Scale	Variable	Higher

Table 2 compares and contrasts risk analysis and criticality analysis. Based on this summary, we provide two definitions:

DEFINITION 1 (Criticality): Criticality is the: (i) level of contribution of an infrastructure to society in maintaining a minimum level of national and international law and order, public safety, economy, public health and environment, or (ii) impact level to citizens or to the government from the loss or disruption of the infrastructure [16].

DEFINITION 2 (Criticality Analysis): Criticality analysis is the process of assessing the criticality level of an infrastructure. It is a special-purpose, society-centric risk analysis process that attempts to protect infrastructures that are vital to society. Criticality analysis mainly considers the societal impacts instead of the organizational impacts. The scope of the analysis is extended to cover interdependent infrastructures and, thus, possible threats and vulnerabilities. Criticality analysis is performed on large-scale CIs that provide services to large numbers of users/citizens and, thus, it usually involves higher impact scales.

The results of a risk analysis of a CI and/or its interdependent CIs may be used as input when assessing the criticality level of the CI. Since there are common impacts, threats and vulnerabilities in both processes, risk analysis can provide preliminary metrics, especially those obtained by examining the security risks based on commonly-used impacts, threats and vulnerabilities.

4. Generic Criticality Analysis Methodology

This section describes a generic criticality analysis methodology based on the preceding discussion of security risk and criticality. The methodology has six steps, which are described below.

- **Step 1: Identify Critical Assets.** As in risk analysis, the assets of the CI under consideration are documented (facilities, services, hardware, software, information, human resources, etc.). This task may be performed with the assistance of infrastructure asset owners.

- **Step 2: Define Interconnections and Dependencies.** Interconnected CIs should be defined. These may be categorized as dependent CIs (i.e., infrastructures that depend on the examined CI) and requisite CIs (i.e., CIs that are required by the examined CI for its operation). Although this process has similarities with the definition of third parties during risk analysis, it serves a different purpose. In risk analysis, third parties are only considered if they pose security risks to the examined system/organization (e.g., service providers, software/hardware suppliers and customers). In criticality analysis, the interconnected CIs that imply a general societal risk should be considered even if they do not imply any risk for the CI. Defining the interconnections and dependencies ensures that the criticality impacts consider more than just the organization/system-oriented impacts; in particular, it helps evaluate the global threats and common vulnerabilities within the interconnected CIs.

- **Step 3: Evaluate Criticality Impact.** After the interconnections and dependencies have been identified, the criticality impact factors are examined. As explained in Section 3, the impact factors have an extended scope and focus on societal rather than internal impacts (e.g., public safety, public services and economy). The assessment of impact is based on scope, severity and time. The analysis may take into account several scenarios where a critical asset or service is unavailable or where the confidentiality or integrity of information is affected.

- **Step 4: Define Threats.** Since criticality depends on the interconnected CIs, an extended list of threats must be created. Examples of threats include masquerading as authorized users, unauthorized use of resources, introduction of malware, interception or manipulation of communications, communication failures, technical failures, power failures, software failures, operational errors, maintenance errors, user errors, fire, water damage, natural disasters, staff shortages, theft, willful damage, terrorism and espionage [9].

- **Step 5: Evaluate Threat and Vulnerability Levels.** Possible threats are evaluated for each CI asset. The threat levels should consider the possibility of realizing a threat within the examined CI as well within the scope of CI interconnections and dependencies. The likelihood of a threat can be based on the history of previous incidents, existing literature and interviews with experts. The threats that affect a CI are a superset of those used in traditional risk analysis. The vulnerabilities that lead to incidents must also be identified and evaluated; this is by no means a trivial task because vulnerabilities can be inherited by other CIs.

- **Step 6: Evaluate Associated Criticality Risk Factors.** As in typical risk analysis, risk is quantified by taking into account all possible combinations of threats, vulnerabilities and criticality impacts for each asset, i.e., risk = threat $\times$ vulnerability $\times$ criticality impact.

Table 3. Scope impact factors.

Impact Factor	Very High	High	Medium	Low
Population Affected	>10,000	1,000–10,000	100–1,000	<100
Concentration (persons/km^2)	>750	500–750	250–500	<250
Range	International	National	Regional	Local

5. Criticality Impact Assessment

We compiled a set of criteria based on our review of critical infrastructure protection approaches (described in Section 2), and proceeded to enrich them using generic risk methodologies [9]. The criteria were categorized in terms of scope, severity and time. A criticality impact assessment was conducted using a survey of experts. The survey respondents were asked to specify their levels of agreement with various statements using a Likert four-item psychometric scale [14]. Note that the numerical scales used in practice vary considerably; to our knowledge, no standardized or widely accepted ranges for these scales exist. The following tables present indicative examples of the scales we use for criticality impact assessment. Our intent is to demonstrate the characteristics of each impact factor and how the scales may differ from traditional risk analysis.

The scope of an incident may be expressed using three factors: population affected, population concentration and range. Table 3 shows the three scope impact factors and their scales (based on [22]).

- **Population Affected:** This is the number of people affected by an incident. Note that this factor is not used to evaluate the type of impact.
- **Population Concentration:** A higher concentration implies a higher potential for catastrophic effects. Population density (persons/km^2) is a useful criterion [17]; Table 3 presents an adjusted scale for this criterion.
- **Range:** This criterion evaluates the geographical scope of an event (e.g., <100 km^2, 100–1,000 km^2, 1,000–10,000 km^2, >10,000 km^2 [17]; or international, national, regional, local [22]).

The three criteria evaluate scope in different ways. The first criterion quantifies the number of affected individuals. The other two criteria do not evaluate scope in absolute terms: concentration expresses the density of population while range provides an abstract representation of the geographical effect.

A number of criteria may be used to quantify the severity of incidents. Table 4 presents several severity impact factors. Note that the scales can be adjusted according to national policy and currency.

- **Economic Impact:** This criterion measures the direct economic impact of an incident. It includes the losses to the CI itself from service degrada-

Table 4. Severity impact factors.

Impact Factor	**Very High**	**High**	**Medium**	**Low**
Economic Impact	>$100 million	$10–$100 million	$1–$10 million	<$1 million
Interdependency	Debilitating impact on other CIs or sectors	Significant impact on other CIs or sectors	Moderate impact on other CIs or sectors	Minor impact on other CIs or sectors
Public Confidence (Perception)	High risk and ability to control in doubt internationally	High risk and ability to control in doubt nationally	Moderate risk and ability to control risk	Low risk and ability to control risk
International Relations	Seriously damage international relations	Raise international tension	Materially damage diplomatic relations	Adversely affect diplomatic relations
Public Order	Direct threat to internal stability	Widespread industrial action	Demonstrations; lobbying	Localized protest
Policy and Operations of Public Service	Shut down or substantially disrupt national operations	Seriously impede the development or operation of government policies	Impede the development or operation of government policies	Undermine management or operation of a public sector organization
Safety	Widespread loss of lives	Severe injuries; chronic illnesses; potential casualties	Severe injuries; chronic illnesses	Minor injuries
Defense	Grave damage to the security of allied forces	Grave damage to the security of a nation	Minor damage to the security of a nation	n/a

tion or loss of assets and information, recovery costs, and the estimated loss due to cascading effects. The GDP can be used to estimate the economic impact. Possible scales are >$1 billion, $100 million to $1 billion, $10 to $100 million, <$10 million [22]; and <€50 million, <€500 million, <€5 billion, <€50 billion, >€50 billion [17]. Note that the scales are

significantly higher than those used in traditional risk assessment methods (which may have a maximum level of £1 million [9]). The scales vary according to the scope of the analysis and the value of critical assets. Furthermore, they should be adjustable as in the case of risk methods [9].

- **Interdependency:** This criterion assesses the likelihood of a cascading effect within the sector and across sectors. Interdependencies may be physical, cyber, geographic and logical [23].

- **Public Confidence:** This criterion assesses the impact on public confidence or on the ability of the government to provide public services, maintain health and safety, etc. [26]. The scale used in Table 4 is based on [22].

Next, we describe five additional criteria that are used in risk analysis [9] as well as in critical infrastructure protection. These impacts, which are primarily societal in nature, are assigned relatively high assessments by [9] (7 to 10 on a ten-point scale) and are generally not applicable to commercial organizations.

- **International Relations:** This criterion evaluates the impact of an incident on diplomatic relationships [9, 17]. The effects include demonstrations or threats against a country or its embassies, negative publicity and diplomatic actions (e.g., expulsion of diplomats, termination of diplomatic relations, cancellation of visits by foreign representatives, cancellation of trade agreements and treaties) [17].

- **Public Order:** This criterion estimates the impact on public order. The impact on public order could be due to the disclosure of confidential information or the unavailability of critical public services (e.g., electricity or water supply). The scaling [9] has been adjusted to fit a four-item scale.

- **Public Policy and Operations:** This criterion assesses the ability of the government to implement its policies and operations. It is different from the public confidence criterion because it does not consider psychological effects, but the actual ability of the government to function. The scaling [9] has been adjusted to fit a four-item scale.

- **Public Safety:** This criterion relates to the welfare of individuals; it includes injuries, chronic illnesses and fatalities. It also encompasses pain, suffering and grief [17]. Unlike the scope criteria, it does not consider the number of people affected or the percentage of the population affected.

- **Defense:** This criterion considers the ability of a government to protect its population from hostile attacks [9] either due to the unavailability of CIs or through the modification or disclosure of critical information. Because of its nature, this criterion does not have a low value; thus, the scale ranges from medium to very high.

Table 5. Time-related impact factors.

Impact Factor	Very High	High	Medium	Low
Recovery Time	Years	Months	Days	Hours
Duration	Years	Months	Days	Hours

Two criteria are used to assess the temporal aspects of incidents (Table 5):

- **Recovery Time:** This criterion measures the time needed for recovery. It is affected by the availability of substitutes and the cost incurred before an asset or service is restored.
- **Impact Duration:** This criterion is different from the recovery time because, although some services may become functional, the long-term effects of the incident may still affect the CI and its environment (e.g., public confidence or economic impact). Possible ways to represent time factors are 2–6 days, 1–4 weeks, 1–6 months, 6 months or longer [17]; and years, months–year, days–weeks, hours–days [22]. Traditional risk analysis methods often use shorter time frames, e.g., <15 mins, 1 hour, 3 hours, 12 hours, 1 day, 2 days, 1 week, etc. [9]. Our scale ranges from hours to years.

Table 6. Critical points of time.

Impact Factor	Points of Time			
Impact Peak	Immediate	Within hours	Within days	Within months
Critical Frames	Time periods that indicate variations in criticality			

The following criteria deal with "time-critical moments" for a CI (Table 6):

- **Impact Peak:** This is the point of time when an incident produces its most severe effect (e.g., immediate, one to two days, one week, etc.).
- **Critical Time Frames:** These refer to moments/periods that demonstrate variations in criticality (e.g., the difference in criticality of telecommunications during normal operation and during a crisis situation).

In order to assess the overall criticality, the applicable scope, severity and time criteria have to be assessed for an incident or threat. It is also essential to define the expected impact peak and the critical time frames for a CI when a particular incident may have a greater impact. Clearly, different impact levels are expected for these critical points of time. We recommend applying a "worst-case" approach instead of calculating the average impact. For each scenario,

Table 7. Applicable criteria.

Criteria	Impact Factor	Normal Traffic	Rush Hour
Scope	Population Affected	Low	Medium
Severity	Economic Impact	Low	Medium
	Interdependency	Medium	Medium
	Public Confidence	High	High
	Safety	High	Very High
Time	Recovery Time	High	High
	Duration	Low	Low

the impact is evaluated for each time point/frame; the worst-case impacts are combined to obtain the overall impact.

6. Illustrative Example

This section illustrates the criticality assessment methodology using a metro system (transportation sector) as an example. The metro system transports up to 975,000 commuters a day, and is interconnected with other transportation sector components (buses and trams). In the example, we evaluate the critical asset "Central Station" with respect to the "Fire" threat.

We use a worst-case scenario to assess the impact of the fire scenario on the metro station. We identify two critical points of time – normal traffic and rush hour – and proceed to perform a separate assessment for each time frame. The rush hour time frame differs from the normal traffic period in terms of the number of people affected and the economic impact (e.g., transportation assets at the station). Also, due to the number of the people at the station, rescue and evacuation would present difficulties, which may lead to a higher safety impact.

Interdependent CIs would be affected due to the presence of connecting stops inside or close to the station. Also, passengers would require other means of transportation during the recovery period, giving rise to congestion elsewhere in the transportation system. Thus, the impact on the interconnected CIs is expected to be moderate. Due to the presence of fire control assets at the station and the proximity of the fire department, the duration is estimated to be a few hours. However, the recovery time is expected to be 1.5 months. The impact peak is estimated to be within one hour for both time frames. The impact on public confidence is anticipated to be high with regard to metro system safety and rescue team efficiency. Based on a worst-case impact assessment, the overall criticality is assessed to be high for normal traffic and very high during the rush hour (Table 7).

In order to assess the associated criticality risk factors, it is necessary to estimate the possibility of a fire occurring in the central station based on statistics of previous incidents (this information would be available from the fire department). Also, the enabling vulnerabilities have to be identified. Examples include the presence of flammable materials, poor maintenance of circuits and cabling, etc. Although the impact is assessed as being high, the overall risk could be low, especially if the threat level and vulnerability level are both low.

7. Conclusions

Current approaches for evaluating and prioritizing CIs are mainly based on criticality impact factors; in particular, they do not exploit the results of well-defined risk analysis methodologies. The resulting CI categorizations and prioritizations are often inherently biased due to their reliance on organization-oriented impacts and security risk factors. The risk-based criticality analysis methodology presented in this paper addresses this deficiency by considering societal and sector-based impact factors as well as CI interdependencies. Our future work will focus on the definition of criticality-oriented threats and vulnerabilities, interdependency modeling and numerical assessments of risk in CIs.

References

[1] E. Adar and A. Wuchner, Risk management for critical infrastructure protection challenges: Best practices and tools, *Proceedings of the First IEEE International Workshop on Critical Infrastructure Protection*, 2005.

[2] C. Alberts and A. Dorofee, *Managing Information Security Risks: The OCTAVE Approach*, Addison-Wesley/Pearson, Boston, Massachusetts, 2003.

[3] A. Bialas, Information security systems vs. critical information infrastructure protection systems – Similarities and differences, *Proceedings of the International Conference on the Dependability of Computer Systems*, pp. 60–67, 2006.

[4] E. Brunner and M. Suter, *International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Infrastructure Protection Policies*, Center for Security Studies, ETH Zurich, Zurich, Switzerland, 2008.

[5] E. Casalicchio and E. Galli, Metrics for quantifying interdependencies, in *Critical Infrastructure Protection II*, M. Papa and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 215–227, 2008.

[6] Emergency Management Australia, Critical Infrastructure Emergency Risk Management and Assurance Handbook, Mount Macedon, Australia, 2003.

[7] European Commission, Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, COM (2006)786 Final, Brussels, Belgium, 2006.

[8] European Commission, Proposal for a Directive of the Council on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection, COM(2006)787 Final, Brussels, Belgium, 2006.

[9] Insight Consulting, CRAMM User Guide, Issue 5.1, Walton-on-Thames, United Kingdom, 2005.

[10] International Organization for Standardization, ISO/IEC Guide 73:2002: Risk Management – Vocabulary – Guidelines for Use in Standards, Geneva, Switzerland, 2002.

[11] J. Kopylec, A. D'Amico and J. Goodall, Visualizing cascading failures in critical cyber infrastructures, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 351–364, 2007.

[12] KPMG Peat Marwick, Vulnerability Assessment Framework 1.1, U.S. Critical Infrastructure Assurance Office, Washington, DC, 1998.

[13] W. Kroger, Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools, *Reliability Engineering and System Safety*, vol. 93(12), pp. 1781–1787, 2008.

[14] R. Likert, A technique for the measurement of attitudes, *Archives of Psychology*, vol. 140(22), pp. 1–55, 1932.

[15] E. Luiijf, Threat Taxonomy for Critical Infrastructures and Critical Infrastructure Risk Aspects at the EU-Level, Version 1.04, Deliverable D1.2, Technical Report VITA PASR-2004-004400, TNO Defence, Security and Safety, The Hague, The Netherlands, 2006.

[16] E. Luiijf, H. Burger and M. Klaver, Critical infrastructure protection in the Netherlands: A quick-scan, *Proceedings of the EICAR Conference*, 2003.

[17] Ministry of the Interior and Kingdom Relations, National Risk Assessment Method Guide 2008, The Hague, The Netherlands, 2008.

[18] J. Moteff, Risk Management and Critical Infrastructure Protection: Assessing, Integrating and Managing Threats, Vulnerabilities and Consequences, CRS Report for Congress, Document RL32561, Congressional Research Service, Library of Congress, Washington, DC, 2005.

[19] A. Nieuwenhuijs, E. Luiijf and M. Klaver, Modeling dependencies in critical infrastructures, in *Critical Infrastructure Protection II*, M. Papa and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 205–213, 2008.

[20] North American Electric Reliability Corporation, Standard CIP-002-1, Cyber Security – Critical Asset Identification, Washington, DC, 2006.

[21] P. Pederson, D. Dudenhoeffer, S. Hartley and M. Permann, Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, Technical Report INL/EXT-06-11464, Idaho National Laboratory, Idaho Falls, Idaho, 2006.

[22] Public Safety and Emergency Preparedness Canada, Selection Criteria to Identify and Rank Critical Infrastructure Assets, Ottawa, Canada, 2004.

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

[24] R. Setola, S. Bologna, E. Casalicchio and V. Masucci, An integrated approach for simulating interdependencies, in *Critical Infrastructure Protection II*, M. Papa and S. Shenoi, (Eds.), Springer, Boston, Massachusetts, pp. 229–239, 2008.

[25] G. Stoneburner, A. Goguen and A. Feringa, Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology, Special Publication 800-30, National Institute of Standards and Technology, Gaithersburg, Maryland, 2002.

[26] U.S. Department of Homeland Security, National Infrastructure Protection Plan 2009, Washington, DC, 2009.