Risk and Vulnerability Analysis of Critical Infrastructure

Kaiyu Wan[1] and Vangalur Alagar[2](✉)

[1] Xi'an Jiaotong-Liverpool University, Suzhou, People's Republic of China
Kaiyu.Wan@xjtlu.edu.cn
[2] Concordia University, Montreal, Canada
alagar@cse.concordia.ca

Abstract. A nation's Critical Infrastructures (CI) is vital to the trustworthy functioning of the economic, health care, and social sectors of the nation. Any disruption to CI will adversely affect the economy, and peaceful functioning of the government. Above all, it will adversely affect the morale and confidence of the citizens. Hence, protecting CI of a nation must be given top priority. Fundamental to protection mechanisms are risk and vulnerability analysis. Based on their outcomes protection mechanisms can be planned, designed, and implemented. In this paper we offer a concise template representation for critical assets, and explain a methodology for vulnerability assessment and risk analysis. We point out the potential role of agents, and deep learning methods in the development and commissioning of future cyber defense solutions.

Keywords: Critical infrastructure · Risk analysis · Vulnerability analysis · Agent system · Deep learning

1 Introduction

Almost every nation in the world has an abundant number of CIs on which the governance and security of the country depends, and the citizens have come to depend upon them for their everyday living. From several reports [6, 9, 12] published by governments of Canada, USA, and European Commission and the recent monograph of Lazari [16] we get an adequate understanding of "what CI is?". From them we extract the following common features to be used in this paper:

- CI can be either physical (facility) or virtual (system) or a mixture of both.
- CI provides services that are vital (essential) to the health (safety, security, governance, reliable, available at all times, resilient to attacks) of the nation.
- There exist many CI sectors, and in each sector many networks and processes exist. Consequently, CI is a System of Systems (SoS).
- Maintaining the CI services without disruption requires protecting the CI components and their interconnectedness.

D.-S. Huang et al. (Eds.): ICIC 2016, Part III, LNAI 9773, pp. 54–66, 2016.
DOI: 10.1007/978-3-319-42297-8_6

1.1 CI Sectors

The four common characteristics discussed above permeate through the 16 CI sectors classified by the Department of Homeland Security (DHS) [12]. To get a good understanding of the concept of SoS within each sector, and cross-sectorial interdependence we have (arbitrarily) chosen 5 of them to discuss below.

Commercial Facilities Sector: This sector is classified into Social, Residential, Business, and Military segments. Social facilities operate to fulfill the social goals of the community and on a principle of "openness", and hence it is a vulnerable segment. Access to Residential buildings might range from semi-private to strictly private. It is known [10, 24] that hackers use remote devices to infiltrate make modifications to the embedded systems in power grids as well as in automobiles. Consequently, we need better and stronger protection methods to safeguard homes, especially the "senior homes". Most of Business facilities are also centers for social get-together. Protecting such facilities is much harder, although media-based technology and closed circuit TVs are widely used. Clearly, Military facilities that store weapons, large servers with confidential information of personnel, and strategic plans of significance for homeland security face greatest threats and should by necessity secured without fail. This sector is dependent on many other sectors, including energy, transportation, water, and emergency services sectors.

Energy Sector: The three major sub-sectors are electricity, oil, and natural gas. All industries, commercial sector facilities, and emergency services rely on electric power. Some of the risks and threats to electric power grids are cyber and physical infiltration, natural disasters, incompatible changes and interoperability failure in information technology infrastructure, and human errors. Other operational hazards, such as blowouts and spills, may be caused by political instability, and terrorist activities.

Transportation Sector: This sector is vital to economy, social well-being, and strategic operations of military. The important sub-sectors are aviation, maritime transportation, mass transit of humans and products, and pipeline. The assets and services of this sector touch on almost every other sector. Most importantly it depends on energy, information technology, and water. Sectors such as healthcare and manufacturing rely on uninterrupted services of this sector.

Financial Sector: This sector is a vital CI component, because any disruption of even a small nature will disrupt social harmony and might cause economic ruin. Power outages, hacking of communication network and cyber assets, and natural disasters have an immense setback on this sector. Cyber-attacks stand out as the primary source of disruption and misuse for this sector.

Healthcare Sector: Healthcare services in many countries are offered by private agencies, public hospitals, and government controlled clinics. The stakeholders need to cooperate with Emergency Services Sector, Chemical Sector, and Government Facilities Sector in order to manage the public health component of health care. This sector is dependent on transportation, energy, communications, information technology, and emergency service sectors. Since protecting this sector is vital for the social well-being of the nation, it is necessary to protect all sectors on which it depends.

From the above discussion it is clear that a CI sector is dependent on one or more CI sectors. Identifying the dependency relation among sectors as well as among the assets within sectors is crucial to investigate the risk factors and vulnerabilities that migrate (cascade) across related sectors. Recent incident of “9/11 attacks” convinces us of the cascading effect. It is in this context that we propose an asset model using which risk and vulnerability analysis can be done effectively.

1.2 Contribution

We define the basic concepts asset, threat, risk, and vulnerability in Sect. 2. We give a concise template, table-based approach, to describe assets in Sect. 3. We explain the semantics of the template segments and emphasize how inter-related assets have a compact representation in the asset table. In Sect. 4 we use the template representation to motivate vulnerability and risk analysis. We conclude the paper in Sect. 5 by pointing out our ongoing work in investigating network of agents and robots that use “deep learning” to collectively learn, rehearse, and collaborate in protecting CI assets and processes.

2 Basic Concepts

Vulnerability and risk analysis require the following five activities, in the order stated: (1) Identification of critical assets, and their dependencies; (2) Identification and assessment of threats to each asset; (3) Vulnerability analysis, which assess the vulnerability of each asset to the threats; (4) Risk calculation, which is the “expected loss to economy, and human lives”; and (5) Risk reduction through prioritization.

A physical asset is an item of economic value that has a tangible or material existence. For most businesses and governments, physical assets usually refer to cash, equipment, inventory and properties owned by them. Virtual assets are electronic data stored on a computer or the internet. A team of CI sector experts should identify critical assets in each CI sector. In general, if economic loss or damage to the integrity of society through the loss of an asset threatens the existence of its owner then that asset must be declared critical. After selecting and ordering critical assets in all sectors, the inter-relatedness between assets within each sector, as well as the intra-relatedness (dependencies across sectors) should be identified. This analysis is essential to understand the cascading effect of asset loss in the system. The experts shall develop a list of associated Critical Cyber Assets (CCA) essential to the operation of the Physical Critical Asset (PCA).

Threat is defined [3, 4] as “any indication, circumstance or event with the potential to cause loss or damage to an asset”. Threat analysis is done to recognize the plausible threats to an asset, based upon the asset features, environment characteristics, and the potential external motivations for harming the asset. Important threat types are (1) those caused by humans (insider, terrorist, military), (2) those caused by nature (hurricane, earthquake, forest fire, tornado, flood), and (3) those caused by humans using technology, cyber space, and communication network. The motive and capacity in triggering threats should be taken with threat types in assessing the likelihood of the attack, the frequency and duration of the attack, and its likely consequences. Vulnerability is defined [2] as a "weakness that can be exploited to gain access to an asset". Some of the common types of weaknesses are (1) physical (accessibility, relative location), (2) technical (eavesdropping, susceptible to cyber-attack), (3) operational (weak business and security policies), and (4) organizational (weak structuring). Risk is defined [4, 9, 12] as "the probability of loss or damage".

A systematic method to assess vulnerability starts with the identification of threats that has the potential to affect the assets in a critical system. A prerequisite is to have a model of system taxonomy, critical assets within each system, a definition of the "interrelatedness" among the assets, and an estimate of impact factor on assets. As an example, the system taxonomy in a sector may consist of the three subsystems "Mission Critical system", "Support System", and "Quality Assurance System". This taxonomy may be linked to the taxonomy of its sub-sectors, sectors that are dependent on it, and the sectors on which it depends. Once taxonomy is defined, the components within each subsystem and their assets should be identified. For example, components within "Mission Critical system" are "Control System", "Supervisory Human Experts", and "Communication System". Assets within Control System include *Instrument/Sensor/Analyzer, Controller, Control valves, and Software & Configuration.* Threat analysis for each asset within each subsystem must be conducted next. It is best based on the "interrelatedness among assets". Thus, modeling interrelatedness at sector level and at asset level within sectors is essential.

Interrelatedness property between sectors can be defined statically, with knowledge of the products and services produced by sectors. Static interrelatedness has been modeled by using matrices [18] and graph structures [13, 19]. Since assets within sectors may vary depending upon policy changes [19], cyber assets and system dynamics [23, 26] interrelatedness property may also vary dynamically. In general, an interrelatedness property is *transitive,* in the sense that if "asset A depends on asset B AND asset B depends on asset C", then asset A depends on asset C. Based on transitivity it is possible to define interrelatedness to higher orders. We say threat of asset A is *cascaded* to asset B if either "*B depends on A directly"* or "*B has a higher-order dependency on A*". Using directed graphs and higher-order dependencies an analysis of "cascading effect of risks" is given in [26]. In our research we explain how such an analysis can be done more efficiently by using the template model discussed in the following section.

3 A Template for Modeling Critical Assets

Once critical assets are identified within a sector and their distribution across the subsystems within that sector, the assets can be modeled to satisfy a set of requirements. We consider "Business/Management (BM)" and "Technical/Scientific (TS)" as the two groups who among themselves will define the system taxonomy. It is remarked in [4] that for BM group, who are involved with policy making and management of resources a top-down dynamic view is preferable, whereas for TS group a detailed bottom-up view of static and dynamic modeling is required. Both these requirements are met in our modeling technique. The key features are (1) each critical asset is modeled as a formal table in which protection mechanisms can be set for preserving information integrity and confidentiality, (2) the asset tables are linked using hyperlinks to model interrelatedness, and (3) a hierarchy of tables is defined based upon the nature of sectors. The CAS Knowledge Description Template (CASKDT), shown in Table 1, is the basic building block to create the asset model. The template CASKDT and the physical (or virtual) asset that it represents can be accessed by any authorized client in the system. Many methods discussed in [22] for protecting critical infrastructures can be adapted to secure CASKDT. The template description may be extended by adding more description elements, as and when policy changes and the criticality constraints vary. Thus, the model serves both static and dynamic requirements. The tabular format shown in Table 1 is meant for human agents in BM and TS groups. We have developed a GUI which automatically generates the XML version of the CASKDT. The XML version is used for knowledge propagation across the different system components for automatic analysis and decision making. Below we briefly discuss the structure and semantics of CASKDT components.

Table 1. Critical Asset Knowledge Description Template

Reference	<ADDRESS>, <URL>
Sector	<generic description of sector type> <link to specific sector information> <link to parent-sector> <links to subsectors>
Expert Knowledge	<link to expert opinions>

Functional Properties of Services	**Type of Use**: <service type>
	Attributes: <criticality level, access constraints>
	Relations:{depends, part-of, requires, contained-in}
	Priority:{ordered list of (asset, sector)}
	Utility:{<a_1, u_1>, <a_2, u_2>, …, <a_k, u_k>}

Nonfunctional Aspects, Trust and Threat Types	**Cost**: cost of replacement **Availability**: <availability constraints, replacement constraints, regional constraints> **History**: attack reports vulnerability and risk metrics list of potential threats **Other Knowledge in the Context of Threat**: link to knowledge store
Policy	**Legal Rules**: for asset sharing **Context Information**: location context, availability context **Context Rule**: for asset release
Exceptional Situations	**Side Effects**: environmental impact factors, emergency procedures

The “Reference” part specifies the “ADDRESS” of the physical location of the facility in which the asset exists, and the “URL” of virtual assets related to the physical asset. The “Sector” part includes (1) the sector name, a generic natural language description of the sector, (2) a link (URL) to a description of sector characteristics, (3) a link (URL) to the CASKDT of its parent sector, and (4) links to the CASKDTs of its sub-sectors. An authorized client/expert of the CASKDT can navigate to learn and reason about its relevance (for criticality), because tacit knowledge cannot be textually described. To assist in such reasoning, the Experts Knowledge section has a link to the expert opinions on the asset’s importance. In Functional Properties/Services section we list the assortment of services available through the asset, critical levels of services, access constraints, and the possible relations between this asset and other assets in the system. The “Relations” and “Priority” sections are very vital for cascade analysis and must be compiled with “experts knowledge” included in “Experts Knowledge” section. The relation “*asset A depends on Asset B*” may be used if the services of asset B are essential for one or more services of asset A. An example is “Nuclear Facility depends on Electricity”. If (s, a) precedes $\left(s', a'\right)$ in “Priorities” section it means that (1) the asset b of sector S modeled in the template is related to asset a of sector s and asset a' of sector s', and (2) the impact of threat spreading from (s, a) to (S, b) is higher than the impact of threat spreading from $\left(s', a'\right)$ to (S, b). In general, we can expect a large number of relations with different semantics to arise in asset specification. Consequently, in “Relations” section each relation name is a “hyper-link” to the cyber location where the relations and their meanings are stored in a directory. By traversing the hyperlinks in a template one can explore all the sectors/assets that are related to the asset/sector specified in it. Because of hyperlinks we can use “web navigation” techniques to conduct threat and risk analysis in an efficient way without having to have a full graph model, as done by many researchers [2, 7, 13, 20]. The representation {$<a_1, u_1>, <a_2, u_2>, \ldots, <a_k, u_k>$} is used to specify the utility factor u_i for the asset a_i, if the asset described in this CASKDT requires a_i. In the section “Nonfunctional…” we include the information necessary to evaluate the risk if this asset is vulnerable to certain threats. So, we have included threat types, attack incidents and how they were handled, availability of this asset in the market place, and the replacement cost. Any knowledge gained in the past is also included, for it might be used in risk analysis. The “Policy” section is useful for both BM and TS groups. The managers of the asset define the policy for asset sharing, determine where and how the asset is to be located (distributed), and define rules for releasing the assets for any application. The structure and semantics of CASKDT are both concise and precise. It is concise because the hyperlinks in the template inherently represent interconnectedness of assets. The description is precise because of the semantics. Each section can include only the information that respects the prescribed semantics. The two primary disadvantages of graph and network models [2, 7, 13, 20] are (1) they do not scale up to large CIs, and (2) they lack precise semantics. Although labeled graphs have been used [19, 21, 25] to assign semantics of interrelatedness the inherent complexity in exploring large graphs make such approaches difficult to adapt for assessing risk in large CIs. Another important virtue of our template representation is that a GUI developed by us can automatically generate the XML version which can be used for communication across system components and cyber communication network. Finally, the most important advantage of our approach is the inclusion of priority and context information in CASKDTs. They help in reducing the amount of information to be gathered dynamically for risk analysis, and in monitoring CI system performance in order to ensure the prevention of attacks in dynamic (such as mobile) situations. No other modeling approach has considered these two aspects; the exception is the recent work [1] which has considered context in the modeling stage. However, no specific method for risk analysis has been reported.

4 Vulnerability and Risk

The two broad categories of Risk Assessment (RA) methodologies *are Structural Analysis (SA), and Behavioral Analysis (BA).* Structural approaches view the CI as a SoS topology [14] in accounting their interdependencies. A SA approach starts developing an interdependency model [18, 21, 23, 25] for use in vulnerability analysis. The graph models annotate edges with information on demand/supply, utility factor, and constraints on service flow. Behavioral approaches [23] focus on developing mathematical definitions to analyze failure (fault) models, failure analysis (causes for failures), and failure propagation (cascading). Probabilistic methods and linear optimization [13] have been used to assess cascading behavior. Given threat probabilities, these approaches attempt to generate all possible event (threat) combinations and compute the probability of failure under each scenario.

Our approach, explained in Fig. 1, is a modification of the approach suggested by Baker [3]. In our approach both static and dynamic flow of threats are combined from the asset model, which is both a structural and behavior model. As a motivation, we explain the vulnerability assessment procedure for a simple case of "Electric Power System". The full vulnerability assessment procedure of this problem can be found in The National Security Telecommunications Advisory Committee Information Task Force Report [19].

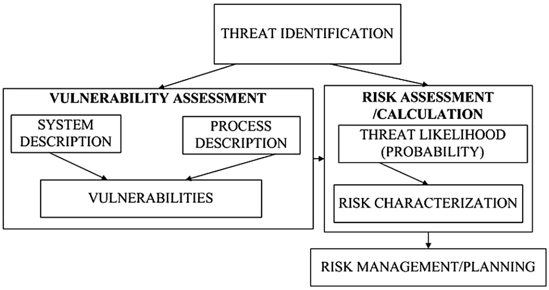

Fig. 1. Risk Assessment Process

The first step is to identify the subsystems for the Power Grid. For the sake of simplicity, we consider the four subsystems "The Control Center, The Substation, The Communications Infrastructure, and The Distribution Network". For each one of these subsystems the CASKDT asset models are created, and vulnerabilities based upon their services/functionality, are assessed. For example, the primary functionality of the Control Center is to monitor power system operations, save history of its operations, and allow the functioning of the control unit under its domain. Other operations include monitoring transmission systems, power distribution networks, and customer distribution loads. We emphasize that support systems are often easy to attack, because they may not be protected as securely as the main mission-critical subsystems. Therefore, it is essential to include the vulnerable points/events and assign priority to them. Key points of vulnerability are (1) remote ports, (2) links to Internet and Internal Information Management Systems, (3) tools that enable support functions to vendors and customers, (4) flow of power to the central facility, and (5) support system links. In a similar fashion the functionality and vulnerability are assessed for other units. From the list of CASKDTS and the functionality of assets we identify the interrelatedness between the assets in the subsystems by navigating the hyperlinks in the CASKDT. A fault-tree is constructed for each asset in each chain created by hyperlinks navigation. A parallel activity for system development team and experts is to list a set of threats and hazards that affect each one of these assets (physical and cyber). The experts should associate with each threat its "threat level", which will be required in the calculation of risk factor. Based on this set of information, risk analysis can be done using matrix algebra, as explained next.

Navigating through the hyperlinks on "Relations" and "Priority" we will get a set of chains, where a chain is a sequence of hyperlinks. We need to analyze each chain for risk. Let us write $\sum = \{\tau_1, \tau_{2,\ldots,} \tau_m\}$ to denote a finite set of threats, and $\Lambda = \{\alpha_{1,} \alpha_{2,\ldots,} \alpha_n\}$ to denote the set of assets in a chain. A threat matrix A of size m × n, whose rows are threats and columns are assets can be constructed. The ith row, j^{th} column entry A[i, j] is the severity level of threat τ_i on the asset α_j. Below we explain a few operations on threat matrices that are sufficient to calculate risks arising from interrelatedness of any order.

Subsystem Threat Matrix: Every subsystem s_k has a finite set α_k of assets. Hence $\alpha_k \subset \Lambda$. The threat matrix A_k for the subsystem s_k is the projection of matrix A on the columns defined by α_k. The set $\sum_k$ of threats that are associated with the subsystem s_k is the set of rows in A_k.

Interrelatedness: Subsystems s_k and s_r have *first-order* interrelatedness if their threat matrices have a non-empty intersection, in the sense that either (1) $\alpha_k \cap \alpha_r \neq$ empty, or (2) $\sum_k \cap \sum_r \neq$ empty.

Cascading: We say s_k and s_r have nth-*order interrelatedness* if they are both in the same chain and there exists $n > 1$ links between them. The progression of threat from one to the other is called cascading effect. First we discuss the cascading effect for one type of first-order interconnection relation, namely for relation "*requires*". Next, we explain how to handle cascading effect. Assume that s_k requires s_r, meaning that the subsystem s_k has one or more assets and each one of them requires the services (functionality) of one or more assets from the subsystem s_r. Each "requesting asset" in

s_k is more vulnerable to the threat attack that will infest the "requested asset" in s_r. Hence it is prudent to "raise" the "severity level" of the "requesting asset". This is accomplished as follows: (1) Denote by A_k and A_r the threat matrices corresponding to the subsystems s_k and s_r. (2) If the matrices are "disjoint" (do not have common assets or common threats) then no cascading happens, because "request" is void. If the matrices have common assets then for each common asset α_p we "augment" the matrix A_k as follows. Let the column number in A_k that corresponds to the asset α_p be p_k, and the column number in A_r that corresponds to the asset α_r be p_r. Notice that p_r and p_k are threat vectors, and some of the threats in p_r may or may not be in p_k. In the former case we will replace the vulnerability value by "the sum of the vulnerability values of the threats common to both", and in the latter case we will augment the matrix by adding a new row for the new threat being cascaded from p_r. These two cases are explained next:

Case 1: Let the threat τ_r^i be the i^{th} row of matrix A_r, and let this threat be in the j^{th} row of matrix A_k. So, we must raise the 'severity level' of this threat in matrix A_k by the amount $A_r[i, p_r]$. That is, the new augmented matrix entry is

$$A_k^{'}[j,\ p_k] = A_k[j,\ p_k] + A_r[i,\ p_r]$$

Case 2: Let the threat τ_r^i be the i^{th} row of matrix A_r, and let this be not a threat in A_k. Then, we should augment matrix A_k, which we do by (1) introducing it in A_k as a new row, and (2) copying the severity level $A_r[i, p_r]$ in column p_k of A_k, while setting the other entries of the new row to 0. To achieve this effect, we let the number of rows and columns in matrix A_k to be r_k and c_k. The augmented matrix entries are

$$A_k^{'}[r_{k+1},\ p_k] = A_r[i,\ p_r], A_k^{'}[r_{k+1},\ j] = 0, 1 \le j \le c_k,\ j \ne p_k. \qquad (1)$$

Example 1. We illustrate threat level calculation when subsystem s_k *requires* (first-order relation) subsystem s_r. The subsystem s_k has three assets and two threats on them. The *subsystem* s_r has two assets and three threats on them. One asset and one threat are common to both subsystems. Two threats that are new in s_r will affect s_k because "s_k *requires* s_r". The threat matrices for the systems are

$$A_k = \begin{bmatrix} & a_1 & a_2 & a_3 \\ t_1 & 0.2 & 0 & 0.6 \\ t_2 & 0.1 & 0.7 & 0.8 \end{bmatrix} \text{ or } B_r = \begin{bmatrix} & b_1 & a_3 \\ t_1^{'} & 0.8 & 0.1 \\ t_1 & 0.7 & 0.9 \\ t_3 & 0.8 & 0.4 \end{bmatrix}$$

Let $A_k^{'}$ denote the cascaded threat matrix. It will have three columns corresponding to the assets a_1, a_2, a_3, because the numbers of assets do not change. Since threat t_1 (first row of A_k) affects the common asset a_3 (in the second row of A_r) the severity level of a_3 becomes 1.5. However, assets a_1 and b_1 are mutually exclusive, meaning that the threats affecting b_1 will not contribute to the "requesting" subsystem. Hence, the threat vector for t_1 in the cascaded system matrix $A_k^{'}$ is (0.2, 0, 1.5). The threat vector t_2 (second row in A_k) is not influenced by the threat matrix A_r. Hence the t_2 row in matrix $A_k^{'}$ is the same as the t_2 row in A_k. Both threats $t_1^{'}$ (first row of A_r) and $t_3^{'}$ (third row of

A_r) affect asset a_3, which is also an asset of system s_k (third column in matrix A_k). They have a cascading effect, which is captured by two new rows introduced in matrix $A_k^{'}$, one for $t_1^{'}$ and another for t_3. The threat levels in these two rows are calculated using Eq. (1). The resulting matrix is

$$A_k^{'} = \begin{bmatrix} & a_1 & a_2 & a_3 \\ t_1 & 0.2 & 0 & 1.5 \\ t_2 & 0.1 & 0.7 & 0.8 \\ t_1^{'} & 0 & 0 & 0.7 \\ t_3 & 0 & 0 & 1.2 \end{bmatrix}$$

Example 2. We explain here threat level calculation when subsystem s_1 requires (nth-order relation) subsystem s_n. Let us denote the chain by s_1 -> s_2 -> … -> $s_{1(n-1)}$ -> s_n. Let their threat matrices be A_1, A_2, …, $A_{(n-1)}$, A_n. We start computing the augmented matrix $A_{(n-1)}^{'}$ for the pair ($A_{1(n-1)}$, A_n.), by using the steps shown in Example 1. Let us write $A_{(n-1)}^{'} = \text{Aug}\left(A_{(n-1)},\ A_n\right)$. Next we calculate $A_{(n-2)}^{'} = \text{Aug}\left(A_{(n-2)},\ A_{(n-1)}^{'}\right)$. Proceeding backwards in the chain until we calculate $A_{(n-1)}^{'} = \text{Aug}\left(A_1,\ A_2^{'}\right)$.

These results are sent by the "Vulnerability Assessment" component to "Risk Calculation Component". Essentially risk implies "uncertainty" and hence risk calculation is based on probability distribution on the set of threats. Expected loss or damage to an asset or a subsystem is calculated by "multiplying the threat severity levels (which are measures of adverse impacts caused by successful threat events) with the probabilities associated with threat/vulnerability". For each category a severity level (say in the range [1, 10]) may be assigned. In order to calculate the "expected risk" of an asset (facility or process), one determines (1) the probability p that the asset will be attacked, (2) the conditional probability q (given the attack probability) that a specific means (such as using a remotely enabled device that blows up) is employed, (3) the probability r of success when that means is used, and (4) damage estimate C (damage to asset). Then, the expected loss E is $p \times q \times r \times C$. Because this number E is only an estimate, often it is "normalized" and expressed qualitatively (Severe, High, Medium, Low). Risk management activity will investigate methods that can reduce risks, such as disabling the adversary before the attack, minimizing the vulnerabilities, and reducing the impact or consequences of an attack. Another way to reduce risk is to distribute the assets geographically to locations where the likelihood of threat is a minimum.

5 Conclusion

The primary merits of CASKDT modeling are its conciseness and precision. It has a rich expressive power to include a wealth of diverse information. It can be expanded and viewed either graphically or mathematically or virtually. As suggested in [25] we can have a multi-agent system consisting of heterogeneous, autonomous, and decentralized agents for template-based CI modeling and risk analysis. Agents can express templates into XML files that can be communicated across sites in a cyber medium. Agents can be taught the semantics of CASKDT and graph algorithms to expand the hyperlinks, generate partial subgraphs for given semantics of interconnectedness, and explore large sparse matrices in order to perform different vulnerability/risk calculations. A Robot is an executable engine in which agents collaborate. Consequently, we can train the agents in a multi-agent system to acquire sector-specific knowledge (CASKDT), facility topologies, terrestrial and aerial views in the surrounding of a facility, and embed it in a robot. Such a robot can be specialized to navigate hazardous terrains and adapt to different attack scenarios. We believe that robot systems approach can be strengthened by automatic learning techniques [17] and "deep learning algorithms [5]".

We also recognize that infrastructure vulnerability and resilience are related to community resilience. Hence it is necessary to include social, organizational, economic, and environment factors in the CI model. However, none of the methodologies practiced today have incorporated the social aspects into the analysis of CI vulnerability. However, there is a great interdependency between humans and CI components in modern times. Bea et al. [4] argue that no system, regardless of how technical or physical it is, is not solely physical and technical. According to their report 80 % of the failure in the Oil and Gas production platform in the North Sea was firmly rooted in human, organizational, and institutional failures. Human factors related to reviews and decision making in CI monitoring and maintenance operations have also contributed to malfunctions in the engineering and control aspects of the system [11]. In a recent monograph, Lazari [16] has discussed the human factor in CI protection, and emphatically states that "the relevance of the human factor in the field of CIP cannot be hidden or underestimated". We reckon that robots, embedding of multi-agent systems, may be given initial models of social, and human aspects related to CI protection, and be trained to combine them with CI model through "deep learning techniques". They might produce unpredictable and surprisingly genuine solutions, after playing against its adversary repeatedly and improving its strategy in every step of their learning cycle.

Acknowledgement. We thank the reviewers for their insightful comments that helped us to improve the paper to the current form.

References

1. Alcaraz, C., Lopez, J.: Wide-area situational awareness for critical infrastructure protection. IEEE Comput. **46**, 30–37 (2013)
2. Arboleda, C.A., Abraham, D.M., Richard, J.P., Lublitz, R.: Vulnerability assessment of healthcare facilities during disaster events. J. Infrastruct. Syst. **15**(3), 149–161 (2009)
3. Baker III., G.H.: A vulnerability assessment methodology for critical infrastructure facilities. In: DHS Symposium, R&D Partnerships in Homeland Security, USA, pp. 1–15 (2005)
4. Bea, R., Mitroff, I., Farber, D., Foster, H., Roberts, K.H.: A new approach to risk: the implications of E3. Risk Manage. **11**, 30–43 (2009)

5. Bengio, Y.: Learning deep architectures for AI. Found. Trends Mach. Learn. **2**(1), 1–27 (2009)
6. Canadian Government Report. Critical Infrastructure. http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx
7. Eusgeld, J., Kroger, W., Sansavini, G., Schläpfer, M., Zio, E.: The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. Reliab. Eng. Syst. Saf. **94**(5), 954–963 (2009)
8. Filippini, R.: Mastering complexity and risks in modern infrastructures: a paradigm shift. GRF Davos Planet@Risk **3**(2), October 2015
9. Giannopoulos, G., Filippini, R., Schimmer, M.: Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. In: European Commission Joint Research Centre, Institute for the Protection and Security of the Citizen (2012)
10. The Hacker News. http://thehackernews.com/search/label/car
11. Hellstrom, T.: Critical infrastructure and systemic vulnerability: towards a planning framework. Saf. Sci. **45**(3), 415–430 (2007)
12. Homeland Security. What is Critical Infrastructure? http://www.dhs.gov/what-critical-infrastructure
13. Ibanez, E., Gkritza, K., McCalley, J., Aliprantis, D., Brown, R., Somani, A., Wang, L.: Interdependencies between energy and transportation systems for national long term planning. In: Gopalakrishnan, K., Peeta, S. (eds.) Sustainable & Resilient Critical Infrastructure Symposium. Springer-Verlag, Heidelberg (2010)
14. Jamshidi, M. (ed.): Systems of Systems Engineering. Innovations for the 21st Century. John Wiley and Sons, New York (2008)
15. Kotzanikolaou, P., Theoharidou, M., Gritzalis, D.: Interdependencies between critical infrastructures: analyzing the risk of cascading effects. In: Bologna, S., Hämmerli, B., Gritzalis, D., Wolthusen, S. (eds.) CRITIS 2011. LNCS, vol. 6983, pp. 104–115. Springer, Heidelberg (2013)
16. Lazari, A.: European Critical Infrastructure. Springer Publications. ISBN 978-3-319-07496-2 ISBN 978-3-319-07497-9 (eBook) (2014)
17. Patrascu, A.: Cyber protection of critical infrastructures using supervised learning. In: 20th International Conference on Control Systems and Computer Science, Bucharest, May 2015, pp. 461–468 (2015)
18. Pederson, P., Dudenhoeffer, D., Hartley, S., Permann, M.: Critical Infrastructure Interdependeny Modeling. A Survey of U.S. and International Research, INL, INL/EXT-06-11464 (2006)
19. Peters, J.C., Kumar, A., Zheng, H., Agarwal, S., Peeta, S.: Integrated Framework to Capture the Interdependencies between Transportation and Energey Sectors due to Policy Decisions. USDOT Region V Regional University Transportation Center Final Project, NEXTRANS Project No. 079PY04, Purdue University, West Lafayette, IN, USA (2014)
20. The President's National Security Telecommunications Advisory Committee. Information Assurance Task Force for Power Risk Assessment (1997). http://www.securitymanagement.com/library/iatf.html
21. Quyang, M., Hong, L., Maoa, Z., Yua, M., Qi, F.: A methodological approach to analyze vulnerability of interdependent infrastructures. Simul. Model. Pract. Theory **17**(5), 817–828 (2009)
22. Rice, M., Shenoim, S. (eds.): Critical Infrastructure Protection IX, IFIPAICT 466 (2015)
23. Rosato, V., Issacharoff, L., Tiriticco, F., Meloni, S., De Porcellinis, S., Setola, R.: Modelling interdependent infrastructures using interacting dynamical models. Int. J. Critical Infrastruct. **4**(1–2), 63–79 (2008)

24. SANS Institute: Can Hackers turn Lights Off? The Vulnerability of the US Power Grid to Electronic Attack. Technical Report, SANS Institute (The Information Security Reading Room) (2001)
25. Stapelberg, R.F.: Infrastructure Systems Interdependencies and Risk Information Decision Making (RIDM). Syst. Cybern. Inform. **6**(5), 21–27 (2008)
26. Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., Lykou, G., Gritzalis, D.: Time-based critical infrastructure dependency analysis for large-scale and cross-sectorial failures. Int. J. Critical Infrastructures Protection **12**, 46–60 (2016)