HAL open science

Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis

Christine Izuakor, Richard White

To cite this version:

Christine Izuakor, Richard White. Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis. 10th International Conference on Critical Infrastructure Protection (ICCIP), Mar 2016, Arlington, VA, United States. pp.27-41, 10.1007/978-3-319-48737-3_2 . hal-01614862

HAL Id: hal-01614862

https://inria.hal.science/hal-01614862

Submitted on 11 Oct 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Chapter 2

CRITICAL INFRASTRUCTURE ASSET IDENTIFICATION: POLICY, METHODOLOGY AND GAP ANALYSIS

Christine Izuakor and Richard White

Abstract Critical infrastructure asset identification is a core component of the risk management process. Amidst growing concerns of terrorist and natural disaster threats to the critical infrastructure, it is imperative that public and private sector stakeholders understand exactly which assets are critical to national security in order to prioritize risk management efforts. Challenges to accomplishing this task are the difficulty in identifying exactly which assets are critical and comparing the risks to assets across the many critical infrastructure sectors. A proven method for critical infrastructure asset identification that meets these needs does not exist today. This chapter explores the critical infrastructure protection policy frameworks and requirements of the United States, European Union and other countries, and summarizes the key requirements and methodologies. The methodologies are analyzed against the outlined requirements. Based on this analysis, a new approach is presented for critical infrastructure asset identification and additional research using multi-criteria decision theory is proposed to resolve the challenges that have limited progress in this area.

Keywords: Critical infrastructure asset identification, multi-criteria decision theory

1. Introduction

Critical infrastructure asset identification is a fundamental component of national risk management and homeland security efforts. While growing threats and hazards have increased the need for better infrastructure protection, budgetary constraints and resource limitations have made it impractical to protect every single asset. The effective identification of critical assets enables protection programs to prioritize asset lists. Detailed risk assessment can then be limited to the key assets, such those whose disruptions could have debilitat-

ing impacts on security, national economic security, national public health and safety or any combination thereof [20].

A limited number of critical asset identification methodologies exist today. While many risk assessment methodologies allude to some type of asset identification, seldom do they provide clear guidelines for doing so. Moreover, the objectives, underlying theories, target audiences and other variables differ between the various methodologies. This chapter explores the critical infrastructure protection policy frameworks and requirements of the United States, European Union and other countries, and summarizes the key requirements and methodologies. The methodologies are analyzed against the outlined requirements. Based on this analysis, a new approach is presented for critical infrastructure asset identification and additional research using multi-criteria decision theory is proposed to resolve the challenges that have limited progress in this area.

2. Policy Frameworks

The need for critical infrastructure asset identification is underscored in presidential directives, acts and plans that guide critical infrastructure protection initiatives in the United States. Other nations have taken on similar efforts to protect their critical infrastructures. This section provides an overview of efforts undertaken by the United States, European Union and other nations.

2.1 United States

The U.S. National Infrastructure Protection Plan (NIPP) is the primary federal government guide for risk management of critical infrastructures. The development of the plan was influenced by several directives, strategies and policies [15]. The Homeland Security Act of 2002 [21] mandated the development of a critical infrastructure risk management program. After several drafts, the first National Infrastructure Protection Plan was released in 2006. Stemming as it did from the attacks of September 11, 2001, the first plan focused on managing critical infrastructure risk from terrorist attacks. As a result of Hurricane Katrina, the National Infrastructure Protection Plan was updated in 2009 to incorporate an "all-hazards" approach to critical infrastructure risk management. The National Infrastructure Protection Plan was again revised in 2013 to emphasize the administration's priority on resilience as articulated in PPD-21 [16]. The current plan specifies the sixteen critical infrastructure sectors listed in Table 1.

At the heart of the U.S. National Infrastructure Protection Plan is a five-step critical infrastructure risk management framework. The essential purpose of the risk management framework is to assess and prioritize critical infrastructure risk as a product of threats, vulnerabilities and consequences. In fact, Step 2 in the risk management process is critical infrastructure identification. This step sets the foundation for evaluating risks and prioritizing asset protection efforts, making the quality of information produced at this stage critical to

Table 1. PPD-21 infrastructure sectors [16].

Chemical	Financial Services
Commercial Facilities	Food and Agriculture
Communications	Government Facilities
Critical Manufacturing	Healthcare and Public Health
Dams	Information Technology
Defense Industrial Base	Nuclear Reactors, Materials and Waste
Emergency Services	Transportation Systems
Energy	Water and Wastewater Systems

the effectiveness of the entire process. The Department of Homeland Security Office of Infrastructure Protection is responsible for critical infrastructure asset identification under the National Critical Infrastructure Prioritization Program (NCIPP).

2.2 European Union

The European Programme for Critical Infrastructure Protection (EPCIP) provides guidance for critical infrastructure risk management efforts in Europe. The program fulfills the requirements set forth by European Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [7]. The program scope is limited to the transportation and energy sectors, and calls for all-hazards consideration in critical infrastructure protection efforts. While the methodology is said to incorporate an all-hazards approach, including man-made, technological and natural hazards, it gives priority to terrorist threats [7].

The European Programme for Critical Infrastructure Protection phases include the identification, designation and protection of the European critical infrastructure. In the identification phase, potential critical infrastructure assets are filtered through a five-step process that involves the application of sectoral criteria, cross-cutting criteria, cross-border considerations, candidacy nomination and final selection [7]. Similar to the risk management framework in the U.S. National Infrastructure Protection Plan, critical infrastructure asset identification lays the foundation for all subsequent phases of the European Programme for Critical Infrastructure Protection. Thus, the success of the risk management process is again dependent on the quality of the critical infrastructure asset identification results.

2.3 Other Countries

Critical infrastructure protection is an important component of national security for other countries as well. A vast amount of information on the topic is available in [4]. Notable examples include the Australian National Strat-

egy for Critical Infrastructure Protection [2] and the Canadian Strategy for the Protection of National Critical Infrastructure [9]. The Australian national strategy aims to address all hazards and defines the critical infrastructure as "physical facilities, supply chains, information technologies and communications networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defense and ensure national security." The Australian critical infrastructure sectors include banking and finance, health, food, transport, energy, communications and water.

The Canadian sectors (in addition) include safety, manufacturing and government. Canada defines the critical infrastructure as "processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government."

It is clear that the identification and protection of critical infrastructure assets are relevant to multiple countries. However, just as the definitions of the critical infrastructure and the associated critical infrastructure sectors vary for different countries, the methodologies used to identify critical infrastructure assets also vary.

3. Methodology Requirements

An effective critical infrastructure asset identification methodology meets two types of requirements: (i) qualitative requirements; and (ii) quantitative requirements.

3.1 Qualitative Requirements

Qualitative requirements are soft criteria that are used to develop a methodology. For example, in 2013, the U.S. Government Accountability Office (GAO) investigated Congressional concerns about changes to the critical infrastructure asset identification methods employed by the Department of Homeland Security. The GAO report [23] listed four criteria as necessary for identifying critical infrastructure assets that support the comparison of risk results across infrastructure sectors. The four criteria, as specified in the 2009 National Infrastructure Protection Plan [19], are: (i) completeness; (ii) reproducibility; (iii) documentation; and (iv) defensibility. These criteria have been used by numerous researchers to evaluate critical infrastructure protection initiatives. Completeness means that a methodology systematically examines every relevant asset in the set of sixteen critical infrastructure sectors; an asset identification methodology is incomplete when it does not consider all potential candidates in a set of assets. Reproducibility means that the results are consistent, simple and precise enough to enable risk comparisons between assets across different sectors; complexity and ambiguity work against reproducibility. Documentation is a record of the information that is used and how it is synthesized to generate a risk estimate.

Table 2. Elements of a critical infrastructure asset identification methodology [1].

Methodology Element	**Description**
Asset Identification	Means for identifying and representing assets for the purpose of criticality analysis
Criteria	List of factors against which asset criticality is measured
Weighted Scoring	Means for allocating scores to achieve a total score indicating asset criticality
Scoring Guides	Templates for applying the scoring against the criteria
Application	Means for applying the scoring against the criteria in an organization

Defensibility means that a methodology makes use of the professional disciplines relevant to the analysis and that it is free from significant errors and omissions. Defensibility can also be viewed in terms of validation and verification. In other words, the right thing is being done and it is being done correctly. Of course, this means that the "right thing" should be defined. In the context of critical infrastructure protection, this means preventing catastrophic damage to an infrastructure through its subversion, disruption or destruction. Catastrophic damage is the primary concern and the right thing is to prevent it from occurring.

3.2 Quantitative Requirements

Quantitative requirements are hard criteria for developing a critical infrastructure asset identification methodology. Table 2 provides the basic elements of a critical asset identification methodology as outlined by researchers at Central Queensland University in Australia [1].

Table 3. Critical infrastructure asset identification methodology components.

Process Component	**Decision Points**
Scope	Systematic OR unsystematic
Approach	Network-based, function-based AND/OR logic-based
Evaluation Method	Criteria AND application method

Table 3 shows how the quantitative requirements are further translated into a framework geared towards critical infrastructure asset identification. It is important to note that these requirements contribute immensely to the completeness of the qualitative requirements listed above.

Asset Identification Scope and Approach. Every methodology must set a specific scope and approach for the initial asset coupled with an evaluation method. The scope of the assessment can be systematic or unsystematic based on the objective and needs of the organization. Systematic methods take on a comprehensive approach to asset identification and conduct a complete evaluation of the asset environment, including the relationships between the assets. Unsystematic methods take an individual asset level approach and do not necessarily consider all the assets.

The assessment approach can be categorized as function-based, network-based or logic-based. Function-based approaches, also referred to as mission-based approaches, begin the identification process by identifying the functions that are critical to the mission of the organization; assets that support these functions are then identified and evaluated against other defined criteria. Network-based approaches identify all the nodes and relationships in a system and use the system mapping as a basis for the evaluation. Logic-based approaches select assets based on the "best judgment" of assessors. In unsystematic approaches, this is typically the approach of choice; in systematic approaches, a logic-based approach may augment the other approaches to consider additional assets beyond the original scope.

Criteria, Scoring and Application. The evaluation method is organized around selecting and applying custom combinations of criteria to asset lists in order to distinguish critical assets from non-critical assets. Criteria are tailored to the organization and purpose of the asset identification effort. After the criteria are established, they are applied via scoring schemes, criticality matrices and other methods to identify the assets that meet the criticality criteria. Universal guidelines for establishing these criteria, scoring and application do not exist. However, this portion of the critical infrastructure asset identification framework is typically performed based on one or both of the following premises:

- Criticality is determined by the position of an asset in a system or network and its relation to other assets. This approach is generally based on network and/or system theory, and may deem an asset as critical based on its connections and/or points of failure. For example, Bouchon [3] has presented a critical infrastructure asset identification method based on asset interdependencies. Stergiopoulos et al. [17] have proposed expanding dependency analysis using graph centrality in order to identify critical infrastructure assets.

- Criticality is determined based on the ability of an asset to meet predetermined selection criteria. The criteria often include metrics such as potential loss of life, economic impact and descriptive characteristics. Criticality can also be considered based on the degree of change that the degradation or loss of an asset inflicts on the quality of the provided

Table 4. Search results of IEEE papers.

Paper Type	**Count**
Critical-infrastructure-related sector-specific	6
Critical-infrastructure-related cross-sector compatible	0
Non-critical-infrastructure-related asset identification	4
Out of scope	46
Total	56

function. This is commonly seen in practice; Section 5 discusses some examples.

Metzger [13] notes that the first premise above aligns more with emergency management goals while the second premise is more applicable to national security efforts. Metzger maintains that the criteria-based approach enables non-technical and non-networked assets to be considered. Mattioli and Levy-Bencheton [12] report that the network approach ignores critical services and is highly complex. Complexity is also cited as a challenge for non-network approaches due to the sophistication needed to identify dependencies and the challenges associated with developing appropriate assessment criteria.

Ultimately, there are a number of ways to combine and customize the framework components in order to establish a critical infrastructure asset identification program. Examples of existing methodologies are discussed in the next section.

4. Methodology

The search for critical infrastructure asset identification methods was conducted on the IEEE database, DHS Journal, ScienceDirect, Taylor and Francis, Google and Google Scholar. A limited amount of relevant results was returned from each database. For example, a search of the phrase "critical asset identification" in the IEEE database yielded the results shown in Table 4.

The survey yielded four exemplars of the different critical infrastructure asset identification approaches: (i) National Critical Infrastructure Prioritization Program (NCIPP); (ii) Defense Critical Infrastructure Program (DCIP), (iii) European Programme on Critical Infrastructure Protection (EPCIP); and (iv) Criticality Accessibility Recoverability Vulnerability Espyability Redundancy (CARVER2):

- **National Critical Infrastructure Prioritization Program (NCIPP):** The National Critical Infrastructure Prioritization Program [23] is used by the Department of Homeland Security to allocate homeland security grants, prioritize voluntary critical infrastructure protection programs and inform incident management planning and response efforts.

The program uses consequence thresholds based on fatalities, economic loss, mass evacuation duration and degradation of national security. The critical infrastructure asset identification process begins with an annual voluntary data call for nominations from state homeland security agencies and federal partners. The data call requires that each nominated asset meet two of the four consequence category thresholds. Thresholds are set at Level 1 or Level 2, where Level 1 corresponds to the highest priority. The prioritization program uses these level designations to identify and prioritize critical infrastructure assets. However, the actual values are not released to the public.

Nominated assets must include "realistic scenarios" to justify their consequence claims. Nominated assets further undergo adjudication that enables state agencies and federal partners to review decisions and submit additional supporting information as necessary before the list is finalized. The National Critical Infrastructure Prioritization Program criteria have evolved as the Department of Homeland Security has gained experience with the program. For example, in 2010, special criteria were introduced for the food and agriculture sector to address the unique risks associated with animal disease. Although the National Critical Infrastructure Prioritization Program prioritizes assets, their ultimate risk values are determined in the remaining steps of the risk management framework.

- **Defense Critical Infrastructure Program (DCIP):** The Defense Critical Infrastructure Program [18] is a systematic, function-based methodology employed by the U.S. Department of Defense to identify critical infrastructure assets. The nine-step process begins by decomposing the mission and identifying the required capabilities. The capabilities are further broken down into task assets. The task assets are then evaluated against five criteria. Only one of the five criteria must be met for an asset to be nominated for advancement to the next step in the identification process.

  Nominated assets are validated by mission owners and are then submitted to the joint staff for additional analysis and development of the initial task critical asset (TCA) list. The initial list is used to conduct interdependency analysis to identify additional assets that may be impacted by the disruption or destruction of task critical assets.

  After the assets have been vetted by the joint staff for verification of mission impact, appropriate defense critical assets are nominated, reviewed and are either approved or denied. The resulting critical asset list forms the basis for other Defense Critical Infrastructure Program activities during the next year, including vulnerability assessment planning and remediation and mitigation prioritization submissions for the DoD [18]. Unlike the National Critical Infrastructure Prioritization Program, the Defense Critical Infrastructure Program prioritizes critical infrastructure assets independently of identifying them.

- **European Programme on Critical Infrastructure Protection (EPCIP):** The European Programme on Critical Infrastructure Protection [6] provides systematic, network-based guidelines for member states to identify critical infrastructure assets. The member states have the option to use these guidelines or to implement their own programs.

  The European Programme on Critical Infrastructure Protection recommends a four-step process that begins with the evaluation of assets against sectoral criteria. Each infrastructure sector has its own set of criteria that can include properties such as capacity and distance from other infrastructures, and may specify assets that must be included. An asset that meets the sectoral criteria is evaluated against Directive CS/2008/10934, which defines a critical infrastructure as an asset, system or part thereof located in a member state that is essential to the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have significant impact in the member state as a result of the failure to maintain the functions [7].

  National thresholds or cross-cutting criteria are used to evaluate the consequences in the definition of a critical infrastructure asset. At this point, alternative back-up resources and time to recover are also considered in determining whether or not an asset meets the critical infrastructure asset definition. If the asset meets the criteria, then it advances to the next step and is evaluated based on the cross-border impact of the asset on other member states. Finally, the asset is evaluated against cross-cutting criteria to determine its entry in the critical asset list. Cross-cutting criteria include the potential number of casualties, degree of economic loss and impact on public morale. This step requires the development of a "reasonable worst case scenario" to support consequence estimates. Note that an asset may only be designated as a European critical infrastructure if it meets the criteria in all four steps and is approved as such by the member state in whose jurisdiction it is located. If the member state disagrees with the critical infrastructure asset designation, then the asset is not deemed as a critical infrastructure asset even if it has met all the criteria.

- **Criticality Accessibility Recoverability Vulnerability Espyability Redundancy (CARVER2):** The Criticality Accessibility Recoverability Vulnerability Espyability Redundancy (CARVER2) methodology [8] is an unsystematic approach to critical infrastructure asset identification. The method is applied across infrastructure sectors by operators, government agencies and private industry to fulfill the non-technical needs of critical infrastructure analyses from the policy maker point of view.

  The methodology scores an asset based on the six criteria that comprise its acronym: criticality, accessibility, recoverability, vulnerability, espyability and redundancy. As in the case of the National Critical Infras-

tructure Prioritization Program, the scoring feature is used to identify critical infrastructure assets as well as to prioritize them. Unlike the other methodologies discussed above, the Criticality Accessibility Recoverability Vulnerability Espyability Redundancy methodology is employed on an individual basis and not systematically within any particular infrastructure sector.

5. Gap Analysis

The research reveals that, while a number of methodologies are available, there is no apparent way to validate and verify that they assess the right assets against the right criteria.

5.1 Completeness

The combination of the selected scope and approach generally determine the coverage of assets or "completeness." However, a method for determining the precise combination that renders the most complete assessment is missing. From a scoping perspective, it is clear that an unsystematic approach would not be complete when implemented as a stand-alone program. This does not mean that an unsystematic program, such as the Criticality Accessibility Recoverability Vulnerability Espyability Redundancy methodology, could not be applied in a systematic manner. However, in general, unsystematic methods fail to meet the completeness criterion.

Systematic evaluation is initially implied in the other approaches, but customized program elements such as the requirements to include threat scenarios and exclude certain asset types as in the National Critical Infrastructure Prioritization Program implementation can render an evaluation incomplete. It is important to understand how these customizations impact completeness. Similarly, the European Programme on Critical Infrastructure Protection has limited focus on the energy and transportation sectors [6]. Indeed, the program struggles to overcome political disagreements on the identification criteria for additional sectors. This temporary limitation of scope hinders completeness.

When selecting an approach with the completeness characteristic, it is difficult to determine whether a function-, network- or asset-based approach is the most effective. In the case of the National Critical Infrastructure Prioritization Program, the various sectors implement their own approaches for identifying assets; this further complicates attempts to measure completeness across sectors. A function-based approach like the Defense Critical Infrastructure Protection methodology focuses on assets that support critical functions and can reduce the effort required by narrowing the scope of the assessment. It is possible that the function-based approach could overlook assets that do not fit the function or mission as defined; however, they can be considered to be application errors, not systemic failures of the basic approach. A network-based approach can be an effective way to approach critical infrastructure asset identification based on the objectives. This is especially helpful in identifying dependencies and

interdependencies between infrastructures. The limitations include complexity and a deep understanding of network analysis.

5.2 Reproducibility

Consistency of results is paramount if risk comparisons are to be made between assets across different sectors. The evaluation components (criteria and application method) are vital to ensuring reproducibility and the components should be objective in nature. Yet, methods that incorporate consequence criteria and require scenario justifications introduce a wide range of subjectivity in their assessments and their results may vary accordingly.

The National Critical Infrastructure Prioritization Program nominating process has been described by some state officials as moderately difficult to very difficult [23]. Indeed, the program results over the years have varied between sectors and users of the method, suggesting a lack of reproducibility and comparability. For example, one user of the methodology included the entire subway system as a single asset in an evaluation whereas another user included each subway station as an asset [14].

Similarly, reviews of the Defense Critical Infrastructure Program and European Programme on Critical Infrastructure Protection have revealed that inconsistent criteria and subjective guidelines limit their effectiveness [6, 22]. Conversely, the Criticality Accessibility Recoverability Vulnerability Espyability Redundancy methodology appears to be intuitive enough to reduce misinterpretation.

Proper documentation also plays a key role in promoting reproducibility. There is no systemic reason why any of the methods cannot be documented effectively. In this case, the principal task is to determine the combinations of components that should be assembled and documented.

5.3 Defensibility

To be deemed defensible, a methodology should utilize state-of-the-art techniques to identify and apply criteria that align with the definition of the national critical infrastructure, meet the four National Infrastructure Protection Plan requirements, contribute to the identification of dependencies and interdependencies, and ultimately produce an appropriate list of critical assets.

Another way of considering defensibility is in terms of validation and verification. In other words, is the right thing being done? And is it being done the right way?

To answer these questions, it is necessary to define the "right thing." In the context of critical infrastructure protection, one answer is to prevent an infrastructure from causing catastrophic damage through its subversion, disruption or destruction. From this perspective, catastrophic damage is the primary concern, and the right thing is to prevent it from occurring. Concern about catastrophic damage is a concern about consequences. This appears to confirm the appropriateness of applying consequence criteria to create an asset list.

One problem with the sole consequence-criteria application, though, is attempting to distinguish between "vector" and "victim." This problem has manifested itself in the National Critical Infrastructure Prioritization Program with regard to the livestock subsector of the food and agriculture sector. Specifically, a GAO report [23] notes that "consequence criteria were unable to account for the fact that individual animals could be the entry point for a scenario – such as malicious contamination with an agent like foot-and-mouth disease – which may cause catastrophic effects." While a single sick cow will not trip a consequence threshold, its potential to infect all cattle would. The cow is only a vector, but it can have a significant number of victims in the livestock subsector.

This dilemma is by no means limited to the food and agriculture sector. Was it the buildings or the airplanes that were responsible for the approximately 3,000 lives lost and $40 billion damage on September 11, 2001? The Twin Towers did not collapse on their own accord. Passenger airplanes were the vectors that caused the towers to collapse; the Twin Towers were the victims. By the same token, aircraft on their own accord do not create catastrophic damage – they must also be the victims of some vector.

A consequence-criteria methodology, as used by the National Critical Infrastructure Prioritization Program, appears to be incapable (on its own) of accounting for additional factors beyond the consequence threshold. The other programs discussed above apply consequence criteria in combination with other criteria. However, the principal challenge is still to determine the combination of criteria that best identifies the right assets.

6. Future Research

Most methodologies engage multiple criteria in evaluating critical infrastructure assets, but the methods often lack scientific support and a theoretical foundation. The best course of action is to leverage the wealth of research in this discipline to design and validate a critical infrastructure asset identification methodology that is applicable to all sectors and all nations. Such a methodology could use a highly customizable and proven multi-criteria decision making model. If customized appropriately, multi-criteria decision making can provide transparency, analytic rigor and decision auditability [5]. The approach is widely used in a variety of industries and has a strong reputation [11].

The goal is to identify the assets that are critical in accordance with the formal definitions of critical infrastructure and policy. Halim and Mohamed [10] have applied multi-criteria decision making to identify the critical levels of assets in the Malaysian water sector. They describe how multi-criteria decision making can be applied to critical infrastructure asset identification. However, they apply criticality analysis to the probability of failure and consequence of failure. In the context of critical infrastructure protection, it may not be appropriate to consider the probability of failure during the initial identification process. Instead, it is prudent to focus on identification before prioritization because prioritization can only occur after risk analysis.

Additional research and the successful application of multi-criteria decision making can meet the qualitative and quantitative requirements outlined in this chapter. By viewing critical infrastructure asset identification as decision making based on objectives, following a logical decision system and developing a systematic process for arriving at criticality decisions, it is possible to obtain a solution that is defensible. The simple and logical nature of multi-criteria decision making also supports reproducibility. Additionally, the highly customizable nature of a multi-criteria decision making methodology provides confidence that the assessment is complete and meets all the quantitative requirements. Finally, organizing critical infrastructure asset identification in this manner yields solutions that are transferable to other areas and are valuable to private and public sector entities.

7. Conclusions

Risk management provides the foundation for critical infrastructure protection. The ability to effectively identify critical assets is a crucial first step to any risk management process. Ensuring that a critical infrastructure asset identification methodology is complete, reproducible, documented and defensible is essential to enabling cross-sector comparisons. The scope, approach and evaluation method are variables that can contribute to meeting these requirements. While several methodologies have been proposed in the literature, no current methodology meets all the requirements. This presents an opportunity for critical infrastructure protection researchers. A multi-criteria decision making model that combines the strengths of existing methodologies is a promising approach – it can provide systematic solutions that address the gaps and challenges associated with critical infrastructure asset identification efforts.

References

[1] D. Anderson, P. Kelcher and P. Smith, Towards an assessment tool for the strategic management of asset criticality, in *Engineering Asset Management*, J. Mathew, J. Kennedy, L. Ma, A. Tan and D. Anderson (Eds.), pp. 1232–1242, 2006.

[2] Australian Government, Critical Infrastructure Reliance Strategy: Policy Statement, Barton, Australia, 2015.

[3] S. Bouchon, The Vulnerability of Interdependent Critical Infrastructure Systems: Epistemological and Conceptual State-of-the-Art, EUR 22205 EN, Institute for the Protection and Security of the Citizen, European Commission Joint Research Centre, Ispra, Italy, 2006.

[4] CIPedia, CIPedia Main Page (`www.cipedia.eu`), 2016.

[5] D. Dunning, Q. Ross and M. Merkhofer, Multiattribute utility analysis for addressing Section 316(b) of the Clean Water Act, *Environmental Science and Policy*, vol. 3(S1), pp. 7–14, 2000.

[6] European Commission, Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP), SWD(2012) 190 Final, Brussels, Belgium, 2012.

[7] European Council, Council Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection, Brussels, Belgium, 2008.

[8] G. Giannopoulos, R. Filippini and M. Schimmer, Risk Assessment Methodologies for Critical Infrastructure Protection, Part 1: A State of the Art, JRC 70046, European Commission Joint Research Centre, Ispra, Italy, 2012.

[9] Government of Canada, National Strategy for Critical Infrastructure, Ottawa, Canada, 2009.

[10] M. Halim and A. Mohammed, Identification of critical level of assets by using analytic hierarchy process for water assets management, *International Journal of Technical Research and Applications*, vol. 2(S1), pp. 54–58, 2014.

[11] G. Kabir, R. Sadiq and S. Tesfamariam, A review of multi-criteria decision-making methods for infrastructure management, *Structure and Infrastructure Engineering: Maintenance, Management, Life-Cycle Design and Performance*, vol. 10(9), pp. 1176–1210, 2014.

[12] R. Mattioli and C. Levy-Bencheton, Methodologies for the Identification of Critical Infrastructure Assets and Services, Guidelines for Charting Electronic Data Communication Networks, European Union Agency for Network and Information Security, Heraklion, Greece, 2014.

[13] J. Metzger, The concept of critical infrastructure protection, in *Business and Security: Public-Private Sector Relationships in a New Security Environment*, A. Bailes and I. Frommelt (Eds.), Oxford University Press, New York, pp. 197–209, 2004.

[14] J. Moteff, Critical Infrastructure: The National Asset Database, CRS Report for Congress, RL33648, Congressional Research Service, Washington, DC, 2007.

[15] J. Moteff, Critical Infrastructures: Background, Policy and Implementation, CRS Report for Congress, RL30153, Congressional Research Service, Washington, DC, 2015.

[16] B. Obama, Presidential Policy Directive – Critical Infrastructure Security and Resilience, PPD-21, The White House, Washington, DC, 2013.

[17] G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou and D. Gritzalis, Risk mitigation strategies for critical infrastructures based on graph centrality analysis, *International Journal of Critical Infrastructure Protection*, vol. 10, pp. 34–44, 2015.

[18] U.S. Department of Defense, Defense Critical Infrastructure Protection: DoD Mission-Based Critical Asset Identification Process, Department of Defense Manual, No. 3020.45, Vol. 1, Washington, DC, 2008.

[19] U.S. Department of Homeland Security, National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency, Washington, DC, 2009.

[20] U.S. Government, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Public Law 107-56, Washington, DC, 2001.

[21] U.S. Government, Homeland Security Act of 2002, Public Law 107-296, Washington, DC, 2002.

[22] U.S. Government Accountability Office, Defense Critical Infrastructure: Actions Needed to Improve the Consistency, Reliability and Usefulness of DoD's Tier 1 Task Critical Asset List, GAO-09-740R, Washington, DC, 2009.

[23] U.S. Government Accountability Office, Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress, Report to Congressional Requesters, GAO-13-296, Washington, DC, 2013.