LA-UR-04-6927

Approved for public release; distribution is unlimited.

Title: ROBUSTNESS OF INTERDEPENDENT INFRASTRUCTURE SYSTEMS

Author(s): Mihaela Quirk and KEVIN SAEGER

Submitted to: HYBRID SYSTEMS: COMPUTATION AND CONTROL - 2005 CONFERENCE

Los Alamos
NATIONAL LABORATORY

Form 836 (8/00)

Robustness of Interdependent Infrastructure Systems

Mihaela D. Quirk, Kevin J. Saeger
Los Alamos National Laboratory .

For Submission to Hybrid Systems: computation and Control - Conference March 2005. This paper will be reduced to about 14 pages- without addition of technical information. The (only) difference from Los Alamos National Laboratory Unclassified Report LA-UR-04-3910 is the addition of section Mathematics/closed form of metrics - 2 The new Mathematics/closed form of metrics will be a merge of the two sections here.

1 Abstract

This report proposes a methodology for estimating robustness across interdependent infrastructures. The introduction describes the challenges of the task. The second section addresses robustness across critical infrastructures from the stand point of the missions to be accomplished. Robustness equates to being the sustenance of a critical mission, under adverse conditions, caused primarily by the loss of one or more support infrastructure components. The metrics associated with this novel approach to robustness are discussed. Robustness may be assessed over various collections of infrastructure components, at various geographical scales. The last section provides future directions for generalizing the methodology nationwide, with emphasis on the use of the metrics in the context of the challenge of protecting our most valuable assets from terrorist threats.

2 Introduction

A methodology to estimate robustness across infrastructures is derived. This methodology is the basis for the design of a system intended to assist analysts and decision makers to address critical infrastructures and key assets protection and failure mitigations.

An infrastructure may suffer physical damages caused by natural causes, accidents or intentional attacks. These attacks may be stealthy in nature, such as cyber attacks. All types of damages to one or more infrastructures are referred to as disruptions.

The national infrastructures are highly interconnected, physically, through a cyber-based system and logically by rules and regulations. The term "interdependent" is used in this context to express all types of influences that the behaviors of infrastructures have on one another.

3 Critical infrastructures and key assets

3.1 Introduction

The Critical Infrastructure Assurance Office defines an infrastructure as [35]: "The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures) and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels and society as a whole."

The fourteen infrastructures are:

- food
- water supply systems
- agriculture
- public health systems
- emergency services – including continuity of government
- energy (electrical, nuclear, gas and oil, dams)
- transportation (air, road, rail, port, waterways)
- information and telecommunications
- banking and finance
- chemical industry and hazardous materials
- defense industrial base
- postal and shipping
- national monuments and icons

- government facilities.

The solution to the problem of mitigating infrastructures' failures from natural causes or intentional attacks is not a simple academic exercise. A variety of theoretical results and practical solutions, within a system engineering paradigm, may answer the complex and large scale problems that describe the functioning of infrastructures, their interdependencies and mitigation of the effects of disruptions. One field that is contributing to the understanding of infrastructure interdependencies is that of complex adaptive systems. A *complex adaptive system* is a system with the following characteristics [11]:

1. it consists of a large number of interacting *agents*
2. the agents exhibit emergence; that is, a self-organizing collective behaviour difficult to anticipate from the knowledge of agents' behaviour
3. the emergent behaviour of the agents does not require necessarily the existence of a central controller.

Complex adaptive systems have survival capabilities from features such as: adaptability, interactivity, self-maintenance and diversity. Section 4.2 gives descriptions of these attributes.

Examples of complex systems are biological systems, the Internet, computer networks, and the electric power grid.

National infrastructures are *heterogeneous* complex adaptive systems where each infrastructure is a complex adaptive system on its own. Any national infrastructure may be modeled as a graph network, with various degrees of dynamic connectivity. The electric power network is very highly connected whereas the Monuments and Icons infrastructure has a lower connectivity [4, 13, 38]. The interdependencies induce an elevated degree of complexity of any model for the national infrastructures viewed as complex adaptive systems.

The task of integrating interdependencies in a model is a continuous challenge; for the electric power grid alone there is a large research and development effort to address contingencies [6]. Many of the solutions devised for the electric power grid are adopted in the area of modeling and simulation of interdependent infrastructures, as well as mitigating contingencies.

3.2 Key factors

In addressing the behavior of national infrastructures, three factors govern a significant part of any modeling effort:

1. **Cascading effects.** The electric power grid is an example of a network where cascading failures are caused by malfunctioning of a small number of components of the network. The Finance and Market sector displays an analog tendency to cascading failures. A disruption of an infrastructure that delivers critical services and supplies critical goods may have very costly economic, health and security impacts. Understanding cascading effects is the first step in preventing them [8, 7, 44].

2. **Time-scale.** The time acts in different ways in quantifying the effects of disruptions as well as restoring lost services. A time-scale that is meaningful for the agriculture sector (weeks, months) is unacceptable for the electricity sector or for the emergency infrastructure. Also, dependence on Internet communications may influence the time-scale that should be considered in modeling a certain sector or infrastructure [43, 44].

3. **Interdependencies.** There are four main types of interdependencies: geographical, physical, cyber and logical. Geographical interdependencies occurs when elements of multiple infrastructures are situated in spatial proximity. Physical interdependency reflects the influence of the material output(s) of one infrastructure on the input of another infrastructure. A cyber dependency is understood in any instance when the state of an infrastructure depends on data transmitted through the information highway.

   Logical interdependencies capture all effects that are not related to physical, geographical or cyber connections. This type of dependency derives from a control schema that links agents form one infrastructure to agents from another infrastructure, and the connection is not of the three previous interdependency types. An example is the logical interdependency between the electric power and the financial infrastructures. In California, the deregulation legislation had influenced both infrastructures and induced the power crisis in this state in late 2000. The logical interdependencies are influenced predominantly by human decisions [38].

   One special case of the interconnection of infrastructures is realized by a cyber-based system – that is, information and communication technologies. The effects of cyber-threats and cyber attacks may be very costly and should constitute a parameter in any modern risk analysis of infrastructure vulnerabilities as well as in any effort aimed at the prevention and minimization of cascading effects. The type of damages caused by cyber attacks may vary, from poor services expressed in economic losses, to panic and discomfort expressed in loss of public confidence in the attacked infrastructure. The Critical Infrastructure Assurance Office of the United Stated Department of Commerce [47] delivered to Congress the first status report on private sector efforts to bolster cyber defenses for systems that run critical sectors of the economy. In the present study

it is assumed that there exist a methodology and measurements in place to address the disruptions caused by cyber threats and attacks.

The sought models of infrastructures have the capability to explicitly deal with time lags, and the flexibility to link databases, other models and fuse diverse types of information [13, 15, 28] .

3.3 Infrastructure description

National infrastructures are divided into sectors, segments and sub-segments. The term "components" is used to denote an element of an infrastructure, similarly to that of a "node" of a network [1]. For example, a national park is a component of the monuments and icons infrastructure.

In the remainder of the document the term "domain of interest" is used for ensembles of infrastructure components, at various geographical scales or over networks. Examples of domains of interest:

- a critical infrastructure to be protected
- an ensemble of sectors from multiple infrastructures
- a sector of an infrastructure for which there exists a threat – such as the cattle industry, which is a sector of the agriculture infrastructure
- a whole city for which there might be intelligence gathering that a terrorist thereat is imminent
- the airline industry – even localized to one flight – as a sector of the transportation infrastructure
- the White House is a domain of interest with components from the government, transportation (the roads to White House. helicopters), emergency, telecommunications and energy infrastructures
- a node of an infrastructure network – such as a branch of a bank from the finance and markets infrastructure, with other infrastructure components present, such as telecommunications and energy components.

[1]The term "node" is used only when the discussion is specific to a network.

Moreover, domain of interest denotes *our* interest to protect the critical infrastructure components that are part of the domain. There is also a dual interest: from the *adversary*'s viewpoint. The airline industry was the adversary's domain of interest – as the mean to carry an attack – during the preparation and development of the World Trade Center attack. The critical infrastructure sectors are the domains of interest over which critical missions are defined with the purpose of protecting them.

"A definition is no stronger than its weakest link" [34]. The term "domain of interest" is intended as a generic term and it is not a "definition" in the proper sense, with a *genus proximus* and a specific difference provided [2]. "Domain of interest" is similar to "private entities" used in a document issued by the Department of Homeland Security (DHS) [2] with the same purpose. It would make the DHS document harder to read if all components of the "private entities" would be listed. The same simplification and common sense understandings applies to the use of "domain of interest". The terminology introduced is not exhaustive and it is intended as a shortcut in discussions and examples. Throughout this report, the domain of interest is either explicitly indicated or it denotes the infrastructure, sector or sub-sector discussed.

3.4 Critical missions and induced functions

3.4.1 Preliminaries

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets [2] provides the guidelines for a variety of missions required to meet the strategic objectives of the critical infrastructures, national security, governance, public health and safety, economy and public confidence.

Acts of terrorism may cause damages such as [2]:

- impair the federal government's ability to perform essential national security missions
- undermine state and local government capacities to maintain order and deliver essential public services
- damage the private sector's ability to deliver essential services and to ensure the proper functioning of the economy

[2] A definition has two parts: a *genus proximus* that classifies the object to be defined in a large class where it belongs and a *specific difference* that identifies the object from other objects in the class. Example: the electric power grid is an infrastructure sector that is responsible with the production, transmission and delivery of electric energy. The genus proximus is "infrastructure sector" and the specific difference the remainder part of this example definition.

- undermine the morale of the public and the confidence in our national economic and political institutions.

Eight principles govern the aforementioned Strategy:

1. assure public safety, public confidence and public services
2. establish responsibility and accountability: organizations and individuals outside the federal government must take the lead in many aspects of critical infrastructure and key asset protection
3. encourage and facilitate partnering among all levels of government and between government and industry
4. encourage market solutions whenever possible; compensate for market failure with focused government intervention
5. facilitate meaningful information sharing
6. foster international security cooperation
7. develop technologies and expertise to combat terrorist threats
8. safeguard privacy and constitutional freedoms.

In the context of disruptions, the definition of criticality of infrastructures parallels the definition for network systems [3]. In case of a domain of interest that comprises components from various infrastructures, criticality may be discussed over sets of infrastructure configurations – that is collection of infrastructure components from possible more than one infrastructure. Figure 1 is an example of infrastructure configurations that contain critical components from the constituent infrastructures.

When a domain of interest is under a specific threat, the extent of the damage dictates whether the domain and its infrastructure components are in a critical state. However, this change of status is the result of case-by-case analysis effectuated by subject matter experts. For example, the emergency courses of actions depend on the number of people who are at risk. There exists threshold values to change from one type of course of action to another. Suppose that this threshold is 10000 (Category III attack). This large number of people at risk triggers a new set of measurements to address this attack. However, the subject matter experts

[3] A component or a sub-network of a network is called critical if its failure causes a significant degradation – even total failure – of the network [10, 29].

might decide that for a certain event in a city, the threshold should be lowered to 9500. This simple example shows that in fact the thresholds that exist are in general not hardwired. For the nuclear plants, it is clear that there is "zero tolerances", i.e., no plant may release nuclear material into the atmosphere.

For each critical infrastructure, sector, or type of key asset that supports an essential mission [2], a *critical mission* is formulated as a goal or set of requirements to be accomplished. As an example, suppose that there exists intelligence gathering that a bio-threat targets the poultry sector. A mission is formulated at the highest decision making level, as simply as: prevent infections of live stock. The technical details of accomplishing this mission are discussed later. This study develops under the assumption that there exists a collection of critical missions, formulated for each infrastructure, sector, segment or sub-segment and for many types of threats.

The critical mission establishes the services and assets that must be maintained and protected at the level of the governing essential mission. For example, a mission may be defined for milk and diary products and another one for the whole food infrastructure.

The disruption of infrastructure components over a domain of interest may be characterized by an "attack vector" [4]. The components of the attack vector show the infrastructures that are under threat, disrupted. The interdependencies indicate also the consequences propagated from one disrupted infrastructure to other infrastructures. One can view this process as: an attack vector points to a certain domain of interest. This attack vector "highlights" certain critical missions, from the collection of critical missions. There might be attack scenarios where the attack vector indicates a certain infrastructure under disruption, but with consequences that affect severely another infrastructure(s). Section 3.4.3 discusses prioritization strategies that are employed to address attacks that trigger more than one infrastructure at a time. Section B discusses attributes of the attack vector based on studies of optimal allocation of resources for critical infrastructures protection.

Example 3.1. If there is foot and mouth disease at a farm, the roads around the affected area are closed. If there is the intent to shut off the roads into a major transportation hub, it suffices to either infect the local livestock with foot and mouth disease or use a cyber intrusion to misinform the authorities (i.e., by spreading the news of a foot and mouth disease outbreak). The effect is ultimately the closure of a major road network. The loss of livestock in the area may be negligible for the food industry, whereas the road closures might carry more costly effects.

[4] A more consistent term would be "disruption vector " - however by convention the attack vector reflects both random failures and intentional acts of terrorism/sabotage

A few examples of critical missions formulated for various domains of interest follow. These examples are suggested by [2].

Example 3.2. Mission: "Protect the nuclear plants". The domain of interest is, obviously, the nuclear plants. The attack vector points to the energy infrastructure. The outage of a nuclear plant causes loss of energy. A nuclear accident at a plant may have other undesired effects such as: panic and loss in public confidence due to bad publicity. This example is revisited in Section 3.4.4.

Example 3.3. Mission: "Protect a specific crop against devastating diseases." This mission is intended to a certain sub-segment of the agriculture infrastructure and a possible attack points to that sub-segment.

Example 3.4. Domain of interest: the government infrastructure components in Washington, D.C. Mission: "ensure evacuation of the president in case of an attack"; the government infrastructure must ensure the safety of the president.

One may question the relevance of the formulation of a critical mission; however recall that the critical mission is defined at a high decision making level, such as DHS. The critical mission is formulated as a short statement, and technical details are yet to be specified by the subject matter experts. It is in general obvious what the critical mission is for a sub-segment of a single critical infrastructure. For a domain of interest with components from many infrastructures there may be more than one critical mission enacted, depending on the characteristics of the attack vector that shows which part of an entity suffers the most damage during a disruption and/or is the most vulnerable. To show the plurality of critical missions, two examples are given:

Example 3.5. Los Alamos, NM, May 2000: protect the scientists in Los Alamos during the Cerro Grande fire and plan their evacuation; this critical mission was successfully accomplished. The attack vector has two strong components: one pointing to the Government infrastructure (the Los Alamos National Laboratory and its Plutonium facility) and another one to the public health infrastructure (the people in Los Alamos and other areas that may be affected by the release of radioactive substances into the atmosphere). Two missions could therefore be activated. Note that the threat, however, comes from only one source: the forest fire.

Example 3.6. Washington, D.C.. Suppose there is a "dirty" bomb threat. A critical mission may be: ensure the evacuation of the foreign diplomats. The attack vector points to the government infrastructure. When a mission dictates to protect the population of Washington, D.C., then the public health infrastructure is the one to which an attack vector points to. Here again the attack vector comprises two significant components.

3.4.2 Self-healing property of a complex adaptive system

A self-healing system has the ability to automatically recover from disruptions. The concept of self-healing or "smart" networks arises from the challenge to develop intelligent agents that ensure the delivery of critical services [5, 29]. In addition, cascading effects are prevented, eliminated or significantly reduced. Typical examples of smart networks are the electric power grid, computer networks and biological systems [16]. Technical solutions that address effective security investments for the electric power grid propose adaptive intelligent "islands" intended to localize the damages caused by a disruption [8, 43, 44].

A collection of infrastructure components endowed with the self-healing property acts similarly. A domain of interest – as a complex system of interdependent infrastructure components – has the self-healing mechanisms more intricate. The challenge of a self-healing domain of interest is to handle complex aggregate of the self-healing mechanisms of each of the infrastructure components comprising the domain.

One can regard the self-healing property of a complex system as a refinement of the survivability quality of a computer network. Survivability is the ability of a system to fulfill its mission, in a timely manner, in the presence of failures, accidents or attacks. Three attributes characterize survivability: resistance (deter an attack), recognition and recovery [29].

An attack may be physical or stealthy in nature (cyber terrorism). The analysis of the behavior of the infrastructure components commences with the identification of the critical sub-networks and a study of the interdependencies. The ability to sense an attack or compromised components is essential for both planning mitigation strategies and preventing cascading effects [29].

An electric power grid may have all – or most of – the self-healing and recovery mechanisms deploy automatically; it is not so obvious that recovery can be fully automated for any collection of infrastructure components – or domain of interest. Recall that during a disruption the "pulse" of the domain of interest is regulated by the decision makers. By convention, a smart collection of networks – or a smart domain of interest – is one whose recovery mechanisms comprise automatic processes and reconfigurations of the infrastructure components, such that the critical mission is sustained. The self-healing mechanisms are considered further, after discussions on metrics and robustness develop and examples are given.

Example 3.7. Suppose that the domain of interest is city X scrutinized mainly with respect to its ability to cope with attacks that target a large number of people – such as biological attacks. Consider the scenario of an attack during which the hospital H1 is the closest to the accident scene. The attack vector has its most significant component toward the public health infrastructure. The critical mission for the public health is obviously "treat the injured peo-

ple". Suppose that while directing people to hospital H1, a power outage occurs at H1. The capacity of H1 is diminished; critically injured people are admitted to H1 while the rest of the injured are redirected to hospital H2. The public health infrastructure reconfigures itself: the component H1 was partially disabled and the component H2 was fully employed. The critical mission is sustained as long as there are no fatalities as a result of longer route to the hospital. To complete the example, the public health infrastructure may employ other components such as mobile hospital units. This example is revisited in Section 3.4.4 to address more details stemming from the critical mission. The domain of interest city X may deploy self-healing mechanisms to restore the power of the outaged areas (including hospital H1). In this alternative, redirection of a large number of patients may not be necessary. The power restoration involves primarily the self-healing properties of the power grid – and it shows how the self-healing attribute of one system (power grid) induces self-healing attributes of the heterogeneous aggregate of complex systems that constitute a domain of interest.

Figure 1 shows an abstract representation of reconfiguration of infrastructure components. In this example only three infrastructure are considered – one can view a domain of interest under scrutiny comprised of only three infrastructures. Or, one can assume that under a certain attack only three infrastructures are seriously threatened and possibly disrupted. Suppose that Configuration 1 corresponds to normal state of functioning. For a certain disruption, Configuration 2 represents the response of the domain of interest to this disruption. Observe that the components from Infrastructure 3 are all dropped and new components are employed, whereas components from Infrastructure 2 are all kept in Configuration 2 as well.

In the context of critical infrastructures, sectors, segments and sub-segments as well as private entities, the "automatic component" of the smart mechanisms is simply understood in the sense of having self-acting or self-regulating mechanisms [1]. The self-healing mechanisms prevent the use of already vulnerable components and promote alternatives that enable the recovery of damaged components. Thus, it is valuable to be able to simulate accurately the behavior of critical sub-networks under various attack scenarios, such that the recovery mechanisms may be designed properly and used confidently.

3.4.3 Prioritization

Recall that a critical mission for infrastructures, sectors, segments or sub-segments present at a domain of interest is defined by the decision makers. The subject matter experts assist the decision making processes at all levels (federal, state and local governments and private entities), with issues that reflect the interdependencies of infrastructures and in-depth knowledge of each infrastructure's behavior. The missions aimed to protect critical infrastructure and key

assets are usually formulated with reference from the states of normal functioning. The list of missions that pertain to infrastructure components over a domain of interest may be long and often common knowledge. In case of disruptions, caused by natural events, accidents or intentional acts of terrorism or sabotage, the concept of a mission of an infrastructures must be re-evaluated in the context of criticality. Certain components within a domain of interest may be neglected whereas certain functions must be maintained. A prioritization methodology is employed to identify the functions relevant to the missions to be sustained.

Establishing the key assets [5] to be protected and the critical mission aimed to mitigate an attack follows two main decision making routes: qualitative analysis and quantitative analysis. The qualitative analysis is quick (days/week time-scale), subjective but systematic, not subject to reviews and suffers from reduced accuracy. The qualitative analysis employs mostly fuzzy logic and theory of evidence. On the other hand, quantitative analysis is slower (months/years), objective and systematic, and subject to review. In general, the quantitative analysis displays high accuracy (probability theory is employed in studies) and depends on the fidelity of information. The quantitative analysis is based on a probabilistic approach [30, 31].

In selecting the type of analysis, the subject matter experts assist the decision makers with key values and features such as: provide objective criteria, fair comparisons and allow for sanity checks of the process mid-stream. The criteria should be: complete, definable, independent, discriminating [31, 20, 28].

Example 3.8. Suppose that during the harvesting of the crops in county X, one field is contaminated with a rapidly developing parasite fungus. The workers abandon the normal activity of collecting the healthy crops or seeding the freed fields, and concentrate their efforts for the immediate cleaning of the contaminated crop and field.

Suppose that a domain of interest has components across various critical infrastructures. The courses of actions aimed to sustain a critical mission reflect the prioritization tasks over that domain. The prioritization stems from an in-depth analysis of the infrastructures, vulnerabilities, possible types of disruptions and consequences of the loss of functionality.

The prioritization tasks and the soft metrics – see Section 5.5.2 – are intertwined. Prioritization influence the public perception of the magnitude of a disruption. And the way a disruption impacts the public dictates prioritization strategy. Recall Example 3.2 regarding the protection of nuclear plants. The consequences of a release of nuclear material into the atmosphere are amplified by the public perception and are propagated at international scales.

[5] See Section 3.5 on disruptions and the focus of an attack

3.4.4 The functions induced by the critical mission

A critical mission induces a *critical function* that is a collection of procedures, tasks, computing efforts and decisions that ensure the sustenance of the mission. The critical function encompasses the specifics of a domain of interest pertaining to the critical mission for critical infrastructures components that are part of that domain.

Further, from the critical function, all the technical details, economic factors, risk analysis and prioritizations, soft metrics, etc., are devised by subject matter experts and decision makers over regional and local level, as well as at the infrastructure segment, sub-segment detailing, in the context of interdependencies. The subject matter expert assist in the stage of modeling the behaviour of an infrastructure or that of the infrastrcuture components present at a domain of interest; their role diminishes after the modeling phase. The subject matter experts may assist further with aspects of the infrastructure behaviour that have not yet been modeled and are required during a disruption.

The critical function is in fact a collection of *required functions* to be devised for the infrastructure components within each domain of interest, for a selected critical mission. Figure 2 shows a selected critical mission and its induced critical and required functions.

The collection of required functions is not just a set of documents consisting of directives, it is also a complex process that monitors and governs at each step, the sustenance of the critical mission and scenarios to be developed under adverse conditions, during disruptions.

Example 3.9. Suppose that the domain of interest is the U.S. armed forces. A critical mission for the government leaders is "Provide continuous command and control of the U.S. armed forces". The critical function is now responsible for ensuring that all the necessary communication gear is available. The communication gear includes first the telecommunication infrastructure components and it may also include roads, airports, people. There are now in place required functions to be maintained by components of various infrastructures (telecommunications, transportation, government, energy) in order to sustain the critical mission of providing continuous control and command. The experts in communications deliver the details of their required functions – obviously their role in the critical mission is prominent. Also, subject matter experts from transportation and energy infrastructures devise the tasks of these infrastructure components that compose the corresponding required functions.

Example 3.10. Consider a nuclear plant that is built in the vicinity of a pharmaceutical plant. Both facilities are also close to a city. Assume that a critical mission[6] is formulated as "Protect

[6]See also Example 3.2. In this section, the critical mission is described in more detail - it is a first step toward the critical function.

nuclear plants against attempts by terrorists to shut them down and prevent leakages of nuclear materials". Each nuclear plant has its own protection plan, tailored to the specifics of the plant, location, etc. That particular domain of interest has obviously more required functions to accomplish than a domain with only one nuclear plant and no other private sectors present in the vicinity of the nuclear plant – such as the pharmaceutical plant. It is at the local level where the sustenance of the critical mission is translated into specific tasks (the required functions). There is a set of required functions to be successfully maintained in order to prevent unnecessary shut down of the nuclear plant – such as maintain the start-up/ shut-up electric power supplies within the range prescribed by regulations and also devise strategies to protect the plants against acts of sabotage and terrorism.

The number and characteristics of the required functions associated with a critical mission depend on the complexity of the domain of interest, and also on the analysis of the consequences of the loss of the mission.

The critical function and the required functions dictate the definition and interpretation of robustness of a domain of interest, for a given critical mission. Robustness is assimilated as the ability to maintain a critical mission; the required functions regulate continuously the reconfiguration/self-healing strategies aimed at the sustenance of the critical mission. The tools for modeling and simulating the behaviour of the infrastructure components across a domain of interest are intended to be planning tools to further address disruptions. The required functions comprise infrastructure interdependencies, and deploy the self-healing and reconfiguring mechanisms. An in-depth and up-to-date analysis of possible outcomes of a disruption and the mitigation strategies accompanies the reconfigurations. If repeated attacks occur, reconfigurations take place unless an *irreducible stage* of the infrastructure components is attained. The irreducible stage equates to the loss of the critical mission, the irreversible damage of a key asset or the failure of the critical infrastructure components.

The sequence of configurations of the infrastructure components that leads to the irreducible stage is not arbitrary and depends on the attack vector(s). Treating a complex attack as a sequence of simple ones is a process that requires prioritization of the missions to be accomplished – and it is only the decision makers who dictate the sequence and order of mitigations. Note that superposition and linearity attributes do not exist, hence complex attack scenarios are challenging in real situations as well in modeling exercises. An analysis of attack scenarios should consider exhaustively the possible sequences that might lead to the irreducible stage. Prioritization techniques are employed to sort the paths of attack scenarios and courses of actions. In other words, although attack scenarios with more than one attack vector are not interchangeable, prioritization techniques call for the analysis of most likely scenarios and may discard sequences of scenarios that decision makers consider equivalent

with respect to consequences and/or courses of actions of the defenders.

Figure 3 is an illustration of the process of establishing the required functions from the critical mission. Consider a domain of interest comprised of infrastructure components. An attack vector points to an infrastructure component. The attack vector highlits a collection of critical missions (Figure 3 shows only one critical mission highlighted). The enrichment of the formulation of the critical mission with pertinent details renders the critical function. Further, decision makers and subject matter experts at all levels (national, regional and local) gives the specifications required to protect the infrastructure present at that domain of interest and to sustain the critical mission. These are the required functions – they encompass models and analysis tools, simulations tasks, decisions, courses of actions, and any activity that is relevant to the critical mission. Econometric techniques and risk analysis are among the factors that govern the construction of the induced required functions. Risk factors include: likelihood of threat, consequences of the threat for the population, economy, ability to intercept and mitigate the threat. Analysis of capabilities include the following [20, 32]:

- probabilistic/possibilistic risk assessment
- logic evolved decision analysis
- human reliability analysis
- custom software development for risk assessment and security analysis
- prioritization of infrastructure components to protect
- identification of the target of an attack
- consequence analysis: public health and safety, diminishing of production capabilities and loss of the public confidence in the government and economy
- recovery and contingency planning, including time and cost
- effectiveness of protection and optimization of resource allocation
- analysis of adversary attributes to defeat the protection of a domain of interest.

The components of the analysis above are cast upon the main types of infrastructure interdependencies [38]. The possible damages of the physical components and the cyber ramifications of an attack as well as the global effects of local disruptions must be all addressed.

3.5 Disruptions

In defining the critical mission to protect infrastructures, sectors, segments or sub-segments, an in-depth analysis of the assets and services is usually performed beforehand. It is customary to create lists with ranked assets so that their protection is first subject to a prioritization analysis (see also Section 3.4.3).

From the adversary's viewpoint, each domain of interest – regarded as aggregates of infrastructure components – has a *focal point* whose attractiveness is greater than that of other components of the domain. For example, if the domain of interest is the electric power grid, the critical nodes constitute a possible target of an attack. Another example: for key assets, the Twin Towers were the focal point for the September 2001 attack, as they represented one of the major symbols of the country. The attractiveness[7] of these buildings was the highest on a large area, and over most of the key assets. Their destruction and the life loss had enormous consequences. The focal point is a concept used in analysis of conflicts in the game theory paradigm [33].

The focal point is more than a physical objective, target of an attack; and it is more than an indicator of the critical components of the infrastructures present within a domain of interest. The focal point or the focus of an attack comprises also non-directly quantifiable attributes, such as the international prestige of the country or the people's confidence in the government and private sectors.

There may be more than one focal point within a domain of interest, depending on the attack vectors and the critical missions that pertain to that domain. Recall Example 3.1: one focal point of an attack is a road hub. If the foot and mouth disease is used to induce road closure, then the focal point of an attack is the closest farm. Depending on the intelligence gathered, the roads are guarded or the farm is quarantined. There are attack scenarios where the loss of the focal point equates to the loss of the critical mission. An example is a nuclear plant. If the preponderant critical mission is to prevent any leakage of nuclear materials into the atmosphere then the focal point is the containment facility. Alternatively, if the preponderant critical mission is to maintain the nuclear plant running, then the focal point is the start-up/shut-down emergency power supply. Once a focal point is identified, specific tasks may be devised within an optimum resource allocation paradigm [21].

[7]The attractiveness measure is introduced in Section 5 as a composite of the success of an attack and its consequences.

4 Robustness

4.1 Introduction

The common understanding of the robustness of an infrastructure or a segment of an infrastructure is the ability to deliver services, maintain public safety within acceptable norms during a disruption inflicted by accidents, natural causes or intentional acts of terrorism or sabotage.

This section begins with a list of attributes of a complex system, followed by definitions and interpretations of robustness from various fields and complex systems. The aim is to develop results that may be applied to the study of robustness of the national infrastructures. A discussion of robustness of complex systems and approaches to describe robustness of critical infrastructures concludes.

4.2 Attributes of systems

Robustness is an attribute of systems – including complex ones – and measures the persistence of certain features under perturbations. The next paragraphs give descriptions of attributes of a system, often considered in the approach of defining robustness. This list is compiled mainly from [10, 26, 29].

Stability. A solution – or an equilibrium state – of a dynamical system is said to be stable if small perturbations to the system (input) parameters result in a new solution that is "not far" from the initial one. Stability, in essence, means: small perturbations in the input cause only small perturbations in the output. There is a wealth of mathematical theory on stability.

Resilience. A system is called resilient if it recovers quickly after a contingency occurs. This is a measure used mostly for network systems such as computer networks and the electric power grid.

Security. The ability of a network to operate under sudden or unexpected occurrences confers a system the quality of security [19]. Security opposes vulnerability.

Reliability is the time-dependent function that describe the delivery of services within prescribed ranges of satisfactory quality. The response of a network to naturally-occurring outages and the duration to fully restore services is described by reliability. The reliability of a network is also the sum of probabilities of acceptable states [10]. The North American Electric Reliability Council defines reliability in terms of adequacy and security. Adequacy is the ability of a network to deliver services under normal or expected sates of operation [19].

Vulnerability. The common understanding of the vulnerability of a network is the existence of a small number of components whose failure may cause extensive damage. Vulnerability is a measure of the severity of damage that can be caused by a disruption of a relatively small part of a system.

Criticality. A component of a network is critical if the failure of that component brings the network down or to a state of abnormal and unacceptable functioning. The notions of vulnerability and criticality are closely related; the difference is prominent in the case of scale-free networks [9].

Performance. This is an attribute that is defined as the percentage of the operating state of a network system; systems that operate at high performance have limited resources to respond to contingencies. Systems that have a high performance – in the sense specified here – are friable; they are in general neither reliable, resilient nor secure [10].

Recovery. This quality reflects the ability of a system to enable the state of normal functioning – or satisfactory functioning – after a contingency, without noticeable disruptions in service delivery. Recovery is an attribute of computer networks and Internet.

Connectivity. This attribute pertains to a topological characterization of a network, without taking into account the dynamics. Connectivity is understood as that of a graph and expresses also the configuration of the critical nodes. In practice this notion applies to energy networks, computer networks, the Internet, the road system and the airline industry [10].

Evolvability. Characteristic to adaptive systems, this property shows the degree of adaptability to changes in the exterior conditions. A typical example of evolvability are biological systems [16].

Flexibility A network system (such as an energy one) is flexible if it delivers services for a wide range of demand parameter values [10].

Survivability of a system is its ability to fulfill its critical mission under unusual operating states such as overload or security breaches.

Figure 4 shows the most common attributes of a complex system, all contributing to the robustness quality. Note that dependencies among these concepts are not introduced, because they depend on the type of system considered.

4.3 On robustness of complex systems

The aggregate of our national infrastructures form a heterogeneous complex adaptive system, where each infrastructure is a complex adaptive system on its own. The discussion in this section pertains to national infrastructures – viewed independently – and is intended to cre-

ate a comprehensive background on robustness that can be utilized to address the notion of robustness for the heterogeneous complex adaptive system of national infrastructures.

Robustness of complex systems has various definitions and interpretations, depending on the type of system. This section lists the most encountered approaches to define robustness of complex systems.

A measure of robustness is the extent of damages caused by disruptions that bring a system to a shut down or to a state of abnormal functioning. This is a definition that leaves little room for evaluating degrees of robustness; it is applicable, for example, to computer networks.

A more qualitative and quantitative approach is to regard robustness as a measure of feature persistence under certain sets of perturbations applied to the system. More specific, sets of features of interest are assigned to sets of possible perturbations. This approach is recently regarded as a "highly optimized tolerance". In this paradigm, a system is "robust, yet fragile". The meaning of this duality is that for certain perturbations there are features that persist – hence robustness – whereas some features are lost and are associated with significant degradation of system behaviour – and this is the fragile side of the system [16, 26]. The "fragile" part of a system is associated with rare events, design flaws and new and unanticipated perturbations. In the "robust yet fragile" context, robustness equates to the prevention of cascading failures. The mechanisms of highly optimized tolerance have been studied for forest ecosystems, Internet traffic and power systems.

For practical purposes, robustness of a system concerns the study of system behaviour under *prescribed* perturbations. There are features whose persistence is sought for a given set of perturbations and if this persistence is achieved, the system under scrutiny is considered robust [27]. The term "perturbations" comprises both fluctuations in the external inputs, internal system parameters as well as changes in the system internal structure, topology, and changes in the environment in which the system is initially designed to operate. This interpretation of robustness agrees with most attempts to describe robustness of a system [4, 39, 23, 48, 29].

An example of robustness definition for a specific type of systems – namely software development – follows: "Robustness is the ability of software to react appropriately to abnormal circumstances, i.e., circumstances outside the specifications, such as new platforms, network overloads, memory bank failures. Software may be correct without being robust." [26].

For biological systems, robustness characterizes the ability to self-repair, self-regulate, self-assemble and/or self-replicate.

A parallel analysis of the concepts of robustness and stability is presented in [27]. The robustness of a complex system is an attribute with more facets than that of stability. Robust-

ness analysis addresses multiple perturbations in a multi-dimensional setting. The robustness analysis is a complex one where fully developed mathematical tools do not exist – as opposed to stability studies of dynamical systems for which there is mathematical theory in place. Historically, in many applications, stability theory addresses consequences of perturbations that lack intentionality – using a probabilistic paradigm. The robustness of complex adaptive systems aims to handle disruptions from attackers familiar with the vulnerabilities of specific systems. The intentional attacks follow gathering information, expertise and resources that may ultimately cause significant damages to a system – or infrastructure. The analysis of robustness with respect to this type of elaborated attack involves a collection of challenging tasks, such as gathering intelligence, anticipate the adversary intentions, and a comprehensive study of the "attractiveness" of the domain of interest [21].

The descriptions of the attributes of a system are employed to express, quantify and monitor robustness via the extent of damages caused by disruptions, or the relative size of a damaged part of a system that translates into loss or degradation of desired features.

4.3.1 Interpretation of interdependent infrastructure robustness

This section proposes an interpretation of the robustness of interdependent infrastructures – or domains of interest that are collections of infrastructure components. The previous considerations on critical missions and general principles on the robustness of complex systems are the foundations of the robustness of a domain of interest.

Our essential national security missions, the delivery of essential public services are expressed in a set of critical missions to be accomplished to protect critical infrastructures and key assets. The formulation of the critical mission does not necessarily contain technical details.

The behavior of a domain of interest[8] may be classified as:

- normal
- abnormal but acceptable – within the limits imposed by the critical function and the required functions
- abnormal and unacceptable – the critical mission is no longer sustained and the domain of interest might be shut down because of loss of the critical components and/or irreversible damage of its focal point.

[8]In fact it is the behaviour of the infrastructure components present within the domain of interest that are under scrutiny with respect to robustness.

The state of operation varies from the optimal design to total loss of services, for all interdependent infrastructures. Although this is a wide range of states, robustness of a domain of interest is evaluated during abnormal operation modes, i.e., under attacks. Robustness is defined with respect to the critical missions, highlighted by the attack vector. There might be multiple attack vectors – in the absence of superposition and linearity properties, prioritization techniques are employed to address consequences and to devise courses of action (see Example 3.5). A domain of interest is robust if the critical mission over that domain are sustained. Equivalently, robustness may be viewed as the persistence of the features of interest described by the critical missions corresponding to – or highlighted by – an attack vector.

A first refinement of the critical mission is the critical function. Here the subject matter experts set a first threshold on the acceptable degradation of infrastructure components.

The critical function branches further into required functions; they refine the specifications, provide self-healing strategies, reconfigurations in the context of interdependencies of the infrastructure systems. The required functions are formulated at national, regional and local level. The required functions at the local level express the most detailed courses of actions, evaluation of risk and consequences and mitigation of contingencies.

Modeling and simulation tools, i.e., complex software applications, decisions, courses of actions give continuously measures of the state of a collection of infrastructure components present at a domain of interest. If the critical missions are sustained – within the thresholds defined by the critical functions – then the robustness of that domain is achieved.

5 Toward robustness metrics

Metrics that capture the interdependencies and describe the operating state of a collection of infrastructure components are yet to be developed. This section is focused mainly on showing the attributes of such desired metrics and challenges in the context of critical infrastructures. Some of the existing metrics are introduced.

5.1 Characteristics of robustness metrics for the interdependent infrastructures

The metrics that observe the operating state of the infrastructures components of a domain of interest must also capture economic, social and security considerations. The robustness of a domain of interest – regarded as a collection of infrastructure components – is the sustenance of the critical mission. The induced required functions are aggregates of tasks across

infrastructures and they capture other aspect of the activities and processes taking place at a domain of interest. Components of a domain such as the labor market, social and security considerations must be captured by the metrics that observe the normal operating state and the disrupted one. Recall that the analysis of vulnerabilities, threats and risks resulted from interdependencies must be subject to prioritization assessments.

The quantitative and qualitative measures can be used in two complementary tasks:

- first, to derive metrics as output from modeling tools (national and metropolitan consequence models) and
- further to
  - validate models and simulations through comparisons with real-world data and
  - create a history of the behavior of the domain of interest, for model refinements.

The metrics that can capture all the infrastructures interdependencies are aimed to assist decision makers, and to address risk management, liability and insurance concerns. The characteristics of such sought metrics are [38]:

- relevant to the effect they measure
- suitable for use in developing data sets
- suitable for use in running and validating models
- helpful in prioritizing threats and risks
- suitable for comparing and measuring alternative responses.

The proposed methodology in Section B can be employed to devise robustness metrics that meet all of the criteria listed above.

The representation of the infrastructure interdependencies is the major challenge in the derivation of robustness metrics – as it is in modeling infrastructures' behaviors [24]. Formal, mathematical expressions for interdependencies are the major difficulty. Hence during a first iteration, the metrics are more suited to be computer outputs derived heuristically, rather than evaluations of closed forms from theoretical studies. Note that there exist metrics that describe robustness of one infrastructure at a time. Such metrics accompany the robustness approaches introduced in Section 4.1. There is still the challenge to capture infrastructure interdependencies in a *realistic* manner. Closed form mathematical models that describe the

behaviour and evolution of complex systems cover only a limited area such as biological systems, the Internet or computer networks. The metropolitan models developed recently [12] contain examples of metrics that capture interdependencies of infrastructures. There are hundreds of metrics that capture every aspect of the behaviour of the infrastructures present at the metropolitan model. The next sections discuss factors to be considered when devising metrics for interdependent infrastructures.

5.2 The economic factor in the definition of a metric

The economic factor is a driving parameter in devising a metric to reflect operating states of an infrastructure from the robustness perspective. The cost and the extent of disruptions, as well as costs to protect an infrastructure sector, a facility or a key asset are determined by economic studies and models already in place. One can view the cost to repair the damages and the disruptions as the common denominator of any (attempt to derive) metrics that capture infrastructure interdependencies [21]. It is not the scope of this report to detail the economic factors. There exist economic models, at any level (national, regional, local) that address prediction of the economy and economic consequences of infrastructure components failures. The economy is the generator of our high standard of living and prosperity and therefore it plays a significant role in addressing robustness of national infrastructures, via the sensible unified measure of cost to repair the damages of a disruption.

5.3 The time-scale

The time scale enters as a parameter in modeling the behaviour of any infrastructure, sector or segment. In any model that captures infrastructure interdependencies, the time-scale should reflect its action upon each infrastructure. The models of interdependencies should have the capability to explicitly deal with time lags, and the flexibility to link databases, other models and diverse types of information [13, 28].

For example, a power outage of half hour of an irrigation pump of a corn field does not cause significant economic loss. However, that same half hour power outage might create significant economic losses if it induces loss of service of an e-commerce network or banks [28]. The electric power grid is subject to fast events in the order of milliseconds as well as slower events (construction of a new generator may take weeks). The time-scale dictates various strategies for mitigation of disruptions within the power grid [10, 44].

5.4 Risk analysis and the optimum allocation of resources

The subject matter experts decision makers act in a synergistic manner to:

- model the behavior of a domain of interest under a disruption
- prevent an attack and
- mitigate the consequences of an attack.

These goals aim to accomplish our essential missions and to protect the key assets of the country. The resources available are limited; however the threat scenarios are virtually unlimited. The study in [21] renders a methodology to assist decision makers to cope with the discrepancy between resources and attack scenarios. In essence this study establishes the "attractiveness" of a focal point and has the realistic inception of the impossibility to fully protect all infrastructures, and focal points at once. Attractiveness is a product between the likelihood of a success of an attack and its consequences. The success and consequences are inverse proportional to each other. The consequence reflect the defender's efforts to protect a focal point – hence the likelihood of success decreases if the consequences are big. The attractiveness metric is a component of soft metrics – see Section 5.5.2. The study in [21] renders a methodology to establish the optimum allocation of resources to protect facilities from a security standpoint as well from the perspective of random accidents using probability and possibility theory and the theory of evidence. This allocation strategy has impacts over the modeling tools and is detailed at the implementation level. This study may be employed in addressing the consequences of a disruption and the likelihood of escalating or cascading effects resulted from repeated attacks on a focal point of a domain of interest and neighboring domains.

Previous studies propose a more classical, probabilistic framework to devise risk and feasibility of an attack. For example, the proposed methods for feasibility calculations in [22] are simple and suited for fast implementations of large scale problems. The authors rank risk and consequences in a few representative classes: low, high, medium. This approach renders fast real-time solutions.

The allocation of resources for the protection of national infrastructures and for the assessment of the attractiveness of a focal point within a domain of interest must address the security of the cyber and telecommunications networks. In the proposed methodology in Appendix B it is assumed that there exist strategies in place to address cyber threats.

5.5 Examples of metrics

This section introduces some metrics that are already used for various infrastructures. Their merits and applicability are also shown.

For networks that have flows through their edges, the robustness and associated metrics are addressed from the graph and network theory [10, 29]. Robustness of a network may also be defined by the level of connectivity of the associated graph, hence connectivity metrics are proposed. These metrics are used in the technical community. The metrics that address reliability are temporal metrics. There are also differential metrics that monitor the flow on a network. The applicability in practice of these metrics for assessing the robustness of interdependent infrastructures is associated with a threshold defined by the critical function.

Consider the Example 3.7. A critical mission is formulated for the public health infrastructure. Suppose that there exists a bio-weapon threat with a known germ. A critical mission might be formulated as: "treat and cure the infected people". However, scientific results lead to a critical function that reflects the fact that for this biological agent the survival rate is 80%. Recall that the critical function refines first the statement of the critical mission – Section 3.4.4. A realistic metric to show the robustness of the public health infrastructure looks then at percentages of people cured that are around 80. The threshold value of 80% is the robustness indicator. Without this realistic expectation taken in account, any loss of life might indicate lack of robustness. Note also that crisp thresholds are difficult to cope with. A re-evaluation of the threshold may give: "around" 80%. The thresholds are in general fuzzy and subject to adjustments on a case by case basis.

Common metrics that address a disruption fall into three main categories [22]:

- injuries and fatalities
- monetary loss; loss of productivity
- extent of impact: morale of the population, consumer confidence.

Other metrics reflect the dimensionality of the goods or services or value of assets within an infrastructure. In [15] the authors present a study of quantitative metrics (kg, casualties, cubic feet) to overcome the fluctuations in prices and avoid as a general metric the cost in dollars. Consumption of goods is also a good metric for the pulse of the economy. These metrics are well suited for gathering the history of events and quantifying the extents of impacts caused by disruptions.

If monetary loss is chosen as a universal metric, the extent of damage should be characterized based on the relative value of the loss, such as percentage of production lost. For

example, $100 billion loss to the financial sector will cause less relative damage than the same loss in the agriculture sector.

The following sub-sections treat the two distinct types of metrics: quantifiable and non-quantifiable ones. A metric that reflects interdependencies should capture both aspects. This requirement is defended at the end of the section.

5.5.1 Hard metrics

Despite the challenges of price fluctuations, the cost to restore/repair the damage caused by disruptions is a convenient and relevant metric [20]. This cost to repair can be used as a uniform criterion for reconfiguration of a domain of interest.

Example 5.1. Suppose that a major hub from the road network is shut and trucks with dairy products must take alternate detours. A cost evaluation of the detours dictates which is the optimum alternative. Note that only the length of the alternate routes is not sufficient. The speed limit must be taken in account. The length of the route and speed limits are essential factors used to evaluate the cost of alternate transportation and to choose an optimum alternative.

Example 5.2. Aside from the presence of a critical mission, planning tools must be used for economics analysis. Here is an example of a formula for the electricity demand and its cost, hence a metric. The expression implemented is

$$q = a + \frac{b}{p} + \frac{c}{p^2}$$

where q is the quantity demanded for consumption, p is the price, a is a function of location and activities and b and c are functions of demographics. Fluctuations in the consumption of electricity impact the price. This metric is used to model interdependencies between the energy infrastructure and the market and finance one.

Robustness may be expressed in terms of costs (hard metric) – evaluated for the possible mitigation alternatives that are within the limits imposed by the critical function. The hard metrics are reliable and they may be confidently used as a first indicator of robustness.

5.5.2 Soft metrics

However, are the hard metrics sufficient to give a realistic insight of the extent of a disruption? Non-quantifiable metrics play a significant role in assessing the extent of an impact. Formally, these metrics address, among other concerns, the "open texture of language" [34] that reflects

the individual's perception of the outcomes of a disruption. Undoubtedly, what a New York City person perceives from the World Trade Center attack is different from what an elderly person living in a small farm in a remote area perceives.

These not directly observable metrics – called *soft metrics* – usually do not have *immediate* associated costs (dollars) or quantities of goods or services. The soft metrics may have derived costs associated – and these costs are established from the consequences of a disruption or in the aftermath of an attack. For example, assuming rational behaviour of the decision makers, the cost of the September 11 terrorist attack may be related to the extra amount spent for increased security, reconstruction, aid for the airline industry, prevention of further attacks. Such possible non-quantifiable metrics are: confidence of the people in the government, consumer confidence, international prestige of the country. Another class of soft metric is the extent of disruption. For example, the death of the mayor of a small village impacts the public less than the assassination of the president [22].

In conclusion, if only hard metrics are considered, the critical function and the threshold induced may be insufficient, because the immediate and obvious costs – reflected in hard metrics – must be augmented with costs dictated by the consequences of soft metric variations.

The extents of damages described by soft metrics – such as "nuisance, mild, severe, catastrophic" – are difficult to quantify, although they are important in the decision making process. The example above regarding the aftermath of September 11 attack is reconsidered in the specific context of the airline industry. After the attack, the government provided financial aid to the airlines. The soft metric that describe the loss of confidence and fear to fly is reflected in severe financial losses to the air lines. The government aid ultimately lessened the impact of soft metrics on the economic outcomes.

The robustness of the financial system was also tested in the aftermath of the World Trade Center attack. One aspect of robustness is related to soft metrics. The Feds told people that cash would be available and checks would be honored. As a result of this reassuring news, there were no withdrawal of excessively large amounts [37].

The soft metrics influence the hard metrics. One example is the availability on the market of the drug Cipro during the anthrax mail scare. People managed to buy and stock this antibiotic "just in case" and patients in need did not have access to the drug (there are certain diseases that are treated mainly with Cipro). The soft metrics that indicates panic influenced the public health infrastructure by reducing the availability of a drug used frequently in diseases other than anthrax infections.

The study of soft metrics is open. These metrics are a significant component of a proper metric that observes infrastructure interdependencies and robustness. Following the study on

optimum allocation of resources from the risk analysis perspective (Section 5.4), this report asserts that the most significant component of a soft metric is the "attractiveness" of a domain of interest. The attractiveness captures a plethora of consequences that are not immediately quantifiable in dollars. For example, the attractiveness of the Twin Towers was the largest among all sky-scrapers because they were a major symbol of the country. Other metrics such as consumer confidence may be used – however these metrics are outcomes of probabilistic studies. Soft metrics that reflect the outcomes of an intentional attack must be based on possibility theory and the theory of evidence.

5.5.3 Connectivity metrics.

These metrics deserve a special attention as they are the most used indicators of robustness of a network system. The connectivity metrics show the degree of loss of nodes, with emphasis on monitoring the critical nodes. A typical example is the road network. The loss of a major hub degrades the transportation sector significantly. These metrics capture also the topological aspect of a network infrastructure. Degrees of robustness may be derived from the number of nodes lost before the network looses its critical mission. The higher the number of nodes lost to failure, the more robust the network is. However, with transportation or aviation networks, this characterization is not immediately applicable, since the hubs are not equivalent to any other node. A weighting procedure is usually employed.

The calculations of the connectivity metrics are computationally very expensive. In the context of interdependent infrastructures, a complication arises from either modeling the infrastructure as a 14-dimensional network or as a one-dimensional network, due to the various degrees of connectivity of infrastructures and the practical challenges derived from the sizes of flow networks – such as the electric power grid.

The connectivity metric may be used to analyze robustness component-wise, i.e., one infrastructure at a time. For computer networks and the Internet, the connectivity metrics are widely used.

6 Mathematics/closed forms for metrics

In the modern era of powerful computers, it is mandatory to express the robustness metrics – and any metric in general – in a closed, compact, mathematical expression or an expression that can be easily converted into a digital input. In [5] the author asks: "What set of theories can capture a mix of dynamics, interactive and often non-linear entities with unscheduled discontinuities?". Developing mathematical expressions for the robustness metrics is an on-

going challenge and it is an interactive task. A mathematical expression for interdependencies and metrics associated with robustness across infrastructures must be tuned with simulation outputs to have the high fidelity expected in modeling infrastructures as complex adaptive systems. There are ongoing research activities in the theory and modeling of infrastructure dependencies and metrics associated with the states of domains of interest.

A metric to monitor robustness should be derived via a tool able to analyze the outputs of infrastructures states and compare them. The main challenge is that there is not yet a universally accepted dimension for quantifying the outputs. The cost to repair the damage (loss of productivity, less consumption of goods, physical restoration, etc.) might be considered. There are interdependent physical metrics that are mathematically derived for flow network infrastructures – such as the electric power grid and the natural gas sector. Economic metrics may be derived from the economic prediction models.

Considerations on metric development are revisited in Section B. That is because the implementation of a methodology to create metrics dictates first flexibility, among other practical criteria.

This section highlights the principles toward a mathematical theory and attempts to present a metric supported by theory.

In order to develop a mathematical theory *seven basic* [46] concerns should be addressed:

- properties
    1. aggregation
    2. nonlinearity
    3. flows
    4. diversity
- three mechanisms
    1. tagging
    2. internal models
    3. building blocks.

From the previous discussions, a metric for infrastructure robustness is based upon two components, a soft metric and a hard metric, $\{\boldsymbol{S}, \boldsymbol{H}\}$ respectively. Each of the components, $\boldsymbol{H}$, and $\boldsymbol{S}$ may be multi-dimensional. The soft metric is considered the attractiveness of a focal point.

The hard metrics may be any collection of the metrics used in economic analyses, such as dollars, watts, productivity, etc. The Critical Infrastructure Protection/Decision Support System (CIP/DSS) project provides a collection of hundreds of such metrics. A robustness analysis must employ a metric that is an aggregate of all relevant such hard metrics and also accounts for the mutual influence of the hard and soft metrics. The link and a mathematical relation between the two components – hard and soft – depend on the critical mission that in turns shapes the robustness criteria. Moreover, the preferences – from the prioritization strategies – of the decision makers must be captured by robustness metrics.

The next discussion focuses on the derivation of a robustness metric. Suppose an attack takes place. The states of the infrastructures before an attack or a sequence of attacks are known, as well as the states after the attack occurs (from the modeling and simulation tools and/or real-time runs). The "Output" in Figure 8 is a state of infrastructures after an initial attack occurs; there may be more than one output, for different times the domain is scrutinized. Moreover, given the adaptive nature of a domain, there might be various outputs considered during a disruption, before the consequences of an attack are fully mitigated. The outcomes of an attack are denoted by $\mathcal{O}_1, \mathcal{O}_2, \ldots$. Each outcome correspond to a sequence of courses of action; the order in which courses of action occur reflects prioritization and there is no superposition. The outcomes form a set Ω of states of the infrastructure components after a disruption initiates. Each outcome in Ω is a 14-tuple that describes the states of infrastructures present at the disrupted domain of interest. Inside the "black box" there are provisions for various courses of actions, such as alternative routes in case a road block or access to different banks during the closure of a branch of a certain bank in a small city.

The input to the black box is a collection of 14 states of infrastructures – in fact collections of components present within the domain under scrutiny/attack. The outputs are also collections of components from the 14 infrastructures - however not necessarily the same components that are part of the Input. One component may be lost during an attack and others may be employed – example: a bridge being closed and additional bridges and roads being used as alternate routes – recall Figure 1 for an abstract representation of reconfigurations. Across each of these components, a comparison between the input and output shows the extent of the damage, cost for lost components and cost for employing new ones and a total cost to mitigate the disruption. These costs can be regarded as a 14-dimensional tuple. For simplification, at this stage, the discussion is kept at the infrastructure level, without detailing on sectors, segments, or sub-segments.

The next discussions considers only two infrastructures to be significant at a domain of interest. A metric across infrastructure must reflect behaviours like:

- Outcome $\mathcal{O}_1$ may be characterized by costs to restore of \$20k on infrastructure 1 and

$5K on infrastructure 2.

- Outcome $\mathcal{O}_2$ may be characterized by costs of $15K on both infrastructures and
- Outcome 3 by costs of $25K on infrastructure 1 and $1K on infrastructure 2.

Which outcome is preferable? How does one choose a metric based on these types of outcomes?

Robustness may be defined from investigating the extrema of these values or the sum for both infrastructures, for all possible outcomes. If the values are smaller than a threshold – established by the subject matter experts and the decision makers – then the domain of interest is robust for a given attack.

Assume that there is only one attack vector. Subsequent attacks are treated similarly; the outcomes of the first attack are inputs for subsequent attacks. Robustness – with respect to the critical mission – is observed over all 14 components of the outcome vectors. One way to devise a hard metric would be to sum up all the costs. Another employable norm associated with a hard metric is the highest cost among all 14 infrastructures.

Here it is how these considerations translate in order to determine a robustness metric. First, evaluate – at each infrastructure level present within a domain of interest – the outcomes of a disruption. These outcomes may be of any meaningful type: dollars, physical units (Watts, cubic feet), relative connectivity, etc. The individual outcomes are calculated from models that account for interdependencies. Denote a vector outcome by $\boldsymbol{o}$. A vector outcome has components of the hard metric, relevant for each infrastructure, such as: costs, fatalities, Watts. The set of outcomes Ω are full descriptions of the states of infrastructure. The vector outcomes $\boldsymbol{o}$ are also elements of Ω, where the full descriptions of the states of infrastructures are replaced by the associated relevant values (dollars, Watts, fatalities).

Secondly, map the vectors $\boldsymbol{o}$ of Ω into the set of real non-negative numbers $\mathbb{R}_+$. The mapped values are non-dimensional. This mapping is realized via a non-linear transfer function. The transfer function reflects:

- infrastructure interdependencies – in the components of the vector $\boldsymbol{o}$
- prioritization and preferences of the decision makers – by exploiting the information in the corresponding descriptions of infrastructures states in $\mathcal{O}$
- hard metrics – embedded in $\boldsymbol{o}$
- soft metrics – derived from both $\mathcal{O}$ and $\boldsymbol{o}$.

This translates mathematically as

$$m = \boldsymbol{T}_{dm}\,(\boldsymbol{o}) \tag{1}$$

where $\boldsymbol{T}_{dm}$ is a transfer function whose expression is derived for the relevant decision makers – hence the subscript dm. The transfer function is tailored for an attack scenario that highlights one or more critical missions. The decision makers are from all levels of decision making: national, regional and local and from various geographical locations. This compact representation allows treatment/analysis of robustness over arbitrary collections of infrastructure and infrastructure components. The decision makers at the Office of Homeland Security have a broad picture of the robustness of an infrastructure – see Example B.1. Whilst robustness at the national level may be achieved, at the local level an attack may have disastrous consequences. An example is given to show the difference between the robustness concerns of two decision makers from different levels of decision making.

Example 6.1. Consider that the main infrastructure under scrutiny is the Public Health. The attack scenario involves a biological weapon. The critical mission of the Public health sector is to prevent the spreading of an epidemic. Recall Example 3.7. At the Office for Homeland Security, the transfer function $\boldsymbol{T}_{OHS}$ reflects the critical mission of the Public Health sector to limit the consequences of biological attacks, i.e., prevent an epidemics, contain the affected people within a small area, possibly quarantining the entire city. For the decision makers – e.g., the mayor – at the city where the attack takes place, the transfer function $\boldsymbol{T}_{mayor}$ comprises courses of actions that respond immediately to the interests of the city, possibly quarantining only selected neighborhoods. The approaches of the trasnfer functions $\boldsymbol{T}_{OHS}$ and $\boldsymbol{T}_{mayor}$ of decision makers at different decison making levels may reflect more often catastrophic effects of the attack at the local level, hence loss of robustness over small domains of onterest. However at the highest decision making level, robustness may still be acheived. In this example robustness from the $\boldsymbol{T}_{OHS}$ transfer function translates into a contained spread of the epidemics and possibly very small effects of the attack at the national level.

The transfer function $\boldsymbol{T}_{dm}$ take various expression and has various levels of complexity in its formulation, depending on the level and the location of the relevant decision makers. For example, an attack may target only one state, hence for the same critical mission, the transfer functions $\boldsymbol{T}_{dm}$ of the decision makers form states other that the threatened one may have fairly simple forms.

The output m of the transfer function is the analogue of the prizes in game theory [33]. A prize carries a complete specification of all aspects that concern the decision maker – in this case implemented in $\boldsymbol{T}_{dm}$. A preference ordering may be assessed to prizes – corresponding

to the values of m. Note that the metric m may be the proper norm of an abstract vector in a linear space as well. The specification of the metric in terms of a transfer function gives flexibility with respect to mathematical expressions and manipulations, as well as with respect to computational realizations of the metrics.

The metric rendered by the transfer function is a scalar – however the compact representation in Equation 1 accommodates dimensional values (hard metrics) as well as soft metrics, via the transfer function $\boldsymbol{T}_{dm}$. The thresholds from the critical functions are embedded into T_{dm}. Fuzzy thresholds may also be used [36].

This approach overcomes the major challenge of the lack of a mathematical order relation between the real outcomes/courses of action in $\boldsymbol{\Omega}$, for multiple decision makers. Had one been employable, there could be correspondence between the real outcome and an abstract space, and sophisticated analysis tools such as optimality analysis, convergence, interpolation, approximation would have been employable.

The next discussion is concerned with an approach to define criteria for robustness, given the abstract metric m on $\mathbb{R}_+$.

Denote by $\mathcal{D}$ a collection of relevant decision makers with respect to the critical missions that are highlighted by an attack vector.

$$\mathcal{D} = \{dm \mid dm \text{ is a relevant decision maker}\} \tag{2}$$

The set $\mathcal{D}$ contains decision makers from various decision making levels and within the same level, from various locations. Denote by $\mathcal{T}$ the set of all transfer functions that address an attack at all relevant decision making levels and locations:

$$\mathcal{T} = \{T_{dm} \mid dm \in \mathcal{D}\} \tag{3}$$

The output of each transfer function, for any outcome $\boldsymbol{o}$ is denoted by m_{dm} and:

$$m_{dm} = \boldsymbol{T}_{dm}(\boldsymbol{o}),\ m_{dm} \geq 0, \text{ for all } \boldsymbol{o} \in \boldsymbol{\Omega},\ \boldsymbol{T}_{dm} \in \mathcal{T} \tag{4}$$

The robustness for each decision maker is ensured by strictly positive values of m_{dm}. A value of zero equates to loss of robustness. Values outside the thresholds imposed by the critical functions also translates into null values for the robustness metric m_{dm}. The optimum course of action – or the optimum outcome – is given by:

$$M = \max_{\boldsymbol{o} \in \boldsymbol{\Omega}} \boldsymbol{T}_{dm}(\boldsymbol{o}) = \max_{\boldsymbol{o} \in \boldsymbol{\Omega}} \{m_{dm} | m_{dm} = T_{dm}(\boldsymbol{o})\} \tag{5}$$

Outcomes may be assigned various degrees of robustness, for the same decision maker. Robustness across different levels of decision making may be discussed via the ordering of the

decision makers. For example, Level 1 may be assigned to the President and Level 2 may be assigned to state governors. A *vector of robustness metrics* is defined such that each component corresponds to a decision maker.

Example 6.2. Consider two decision makers, of levels 1 and 2, dm_1 and dm_2, respectively. Suppose there is an attack vector for which the transfer functions $\boldsymbol{T}_{dm_1}$ and $\boldsymbol{T}_{dm_2}$ are defined. The vector of robustness metrics can be represented in a plane with the values corresponding to each decision making level on one axis – as in Figure 6. The robustness for decision maker of level one is represented on the horizontal axis, dm_1 and level 2 decision maker on the vertical axis, dm_2. Suppose that two outcomes $\boldsymbol{o}$ and $\boldsymbol{\omega}$ give the metrics m and μ, respectively and the values of the metrics, for the decision makers dm_1 and dm_2 are:

$$m_{dm_1} = \boldsymbol{T}_{dm_1}(\boldsymbol{o}) = 2, \qquad \mu_{dm_1} = \boldsymbol{T}_{dm_1}(\boldsymbol{\omega}) = 7$$
$$m_{dm_2} = \boldsymbol{T}_{dm_2}(\boldsymbol{o}) = 5, \qquad \mu_{dm_2} = \boldsymbol{T}_{dm_2}(\boldsymbol{\omega}) = 1$$

The outcome corresponding to $\boldsymbol{\omega}$ is preferable – given the ordering of the decision makers that gives higher priority to decision maker at level 1. Moreover, an outcome characterized by a metrics vector $(8, 0)$ is preferable to the outcome $\boldsymbol{\omega}$ that gives the vector $(7, 1)$. A value of zero corresponds to a loss of robustness at decision making level 2 – however this outcome is preferable to the decision maker at level 1 – see also Example B.1. Further, the vector of robustness metrics for these two decsion makers may lie in convex areas in the plane (dm_1, dm_2). Figure 7 shows three possible areas delimitated by the curves $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_3$, for maximum (hence optimum) values of each robustnes metric Max_1 and Max_2 corresponing to decsion makers at level 1 and 2, respectively[9]. Note that these maximum values may be interpreted as normalized values where $Max_1 = Max_2 = 1$.

The derivation of the robustness metric via the transfer function provides the decision makers an output of an utility function and enables a fast decision based on a relation of preference [33]. The challenge of devising the transfer function at decision making level is handled by the relevant decision makers –possibly at all levels of decision making – as well as support. The subject matter experts provides models of the infrastructures, sectors, etc. and also the computational and software implementation of the transfer function.

7 Mathematics/closed forms for metrics -2

In the modern era of powerful computers, it is mandatory to express the robustness metrics – and any metric in general – in a closed, compact, mathematical expression or an expression

[9]More rigurous mathematical interpretation may be found in [17].

that can be easily converted into a digital input. In [5] the author asks: "What set of theories can capture a mix of dynamics, interactive and often non-linear entities with unscheduled discontinuities?". Mathematical expressions for the robustness metrics is an ongoing challenge and it is an interactive task. A mathematical expression for interdependencies and metrics associated with robustness across infrastructures must be tuned with simulation outputs to have the high fidelity expected in modeling infrastructures as complex adaptive systems. There are ongoing research activities in the theory and modeling of infrastructure dependencies and metrics associated with the states of domains of interest.

Considerations on metric development are revisited in Section B. That is because the implementation of a methodology to create metrics dictates flexibility, among other practical criteria.

This section highlights the principles toward a mathematical theory and attempts to present a metric supported by theory.

In order to develop a mathematical theory *seven basic* [46] concerns should be addressed:

- properties
    1. aggregation
    2. nonlinearity
    3. flows
    4. diversity
- three mechanisms
    1. tagging
    2. internal models
    3. building blocks.

From the previous discussions, a metric for infrastructure robustness has two components, hard and soft. Denote the metric by $\boldsymbol{M}$:

$$\boldsymbol{M} = (\boldsymbol{H}, \boldsymbol{S})$$

where $\boldsymbol{H}$, $\boldsymbol{S}$ stand from Hard and Soft, respectively. Each of the components, $\boldsymbol{H}$, and $\boldsymbol{S}$ are multi-dimensional – at least in this incipient stage of the development of metrics. A dimension of 14 for the hard metrics is considered; it accommodates the presence of the fourteen infrastructures at a location and is a uniform approach. The soft metric is considered

the attractiveness of a focal point. The link and a mathematical relation between the two components – hard and soft depend on the critical mission that in turns shapes the robustness criteria.

The next discussion focuses on the hard metric $\boldsymbol{H}$ and the types of norms that may be used. Suppose an attack takes place. The states of the infrastructures before an attack or a sequence of attacks are known, as well as the states after the attack occurs (from the modeling and simulation tools and/or real-time runs). The "Output" in Figure 8 is a state of infrastructures after an initial attack occurs; there may be more than one output, for different times the domain is scrutinized. Moreover, given the adaptive nature of a domain, there might be various outputs considered during a disruption, before the consequences of an attack are fully mitigated. The set of outcomes of an attack are denoted by $\mathcal{O}_1, \mathcal{O}_2, ...$ and they form a set $\mathcal{O}$ of states of the infrastructure components after a disruption initiates. Each outcome in $\mathcal{O}$ is a 14-tuple that describes the states of infrastructures present at the disrupted domain of interest. Inside the "black box" there are provisions for various courses of actions, such as alternative routes in case a road block or access to different banks during the closure of a branch of a certain bank in a small city.

A metric to monitor robustness should be derived via a tool able to analyze the outputs of infrastructures states and compare them. The main challenge is that there is not yet a universally accepted dimension for quantifying the outputs. The cost to repair the damage (loss of productivity, less consumption of goods, physical restoration, etc.) might be considered. There are interdependent physical metrics that are mathematically derived for flow network infrastructures – such as the electric power grid and the natural gas sector. Economic metrics may be derived from the economic prediction models.

The input to the black box is a collection of 14 states of infrastructures – in fact collections of components present within the domain under scrutiny/attack. The outputs are also collections of components from the 14 infrastructures - however not necessarily the same components that are part of the Input. One component may be lost during an attack and others may be employed – example: a bridge being closed and additional bridges and roads being used as alternate routes – recall Figure 1 for an abstract representation of reconfigurations. Across each of these components, a comparison between the input and output shows the extent of the damage, cost for lost components and cost for employing new ones and a total cost to mitigate the disruption. These costs can be regarded as a 14-dimensional tuple. For simplification, at this stage, the discussion is kept at the infrastructure level, without detailing on sectors, segments, or sub-segments.

The next step is to compare various outcomes, to decide which alternative is preferable and to evaluate robustness. The notion of "distance" between outcomes would be a perfect

instrument. The challenge here is how to map the outcomes into a vector space where triangle inequality holds. In other words, how should one interpret

$$Dist(\mathcal{O}_1, \mathcal{O}_2) + Dist(\mathcal{O}_2, \mathcal{O}_3) \geq Dist(\mathcal{O}_1, \mathcal{O}_3)$$

It is obvious for roads (length) and for Internet traffic – and not so obvious for other infrastructures. Also, the time enters – by default – as a label of these outcomes and as a dictating parameter. The order of outcomes is a result of prioritization, and not that of superposition.

The next discussions considers only two infrastructures to be significant at a domain of interest. A metric across infrastructure must reflect behaviours like:

- Outcome $\mathcal{O}_1$ may be characterized by a cost of \$20k on infrastructure 1 and a cost of \$5K on infrastructure 2.
- Outcome $\mathcal{O}_2$ may be characterized by \$15K on both infrastructures and
- Outcome 3 by \$25K on infrastructure 1 and \$1K on infrastructure 2.

Which outcome is preferable? How does one choose a metric based on these types of outcomes?

Robustness may be defined from investigating the extrema of these values or the sum for both infrastructures, for all possible outcomes. If the values are smaller than a threshold – established by the subject matter experts and the decision makers – then the domain of interest is robust for a given attack.

Assume that there is only one attack vector. Subsequent attacks are treated similarly; the outcomes of the first attack are inputs for subsequent attacks. Robustness – with respect to the critical mission – is observed over all 14 components of the outcome vectors. One way to devise a metric would be to use the taxicab norm in the 14-dimensional space of dollar outcomes, i.e. sum up all the costs. Another good norm is the infinity norm that shows the highest cost among all 14 infrastructures. These norms are equivalent and they are also equivalent to any of the L_p norms, provided all the components of outcomes are expressed in dollars and the triangle inequality holds. Note the flexibility in analysis when equivalent norms are employed : one can analyze attack scenarios that target only a few infrastructures from all fourteen possibly present at a domain of interest.

Note. In a finite dimensional normed linear space $\boldsymbol{X}$ all norms – and metrics derived from norms – are equivalent [17] in the sense that if $\mathcal{N}_1$ and $\mathcal{N}_2$ are two norms then there exists two positive constants α and β such that

$$\alpha\mathcal{N}_1(\boldsymbol{x}) \leq \mathcal{N}_2(\boldsymbol{x}) \leq \beta\mathcal{N}_1(\boldsymbol{x}),\ \forall \boldsymbol{x} \in \boldsymbol{X}$$

Here it is how these considerations translate mathematically.

1. Evaluate – at each infrastructure level present within a domain of interest – the outcomes of a disruption. These outcomes may be of any meaningful type: dollars, physical units (Watts, cubic feet), relative connectivity. The individual outcomes are calculated from models that account for interdependencies. Denote a vector outcome by $\boldsymbol{o}$. A vector outcome has components of the hard metric, relevant for each infrastructure, such as: costs, fatalities, Watts. The set of outcomes $\mathcal{O}$ are full descriptions of the states of infrastructure. The vector outcomes $\boldsymbol{o}$ are also elements of $\mathcal{O}$, where the full descriptions of the states of infrastructures are replaced by the associated relevant values (dollars, Watts, fatalities).

2. Map the vectors $\boldsymbol{o}$ of $\mathcal{O}$ into a 14-dimensional linear space $\boldsymbol{X}$ (could be simply $\mathbb{R}^{14}$) such that for each infrastructure the outcome reflects now the relative difference between the Input and the Output. Each component is non-dimensional in the sense that it is not expressed in dollars, Watts, etc. Mathematically, the hard outcome $\boldsymbol{o}$ is transformed into a vector $\boldsymbol{x}$ via a relation of the type::

$$\boldsymbol{x} = \boldsymbol{T}_{cm}\, \boldsymbol{o}$$

   where $\boldsymbol{T}_{cm}$ is a transfer matrix function whose expression is derived from the critical mission – hence the subscript cm.

3. Derive a metric using norms in this 14-dimensional space. The metric for this space $\boldsymbol{X}$ is also dictated by the critical mission and it is denoted by $\|\cdot\|_{cm}$.

Consider Example 3.5. When the attack vector is the one that points to the government infrastructure, the $\|\cdot\|_{cm}$ metric might be a Boolean one, for the absence of nuclear pollutants leaked into the atmosphere. When the attack vector is the one that points to the public health infrastructure, with the critical mission "Protect the scientists", the $\|\cdot\|_{cm}$ metric may be chosen just as the percentage of people rescued. Both these metrics may be viewed as L_1 metrics (summation of components) where all the components that represent irrelevant infrastructures are zeros. Here "irrelevant infrastructures" are those that are not contributing to the outcomes of the disruption - for simplification all but the public health component are zero. Note that there is no obvious morphism[10] from the space of outcomes $\mathcal{O}$ to the space $\boldsymbol{X}$. **Kevin: morphism means that there is a structure on $\mathcal{O}$ - there exists a function, but not a morphism - I can get rid of this notion, though if you think it makes the discussion**

[10]A morphism preserves the structure of the spaces mapped onto one another [17].

to mathematical. This restriction limits considerably the mathematical manipulation of the metrics.

In the hypothesis of norm equivalence on $\boldsymbol{X}$ one can consider any norm for theoretical manipulation – in practice, again, it is the critical mission that dictates which norm to be employed.

The thresholds from the critical function may also be mapped. Fuzzy thresholds are also accommodated [36] using fuzzy topologies to define $\boldsymbol{X}$. A robustness metric may be devised in terms of a radius of robustness: abstract representations $\boldsymbol{x}$ of outcomes that stay within the bounds imposed by the thresholds are compared and the one that gives an extreme value (min or max) is selected as the corresponding to the optimum course of action.

The major challenge is the lack of a mathematical order relation between the real outcomes/courses of action. Had one been employable, the correspondence between the abstract space and the real outcomes would have been subject to sophisticated analysis such as optimality analysis, convergence, interpolation, approximation, etc.

The next discussion is concerned with an approach to define criteria for robustness, given the abstract metrics on the space $\boldsymbol{X}$.

Denote the domain of interest by $\mathcal{D}$ and the set of critical missions that are relevant to $\mathcal{D}$ by $\mathcal{C}$; that is:

$$\mathcal{C} = \{cm \mid cm \text{ is a critical mission over } \mathcal{D}\} \tag{6}$$

For each critical mission, a specific metric is defined over $\boldsymbol{X}$, denoted by $\|\cdot\|_{cm}$. The critical function and the required functions on $\mathcal{D}$ impose a threshold on the metric, denoted by M_{cm}. Robustness imposes that the norm on the metric is less than M_{cm}:

$$\|\boldsymbol{x}\|_{cm} < M_{cm}, \qquad \text{for all } \boldsymbol{o} \in \mathcal{O},\ \boldsymbol{x} = \boldsymbol{T}_{cm}\boldsymbol{o},\ cm \in \mathcal{C} \tag{7}$$

where $\boldsymbol{T}_{cm}$ is the transfer matrix corresponding to each critical mission cm in the set $\mathcal{C}$ of critical missions.

For the possible outcomes of one attack vector – hence one critical mission – a *robustness radius* [3] may be defined:

$$R_{cm} = \max_{\boldsymbol{o}\in\mathcal{O}}\{\|\boldsymbol{T}_{cm}\boldsymbol{o}\|_{cm}, \text{ such that} \|\boldsymbol{T}_{cm}\boldsymbol{o}\|_{cm} < M_{cm}\} \tag{8}$$

This robustness radius determines a ball centered at zero in the space $\boldsymbol{X}$ – zero corresponds to the state of the infrastructure components of the domain $\mathcal{D}$ before a disruption commences. All the outcomes $\boldsymbol{o}$ corresponding to vectors $\boldsymbol{x}$ within the ball of radius R_{cm} correspond to robustness states. Figure 9 shows the robustness ball centered at $\boldsymbol{I}$ which is the zero reference

in $\mathbf{X}$. The robustness radius is denoted by R and one can now assert that the outcome $\mathcal{O}_1$ is more robust than outcome $\mathcal{O}_2$ since their corresponding cm-metrics satisfy $r_1 < r_2$, where $r_1 = \|\boldsymbol{T}_{\rfloor\Updownarrow}\boldsymbol{o}_1\|_{cm}$, $r_2 = \|\boldsymbol{T}_{\rfloor\Updownarrow}\boldsymbol{o}_2\|_{cm}$. Consider a sequence of attack vectors that highlights the same critical mission or point to the same infrastructure component of $\mathcal{D}$, and denote the corresponding set of critical missions $\mathcal{C}_1$. The robustness radius for this attack scenario may be defined as:

$$R = \min_{cm \in \mathcal{C}_1} R_{cm} = \min_{cm \in \mathcal{C}_1} \max_{\boldsymbol{O} \in \mathcal{O}} \{\|\boldsymbol{T}_{cm}\mathbf{0}\|_{\mathbf{cm}} < \mathbf{M_{cm}}\} \tag{9}$$

Note that if this robustness radius is calculated for the same mission, the min evaluation is superfluous.

For complicated attack scenarios, where the outcome of the first attack may be the input of subsequent attacks, the robustness balls are interpreted differently. Consider an attack with N vectors, not necessarily directed to the same infrastructure component and not necessarily enacting the same critical mission. There are now robustness radii $R_0, R_2, \ldots, R_{N-1}$ for each of the N attack vectors, with respect to each of the N critical missions. Consider an example where N is 3, in Figure 10. The first attack vector highlights a critical mission with a robustness radius R_0, centered at $\boldsymbol{I}$ corresponding to the input state, before attacks. The outcome is $\mathcal{O}_1$ and is further subject to an attack vector that enacts a critical mission with robustness radius R_1. The third attack vector determines a ball of radius R_2, centered at a point corresponding to $\mathcal{O}_2$. Note that in the context of robustness, the norm with respect to the first critical mission of the first outcome $\mathcal{O}_1$, denoted by r_1 satisfies $r_1 \leq R_0$, i.e., the outcome $\mathcal{O}_1$ has its corresponding in the space $\boldsymbol{X}$ situated *inside* the robustness ball of the first attack. The same reasoning applies to $\mathcal{O}_2$ located inside the ball centered at $\mathcal{O}_1$, of radius R_1. Similarly: $r_2 \leq R_1$, where r_2 is the norm of the third outcome with respect to the third critical mission. Note that there is no relation or order between the robustness radii of each critical mission. The explanation of this lack of ordering is that the radius R_k corresponds to a mission whose norm definition differs from the norm definition that renders R_j, with $k \neq j$, $k, j = 0, 1, \ldots, N-1$.

In the case a component of the vector $\boldsymbol{o}$ will indicate degrees of robustness inverse proportional to its values, such as "days to repair", the transfer matrix $\boldsymbol{T}_{cm}$ uses a non-decreasing function to map this component into the corresponding component of the vector $\boldsymbol{x}$, such as an exponential:

$$f(t) = 2^{-t}, \qquad t > 0$$

where t represents time.

Example 7.1. This example shows how the abstraction from $\mathcal{O}$ to $\boldsymbol{X}$ takes place. Suppose

there is a disruption. The input state is a description of states of infrastructures before the disruption. This example focuses on only one infrastructure. Suppose that the road sector is damaged. The outcome $\mathcal{O}_1$ has an entry for transportation that describes the disruption, for example: "Interstate I58 closed; bridge collapsed after earthquake". The vector $\boldsymbol{o}$ has now for the transportation entry the value to repair and possibly costs associated with the closure of the highway: \$20M. Depending on the duration to reopen the freeway – and to rebuild the bridge– the \$20M has different meanings. If one year time is the estimated time to repair the damage and the road maintenance costs \$5M per year, then the abstract vector $\boldsymbol{x}$ has the entry corresponding to transportation 400(%).

8 Concluding remarks

This report gives a novel interpretation of robustness of the national infrastructures, regarded as heterogeneous complex systems. A methodology is developed to monitor and estimate robustness.

The accomplishment of the essential missions carried by the national infrastructures may be jeopardized by disruptions caused by accidents or intentional acts of terrorism or sabotage. Each attack scenario highlights a set of *critical missions* that must be maintained by infrastructures, sectors, etc., in order to continuously sustain the essential missions. The critical missions are defined at the highest level of decision and policy making - such as the Office for Homeland Security.

The scope of an attack may be a domain of interest constituted by whole infrastructures, or components of infrastructures, one or more cities, a region or a certain key asset. The robustness of the national infrastructures is defined with respect to the critical missions that correspond to a certain attack scenario. The attack vector comprises the perturbations a domain of interest is subjected to. The features to be preserved are expressed by the critical mission. Robustness of an infrastructure, sector, etc., for which a critical mission is defined, equates to the sustenance of the critical mission corresponding to a given attack scenario.

An attack vector highlights a collection of critical missions to be sustained. The technical details pertaining to the sustenance of a critical mission constitute the corresponding *critical function*. Further detailed specifications, courses of actions, modeling and simulation exercises aimed to mitigate the consequences of disruptions are given by the *required functions*.

The robustness metrics are derived from two components: hard and soft. The hard metrics represent quantities that may be quantifiable in dollars, number of injuries or fatalities. The hard metrics are derived mathematically via appropriate continuous or discrete models

[14, 12]. The soft metrics are not directly observable or quantifiable in dollars. This report selects as soft metric the attractiveness of the target of an attack [21]. The attractiveness metric is an aggregate measure of the consequences of an attack and its success. The robustness metrics are determined via a transfer function that captures the infrastructures' interdependencies and prioritizing strategies. Each critical mission has associated transfer functions, for each relevant decision maker. The robustness metrics are calculated from the modeling and simulation software tools.

The required functions induced by a critical mission are expressed at each level: national, regional and local and they are incorporated into the transfer functions expressed for the relevant decision makers at all these decision making levels. The local level comprises the most detailed specifications. At the regional level the required functions encompass the propagations of the consequences of disruptions from the local level. Analogously, at the national level the required functions capture the effects of disruptions form the regional level. The infrastructure interdependencies govern – at any level – the specifications of the required functions.

The outcomes of an attack have various degrees of consequences. Catastrophic effects are likely to occur over smaller areas, at geographical scales or infrastructure components. Robustness – from the perspective of the required functions induced by a critical mission – may be discussed over various scales. This hierarchical approach allows parallelization of the efforts to mitigate the consequences of an attack.

The methodology proposed here has the advantage of an immediate implementation, with tasks developed in parallel at the local levels. The specification over various scales ensures that any particularity of a domain of interest is addressed and redundancies are eliminated. This decentralized approach has the flexibility to embrace novel theoretical and technological approaches within the modeling and simulation packages and into the analysis of interdependent infrastructures.

A Systems Engineering Basics

The approach taken in this report to the modeling of the national infrastructures from the perspective of robustness is within a system engineering framework [38]. Such an approach has tradition in solving large and complex problems where technological fixes to remedy symptoms and the corresponding hardware are not always sufficient. Many of the current challenges are exacerbated by interdependencies; the elapsed time to the full implementation of a solution may render an alternative with considerable negative impacts. Systems

engineering is a rich combination of the mathematical theory of systems, behavioral theory supported by new technologies in a setting that facilitates the resolution of real world complex problems [39]. It is this setting that promotes the development of a complimentary link between quantitative and qualitative analysis, together with interdisciplinary and institutional interfaces.

Two great abstractions of the twentieth century govern the study of complex systems [16]:

1. Separate systems engineering into control, communications and computing and emphasize the development of theory and applications
2. Separate systems from physical substrate.

The system engineering methodology is a framework that consists of seven stages [39]. Here these stages are described in light of modeling the interdependent national infrastructures and mitigating disruptions.

- *Problem definition.* In modeling the behaviour of national infrastructures one distinguishes between modeling one infrastructure at a time or capturing the interdependencies. In this report, it is assumed that interdependencies are always considered when referring to the analysis of the state of a collection of infrastructure elements; in other words no infrastructure is regarded as a standalone system.
- *Value system design* includes 1) the definition of objectives and their ordering in a hierarchical structure; 2) determining the relations between objectives and practical constraints; and 3) the definition of the metrics that determine the attainment of the objectives.
- *System synthesis* follows the value system design. This stage is responsible for collecting alternative approaches pertaining to each objective and the description of these approaches.
- *System analysis and modeling.* The analysis of interdependent infrastructures comprises two parts: one is a detailed behaviour, described by the subject matter experts and the other one is the attempt to capture the perceptions of the underlying theories and abstractions that are both accurate and subject to computer simulations.
- *Optimization of alternatives and their ranking* is a collection of iterations of the previous steps. This stage aims to reduce the number of alternatives – and courses of action – through the application of a variety of analysis procedures that are highly contextual.

- *Decision making.* Metrics for determining the attainment of objectives are defined during the synthesis phase. Activities and metrics for guiding subsequent activities toward the development of a complete program plan are defined during the decision making stage – see also Section 3.4.4. Two issues are addressed during this stage: the criteria used to select appropriate courses of actions and information from the previous steps that can be used in prioritizations. In addition, the decision makers face four major challenges:

  1. the scopes of the problems to be solved; these scopes must be consistent with existing policies
  2. comparative economics of alternatives
  3. risk analysis
  4. benefits of each alternative – see also Section 3.4.3.

- *Planning courses of action (analysis of alternatives)* is the implementations of the tasks and objectives determined in the previous steps. This stage involves decision makers and subject matter experts at all levels where the attainment of objectives is relevant. The details on the challenges incurred during this task are presented in [39].

B Estimating Robustness Across Infrastructures

B.1 Overview

Recall that the robustness of a domain of interest is understood as the ability to maintain certain feature of interest – or equivalently, to sustain the critical missions – under prescribed perturbations, i.e., an attack scenario. The evaluation of the persistence of the features of interest is rendered via the transfer function, introduced in Section 6. The transfer function is expressed for various levels and locations of decision makers. This approach follows the DHS document [2] "In effect the front lines of the defense in this new type of battle have moved into our communities and the individual institutions that make up our critical infrastructure sectors. During the Cold War era, many government and private organizations isolated parts of their physical and information infrastructures into 'stovepipes' to assure their protection. this approach is no longer adequate to protect our homeland from determined terrorists. Stimulating voluntary, rapidly adaptive protection activities require a a culture of trust and ongoing collaborations among relevant public – and private – sector stakeholders, rather than more traditional systems of command and control." The challenges of modeling and simulation of a

complex adaptive system that is the abstraction of a domain of interest call for a broad range of theoretical and applied research tools to solve problems of very large sizes.

There are three main types of failures of a domain of interest: common cause, escalating and cascading, with the most effects of interdependencies carried by the last two types – see Section 3.2. The self-healing mechanisms ensure that the effect of disruptions are constrained within a functioning state of the domain of interest and that the escalating failures are minimized and the cascading ones are prevented. A domain of interest may reconfigure its nodes and services, unless an irreducible stage is attained and one or more critical missions are lost over that domain of interest. Three stages describe the process of addressing disruptions and estimating the robustness of a domain of interest - within the sustenance of the critical mission and its induced critical and required functions.

1. Model and simulate the behavior of the domain of interest
2. Build knowledge bases
3. Devise appropriate courses of action.

B.2 The proposed methodology

Estimating robustness across infrastructures is first considered at the local level. Section B.4 addresses larger geographical areas.

After the critical missions are formulated at a high level of decision making, the critical function associated with each mission is devised during a first iteration by the subject matter experts, also at a high decision level. Recall that the critical function branches further into required functions. The required functions encompass procedures, rules, decisions, software simulation, costs thresholds, etc that are not obviously stated from the first statement of the critical mission or from the critical function. Expressing fully the required functions is itself an interactive and iterative process. The transfer function exploits all the considerations provided by the required functions and renders the robustness metric.

An example illustrates this hierarchical approach.

Example B.1. Consider that the domain of interest is the cattle industry and the critical mission is to protect the sector with respect to the mad cow disease. This formulation does not specify what "protection of the sector" means. After the relatively few cases of mad cow disease it may be inferred that the cattle sector is not robust and the sector is endangered. However, the subject matter experts at the Department of Agriculture level refine this mission, such as: "A loss of 1% of the cattle due to mad cow disease is acceptable over a period

of 2 years". This refinement of the specification of the critical mission constitutes the critical function. Robustness of the cattle sector is considered with respect to this threshold from the critical function. This example is revisited from the perspective of scale-dependent robustness analysis.

B.2.1 Modeling and simulating the behavior of a domain of interest

The first task of modeling and simulation of the behaviour of a domain of interest as a heterogeneous complex adaptive system is the most challenging of the stages above and it is itself adaptive. From a first iteration/approximation it is likely that refinement steps follow with the aid of real data and the real-time responses from the monitoring systems and simulation packages. The heterogeneous complex adaptive system approach may accommodate any type of system control and monitoring of infrastructures [23, 11]. Moreover the self-healing mechanisms and reconfigurations are interactive designs as well.

During the tuning phase, modeling and simulation tools for each infrastructure behaviour provide outputs from both inputs of normal functioning and disrupted states. Once these tools are tuned and have a satisfactory level of fidelity, their outputs provide the hard metrics. The metrics represent the quantification in dollars of poor or lost services and assets. The required functions are detailed based on these output information. The soft metrics contribute to assess priorities. The interdependencies are yet to be integrated. The approach may be sequential – such as the integration of interdependencies between the electric power grid and the natural gas system. Further, the interdependencies of other infrastructures are integrated [14]. It is also possible to use a transfer function that integrates interdependencies of all infrastructure over suitable scales, such as the metropolitan models [12] developed within the Critical Infrastructure Protection/Decision Support System (CIP/DSS) project.

Complex adaptive systems may be efficiently investigated if the interactive agents ensures a continuous monitoring such that any change in the behavior of the domain of interest can be detected. The monitoring agents play an essential role in capturing interdependencies and preventing escalating and cascading failures. It is at this stage where the design of the self-healing mechanisms is refined and completed. The required functions are established and a full simulation renders the new state of the domain of interest with hard metrics associated with disruptions and loss of services and components.

At each infrastructure level, intelligent agents can be employed to monitor the operating state and also to:

- develop a high-fidelity scenario-free modeling and optimization tools

- develop networks of intelligent agents that communicate and cooperate to accomplish their routine tasks
- create self-optimizing and self-healing capabilities of the infrastructure they serve as well as the interconnected ones.

An agent assisting a complex adaptive system is characterized by:

- reactivity: can sense the environment and act accordingly
- autonomy: it does not require human intervention/supervision/interaction
- collaborative behavior: it can work with other agents toward a common goal
- inferential capability
- temporal continuity: its domain of interest and state persists over long periods of time
- adaptive: it can learn and improve with experience

The architectures proposed for modeling complex adaptive systems are hybrid distributed systems [5, 29] with intelligent agents. Their capabilities are:

- recognizes an attack or loss of services
- responds quickly to mitigate the effects
- minimizes the risk of cascading effects
- determines an optimum recovery path
- contributes to the knowledge base and the learning tasks.

This type of architecture is organized on three layers: a reactive layer, a coordination layer and a cognitive/decision making one. The response from the reactive layer is deterministic in general (input from monitoring agents) and reflects little on the interdependencies. The cognitive layer is capable of filtering information, interpreting commands, infer knowledge. The cognitive layer is the one that process the information and ultimately decides on a strategy to addresses failures.

B.2.2 Building knowledge bases

Modeling and simulations tools of the behaviour of a domain of interest are intended mainly for planning. Each of the simulation tasks is a computationally expensive one. Hence these simulation exercises should be stored in a Scenario Library – Figure 11 – that should include both the input state of an domain of interest, together with outputs from various behaviors under adverse conditions.

The costs associated with each outcome of a disruption may be the hard metric that indicates the sustenance of the critical mission and reflects therefore on the robustness across the domain of interest. The Scenario Library may also store all the detailed tasks for each of the outputs: the reconfiguration of the components and also the functionality of a domain of interest. This library is a large heterogeneous database, with a considerable size for each of its entries (Figure 11). However, it is not possible to plan and store exhaustively attack scenarios and courses of actions. Prioritization should be employed first to decide which attack scenarios must be analyzed; further prioritization assists in storing relevant details. The Scenario Library – in short – contains *very high impact* scenarios.

The information arises from a variety of sources [29] and within this stage the fusion of heterogeneous information takes place. The knowledge basis formation consists of three stages: formalization, acquisition and application [5, 29, 40]. The decision makers may also influence the construction of the Scenario Library: this large collection of information has to be as exhaustive as possible, yet realizable and accessible within acceptable time frames and sizes. The prioritizing strategy must be supervised by the decision makers. For each course of action devised, soft metrics may be incorporated as extent of damage labeled simply: "mild", "moderate" or "severe". In particular, the attractiveness metric may be stored for each focal point. The evaluation of the attractiveness metric s subject to updates, dictated by the terrorist threat level or major national and international events, such as elections or international sport competitions.

B.2.3 Devise courses of action

Suppose that a domain of interest is under scrutiny, subject to an attack scenario or a disruption. The Scenario Library provides a collection of simulations of the behavior of the domain of interest, costs associated with loss of services, and also recovery alternatives designed using the self-healing and reconfiguration strategies. Given the size and the complexity of investigating the collection of infrastructure components present within that domain, a considerable number of outputs may be delivered for one disruption instance. These scenarios

may not be all manageable by decision makers within the time-frame dictated by the severity of the disruption and the requirements of the critical function. Hence a decision maker must be assisted by a powerful intelligent agent computer system to choose from fewer items in the scenario library. This intelligent system must be able to learn and infer knowledge so that scenarios that are not already part of the library can be designed, also in a timely manner. Planning strategies may also be employed [25]. The fast response of the simulation tools is an indispensable attribute for addressing critical situations. The critical situations that have not been modeled and are not part of the Scenario Library may be addressed in situ provided real-time capabilities of the NISAC software, metropolitan models and faster artificial intelligence/expert systems.

The system agents are specialized for a variety of tasks to perform: interface, profiling and filtering, retrieval, navigation and monitoring.

A learning shell is an artificial intelligence software tool that can be employed to help sorting and processing the scenarios at hand and to infer new possible scenarios for optimum courses of action [40, 41]. A subject matter expert analyzes the domain of interest, assesses risks, and assists a decision maker with tasks that are part of the required functions – during both disruption and planning exercises. Neither the subject matter expert nor the decision maker are required to be computer experts. The subject matter expert interacts with a knowledge engineer who is able to translate into a machine language the information from the subject matter expert. An intelligent agent consists of a knowledge base and an inference engine. A refinement of this process is the use of a learning agent, whose effect is to eliminate the knowledge bottleneck while populating the Scenario Library.

Ultimately, the learning agent shell interacts only with the decision maker and is able to learn and pass knowledge such that their interaction is fast and reliable. Moreover, assessment of vulnerability and criticality of interdependent infrastructures can also be realized with a learning agent tool. This interactive real-time task minimizes escalating failures and prevents cascading ones. The multi-level synergism achieved through mixed-initiative reasoning that integrates complementary human and automated reasoning takes advantage of their respective knowledge, reasoning styles and computational strength [41]. Figure 12 illustrates the decision making process during a disruption in progress.

The learning shell tool briefly described is involved in fact in all the three steps of the methodology. This tool is implicitly regarded as an integration hybrid package that employs software already implemented within the NISAC and CIP/DSS efforts as well as the power of learning agent technology. There exist expert systems tools in the class of learning agent shells that can be extended to integration tools to be employed in the simulation of heteroge-

neous complex adaptive systems that model the national infrastructures [41, 40, 48, 18, 42].

B.3 The induced functions revisited

The purpose of this section is to discuss the evaluation of robustness at various scales and to interpret robustness over various domains of interest, for the same critical mission.

Local subject matter experts can address exhaustively the tasks derived from the critical function – these are the components of the required functions. Decentralization of control is becoming a more embraced approach for the analysis of large complex systems and networks, such as the national infrastructures. Smaller, local systems become the system configuration of choice. Centralization carries increasing complexity and has weaknesses that can be exploited by terrorists. In contrast, detailed local analysis of risk renders an optimum allocation of resources from a more accurate analysis of vulnerabilities [20].

The directives travel from DHS to national, regional and local levels, one step at a time in case of refining a critical mission, or propagate simultaneously at all level – such as the terror threat level, in which case most of the measurements to be taken are already devised, for each level. At each scale transition, from larger to smaller, more specifics are added to the required functions. The robustness may be considered at each level from the perspective of accomplishing the required functions stemming from the critical mission.

Robustness with respect to the threshold imposed by the critical function has one interpretation at infrastructure or sector level; and that is – in general – to maintain the infrastructure/sector/segments in a functioning state, within the threshold that observes the large scale (national level). However, at smaller scales, local level, the robustness of the whole infrastructure/sector/segment has little relevance on the consequences of a local disruption. Robustness therefore may be evaluated over all the domains of interest where the critical mission must be sustained.

Recall the Example B.1 about the cattle industry. The sector is robust – even with the relatively few cases of mad cow disease. Over the states and counties where there were cases of the disease outbreak, the consequences impact largely these domains of interest.

The required functions may be devised to carry robustness metrics at any level they are formulated. The specifics of the required functions enrich over smaller domains, while the robustness estimates carry coarser information from lower scales to larger scales.

Example B.2. Suppose that there is a biological attack in city X. Suppose that city X is a small city, not regarded as a terrorist target – hence it is unprepared for an attack. The robustness of the public health sector – at the national scale – with respect to biological attacks may be

achieved even if city X must be quarantined and isolated. For city X, however, the attack was catastrophic and there is no local robustness to speak of.

This example and the previous considerations on decentralization, together with the emphasis of the DHS document of the responsibilities of local domains of interest to protect key assets, suggest that robustness with respect to a certain critical mission must be discussed over each scale, with higher probability to loose robustness (reflected in catastrophic consequences) at local levels.

Under attacks, local level domains of interest – such as a small town or the cattle industry of one county – are more likely to collapse. However, as emphasized in Example B.1 the large impacts at local levels do not equate to loss of robustness with respect to the critical mission formulated for the whole sector, at the national scale.

A main advantage of devising required functions for the local levels is the parallelization of the process of devising courses of action to address disruptions: local subject matter expert work simultaneously and almost independently to asses their focal points and the tasks involved in attaining their objectives derived from the critical mission. However, the activities at local level are not totally independent: supervision from larger scales and higher decision making levels ensure consistency, cooperation and sustenance of the tasks to be performed at regional level and further to national level. The next section discusses the degree of independence of the activities performed at local levels by the decision makers and subject matter experts.

This hierarchical approach suggests that the modeling and simulation tools should accommodate various granularities in data processing and analysis. All the modeling software tools in place are able to easily accommodate coarse granularity and smaller regions. Further software development is in progress to address accurate modeling of local effects [43, 44, 13].

The critical mission over a domain of interest, as formulated by the decision makers, has little insight on how to accomplish the mission; however the critical mission has an active role in prioritizing the relevant tasks. The required functions explicitly describe all the tasks, decisions, simulations, etc. to be performed in order to continuously maintain the critical mission. The local experts are the ones that can detail accurately the required functions and also address at first the consequences of disruptions that cannot be expresses strictly and immediately in dollars.

The sizes of the problems to be tackled at a national level are very large. For example, the number of constraints for the electric power grid alone is 2.65 billion. A smaller scale implementation may speed the whole task of addressing robustness and preventing cascading failures at the local level. A first iteration of assessing the required functions and strategies

to mitigate contingencies might use simple models - even as simple as spreadsheets - that capture the essential tasks of the critical function. It is possible to derive courses of action in this way for domains of interest as large as a state [45].

B.3.1 Characteristics of the induced metrics

The metrics derived from the processes involved in establishing and monitoring robustness have all the characteristics listed in Section 5. First the metrics that are costs associated with courses of action are not just aggregates of hard metrics. Recall that prioritizing tasks are fused in both the statement of the critical function and the procedures of the required functions. Hence these metrics are helpful in further prioritization of threats and risks. That is because the cost associated with each course of action includes possible quantizations of soft metrics associated with the extent of the damage; and these are the primer in evaluating and prioritizing the threats to be addressed.

What do these metrics indicate, ultimately? Recall that the hard metrics are outputs from the planning tools and they capture interdependencies. The components over each infrastructure may be detached or monitored separately. Hence these metrics are suitable in developing data sets.

Once the modeling tools are tuned, comparisons with past events – with respect to evaluation of consequences – give the metrics the role of validating models.

The methodology proposed here is characterized by the evaluation of course of actions and the adoption of an optimum one. The decision maker selects the best course of action by comparing the metrics – both hard and soft – associated with each course of action[11].

The efforts to tune modeling and simulation tools to capture interdependencies and those involved in designing the hybrid technology using a learning agent shell are extensive. The metrics proposed by this methodology may be devised, however the time frame is likely in the order of years.

B.4 Generalization

The methodology proposed in this report suggests that robustness should be treated first over small domains of interest and at the local level, at smaller geographical and logical scales. This approach is not exhaustive in protecting the critical infrastructures – rather it is a first efficient step within a "bottom-up" framework. Recall that engaging local subject matter

[11] Rigorously speaking, the decision maker chooses a course of action that maximizes the utility function [31].

experts amounts to parallelizing the tasks related to ensuring the robustness of domains of interest at the local level.

This localized approach relies on a fine partition of national infrastructures where each sub-ensemble is examined – with respect to robustness – in the finest detail. There exist econometric techniques that render reliable prediction model at any scale. However, the local business expertise provide a more accurate evaluation of the costs of disruption. This also dictates decentralization. Local models employed to predict the effects of disruptions are also likely to have capabilities to address any range of time-scales.

The estimating of robustness over larger areas – and implicitly the prevention of large scale cascading failures – is the concern of this section. Preventing cascading failures is the most important mitigation task and the main attribute of robustness [16]. Besides a fine partitioning of infrastructures at the finest level (local, individual infrastructure components), there are coarser partitions where robustness is observed over larger domains of interest. Coarser partitioning capture the possible cascading effects and the effects a disruption at a certain location may have over its neighboring domains. In other words, a collection of required functions may be defined locally but the effects of losing the critical mission might propagate globally – and in this case there should be required functions defined over larger domains of interest. This is the next level of refinement within the "bottom-up" paradigm. In a nutshell:

- create a coarser partition of infrastructures (for all types of interdependencies: geographical, physical, cyber and logical)
- gather from the local domains of interest of the fine partition the studies on the critical missions and required functions, and courses of action
- gather subject matter experts from the coarser scale (larger) domains of interest and define required functions over these larger domains; there will be coarser details within these required functions
- follow the same steps as for the fine partition
  - create the scenario library
  - devise courses of action.

This strategy captures the propagation of consequences at larger levels as well as the global effects on highly connected infrastructure networks (telecommunications, banks). The coarser granularity translates into reduced size of models and thus ensures fast real-time analysis and computer simulations.

The next example shows how the required functions at the local level induce required functions at the regional level.

Example B.3. Suppose the domain of interest is a small city X in state S. City X holds government key assets and has only one hospital. An attack scenario is: "dirty bomb threat". The critical mission that is highlighted first is: "Protect the government key asset". If the required function in X has one alternative course of action the evacuation of the local hospital, then, at the state level, the Public Health infrastructure should have measures in place to accommodate the evacuation of the hospital located in X. Therefore, at the state level, there should be a required function that addresses the consequences of disruptions and the mitigations of disruptions at city X level. A required function for the Public Health infrastructure over the state S would describe the other hospitals that would accept patients transferred from X – provided that the critical mission in X is still sustained and the key assets are protected.

The "bottom-up" strategy incurs both parallel and sequential tasks, hence the elapsed implementation might take years. It is the responsibility of subject matter experts and decision makers to employ prioritizing strategies such that courses of action are properly projected, without the obvious difficulty of dead-ended recursions.

The methodology proposed here has the merit of an immediate commence at local domains of interest, and the required functions stemming from a critical function may be defined. The first tasks of the required function may be detailed. A risk analysis may be performed resulting in a first prioritizing task. The generalization of this approach to larger geographical and logical scales is natural and uses the same strategies and tools as at local level. The software and methods used are not restricted and any theoretical result as well as existing software tool can be incorporated into the machinery of the learning agent integration tool. Hence this methodology that allows subject matter experts to detail their critical mission – at any level – is a versatile strategy that is open and subject to continuous upgrades that benefits from the most novel technologies and studies.

References

[1] *Webster's Ninth New Collegiate Dictionary*. Merriam-Webster Inc., Springfiled, MA, 1983.

[2] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Technical report, Department of Homeland Security, Feb. 2003.

[3] S. Ali, A.A. Maciejewski, H.J. Siegel, and J.K. Kim. Measuring the Robustness of a Resource Allocation. *IEEE Transactions on Parallel and Distributed Systems*, 15(5), May 2004. Preprint.

[4] M. Amin. *Automation, Control and Complexity: An integrated approach*, chapter National Infrastructures as Complex Interactive Networks, pages 263–286. John Wiley and Sons, 2000.

[5] M. Amin. Toward Self-Healing Energy Infrastructure Systems. *IEEE Computer Applications in Power*, Jan. 2001.

[6] M. Amin. Impact of Data-driven Modeling on Electricity Infrastructure Operations and Security Operations. In *IMA Workshop on Data-driven Control and Optimization*, Minneapolis, MN, Dec. 2002.

[7] M. Amin. *Market Analysis and Resource Management*, chapter 3: Simulating the Evolution of the Electric Power industry with Intelligent Adaptive Agents. Kluwer Publishers, March 2002.

[8] M. Amin. Security challenges for the electricity infrastructure. *Supplement to Computer: Security and Privacy*, 2002.

[9] A. L. Barabasi. *Linked: How Everything Is Connected to Everything Else and What It Means*. Penguin Group USA, New York, NY, reissue edition edition, 2003.

[10] M. Blue, B. Bush, and C. Unal. Robustness and Reliability Metrics for Energy Transmission Networks. Draft, 2003.

[11] N. Boccara. *Modeling Complex Systems*. Springer-Verlag, New York, NY, 2004.

[12] B. Bush. Critical infrastructure protection/decision support system (cip/dss) project metropolitan infrastructure Model. Technical Report LA-UR-04-1217, Los Alamos National Laboratory, 2004.

[13] B. Bush, C. Files, and D. Thompson. Empirical Characterization of Infrastructure Networks. Technical report, Los Alamos National Laboratory, Los Alamos, NM, 2001.

[14] B. Bush, O. Giguerre, J. Holland, S. Linger, A. McCoown, M. Salazar, C. Unal, D. Visarraga, K. Werley, R. Fisher, S. Folga, E. Portante, and S.Shamsuddin. Nisac energy sector: Interdependent energy infrastructure simulation system (IEISS). Technical Report LA-UR-03-1159, Los Alamos National Laboratory, Los Alamos, NM, 2003.

[15] B. Bush, C. Joslyn, and D. Powell. Dimensional Infrastructure Sub-sectors. Technical report, Los Alamos National Laboratory, Los Alamos, NM, Aug 2003.

[16] J. M. Carlson and J. Doyle. Complexity and robustness. *Proc. National Academy of Sciences*, (99, Suppl. 1):2538–2545, 2002.

[17] W. Cheney. *Analysis for Applied Mathematics*. Springer-Verlag, New York, 2001.

[18] P. Cohen, R. Schrag, E. Jone, A. Pease, A. Lin, B. Starr, D. Gunning, and M. Burke. The DARPA High-Performance Knowledge Bases Project. *AI Magazine*, 19(4):25–49, 1998.

[19] North America Electric Reliability Council. The Reliability of Bulk Electric Systems in North America. http://www.nerc.com, October 2002.

[20] J. Darby. Vulnerability Analysis Capabilities, Unpublished Internal Report. Los Alamos National Laboratory, Los Alamos, NM, 2001.

[21] J. Darby, B. Bush, S. Eisenhawer, and T. Bott. Methodology for optimizing allocation of resources to protect infrastructure against acts of terrorism. Technical Report LA-UR 04-0590, Los Alamos National Laboratory, Los Alamos, NM, 2003.

[22] J. Day and S. Thompson. A global template for evaluating and ranking innovative attack scenarios. DIA Working Draft 1, Jan 2003.

[23] K. A. El-Metwally and O. P. Malik. Fuzzy logic power system stabilizer. *IEEE Proc.-Gener. Transm. Distrib.*, 142(3), May 1995.

[24] N. Hengartner. Interdependencies of financial and communication sectors, unpublished internal report. CIP/DSS Web page, Los Alamos National Laboratory, Los Alamos, NM, 2003.

[25] J. Hoffmann. *Utilizing Problem Structure in Planning - A Local Search Approach.* Number 2854 in Lecture Notes in Artificial Intelligence. Springer-Verlag, Berlin, 2003.

[26] Robustness Project, http://discuss.santafe.edu/robustness. Santa Fe Institute, Online, 2001.

[27] E. Jen. Stable or robust? what's the difference? *Complexity*, 8(3):12–18, 2003.

[28] V. Loose. Supply of the Militarily Critical Commodities, Unpublished Internal Report. Los Alamos National Laboratory, Los Alamos, NM, 1996.

[29] S.D. Matthews, L. Wilder, and F. J. Varas. The GTD and INEEL Survivable Subnetworks collaboration. Technical report, INEEL, April 2003.

[30] M. McNulty. Multi criteria decision making tools and systems. Personal communication, Los Alamos National Laboratory, Los Alamos, NM, 2003.

[31] M. McNulty. Prioritization methodology. Personal Communication, 2003. Los Alamos National Laboratory, Los Alamos, NM.

[32] M. McNulty. Risk-consequence scoring definitions. Personal Communication, Los Alamos National Laboratory, Los Alamos, NM, 2003.

[33] R.B. Myerson. *Game Theory: Analysis of Conflict.* Harvard University Press, Cambridge, MA, 2002. Fifth printing.

[34] C.V. Negoita. *Expert Systems and Fuzzy Systems.* The Benjamin Cummings Publishing Company, Menlo Park, CA, 1985.

[35] Presidential decision directive 63. Online: http://www.ciao.gov.

[36] N. Palaniappan. *Fuzzy Topology.* CRC Press, Boca Raton, FL, 2002.

[37] W. Poole. Financial System Robustness. Technical report, Federal Reserve Bank of St. Louis, St. Luois, MI, Nov. 2001.

[38] S.M. Rinaldi, J.P. Peerenboom, and T.K.Kelly. Identifying, understanding and analyzing critical infrastructure dependencies. *IEEE control systems magazine*, pages 11–25, Dec. 2001.

[39] A. P. Sage and W. B. Rouse, editors. *Handbook of Systems Engineering and Management.* Wiley-Interscience, New York, NY, New York, NY, 1999.

[40] G. Tecuci. *Building Intelligent Agents.* Academic Press, San Diego, CA, 1998.

[41] G. Tecuci, M. Boicu, M. Bowman, , D. Marcu, and M. Burke. An Innovative Application from the DARPA Knowledge Bases Programs: Rapid Development of a High Performance Knowledge Base for Course of Action Critiquing. *AI Magazine, AAAI Press*, 22(2):43–61, 2001.

[42] G. Tecuci, M. Boicu, D. Marcu, B. Stanescu, C. Boicu, and J. Comello. Training and Using Disciple Agents: A Case Study in the Military Center of Gravity Analysis Domain. *AI Magazine*, 2002.

[43] G. L. Toole. Request for Proposal: Fast Simulation and Modeling System Statement of Work: Electricity innovation Institute/Consortium for the Electricity Infrastructure for a digital society (CEIDS) Program.

[44] G. L. Toole. Algorithms for electric power network contingency response. Draft, Feb 2003.

[45] G. L. Toole. Critical mission- personal communication. Los Alamos National Laboratory, Los Alamos, NM, October 2003.

[46] P.A Vargas, L. N de Castro, and F. J. Von Zuben. Mapping Artificial Immune Systems Into Learning Classifier Systems . In *Learning Classifier Systems*, number 2661 in LNAI, pages 163–186.

[47] D. Verton. Experts Debate U.S. Power Grid's Vulnerabilities to Hackers. *Computerworld [Online]*, Mar 2001.

[48] K. Wang. *Intelligent Condition Monitoring and Diagnosis Systems: A Computational Intelligence Approach.* IOS Press, Amsterdam, 2003.

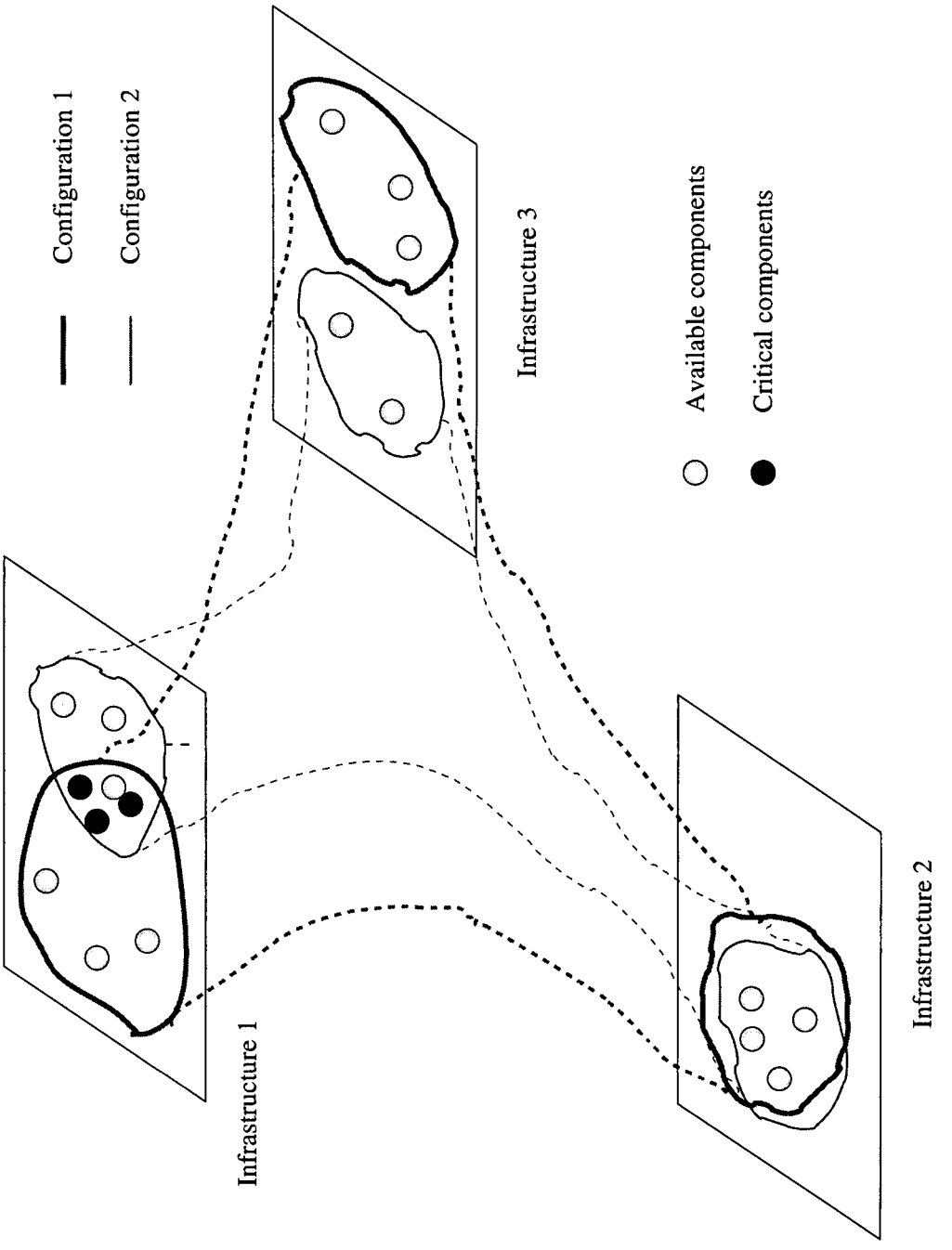

Figure 1: Reconfiguration of infrastructure nodes

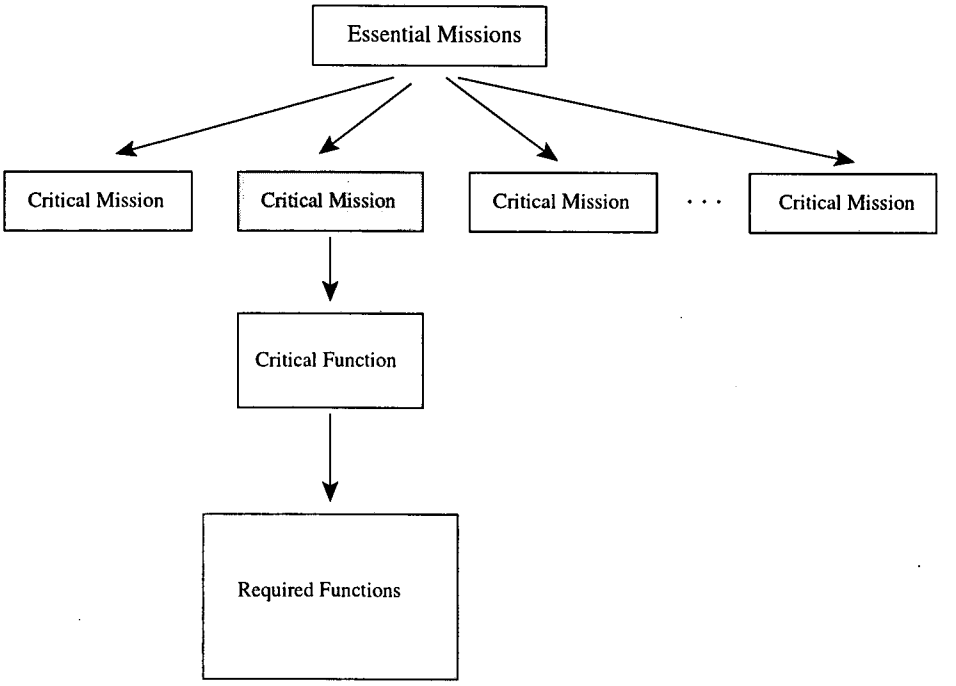

Figure 2: The essential mission, a selected critical mission and the functions induced by the critical mission.

Figure 3: The Required Functions

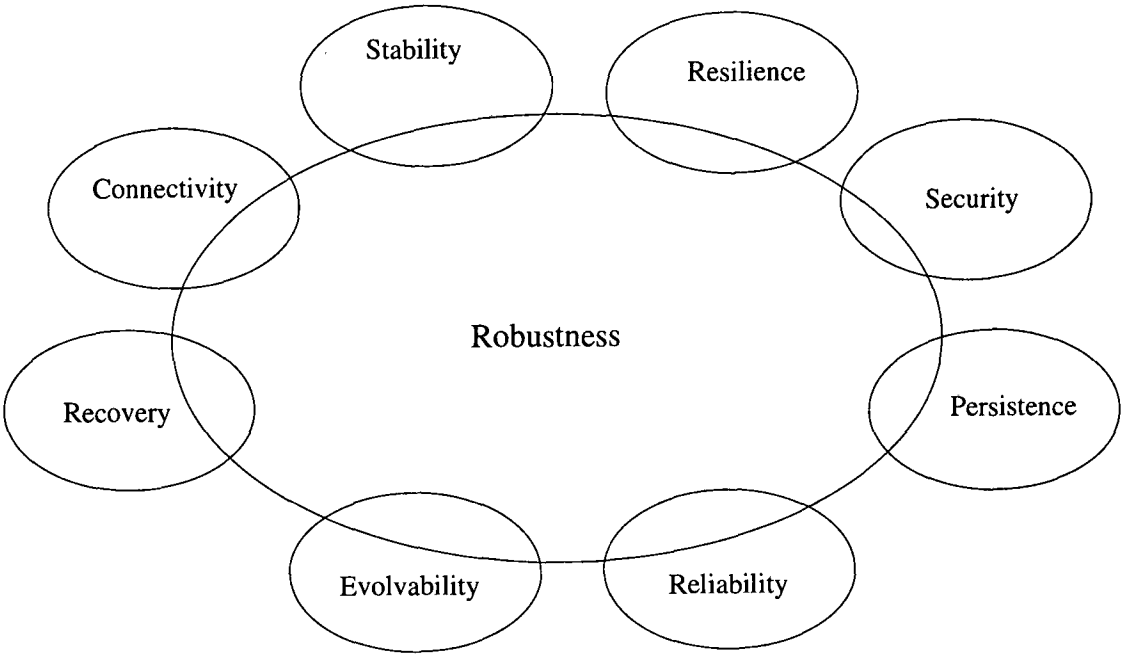

Figure 4: Attributes of a system

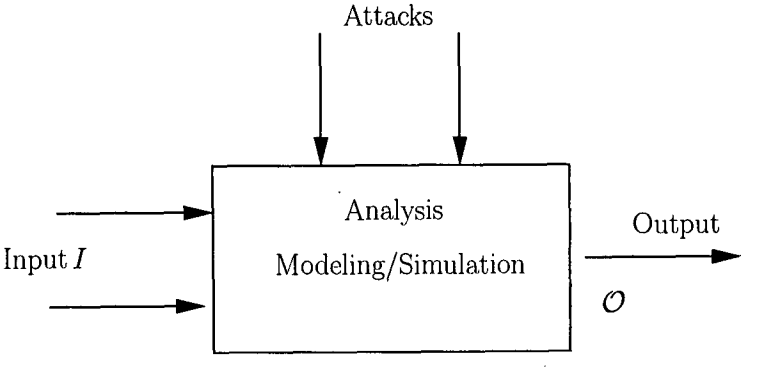

Figure 5: Attack Scenario

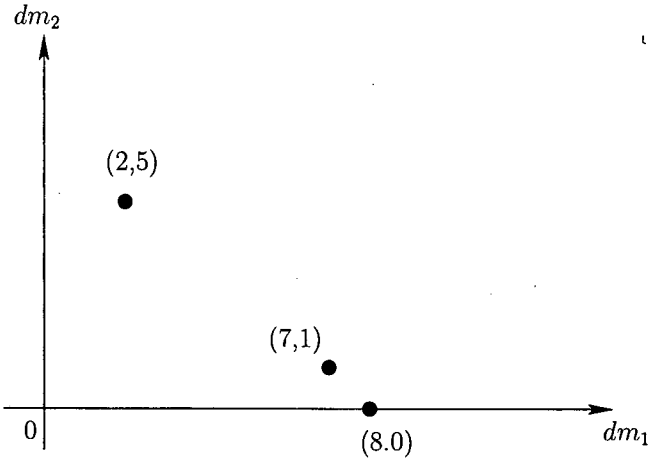

Figure 6: Robustness metrics for two decision makers

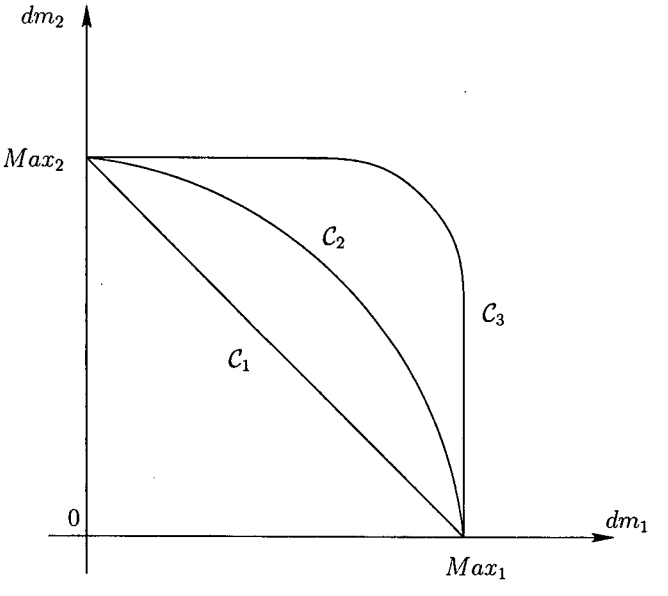

Figure 7: Robustness areas for two decision makers

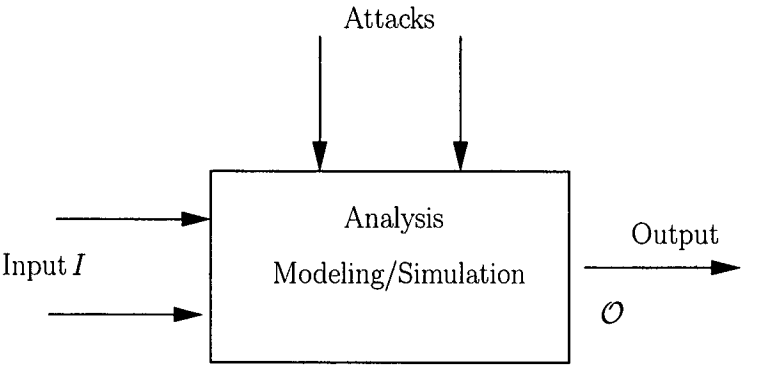

Figure 8: Attack Scenario

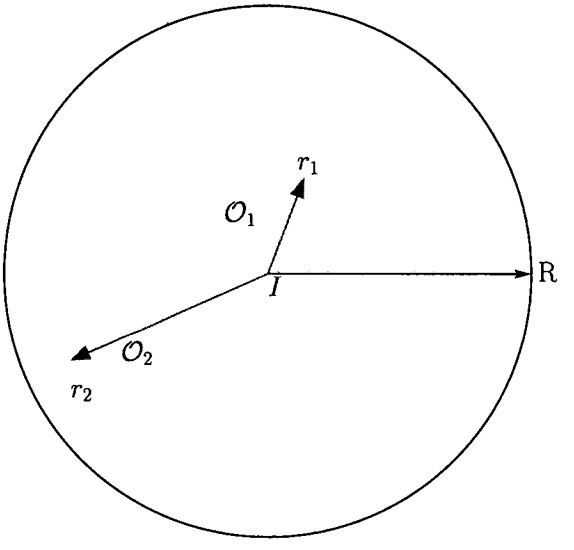

Figure 9: Robustness radius for one attack vector

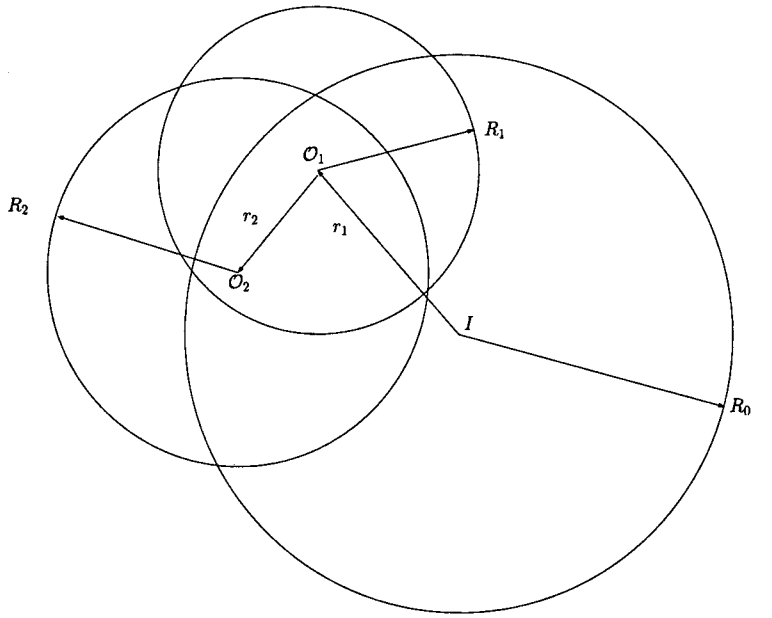

Figure 10: Robustness balls for an attack scenario with 3 attack vectors

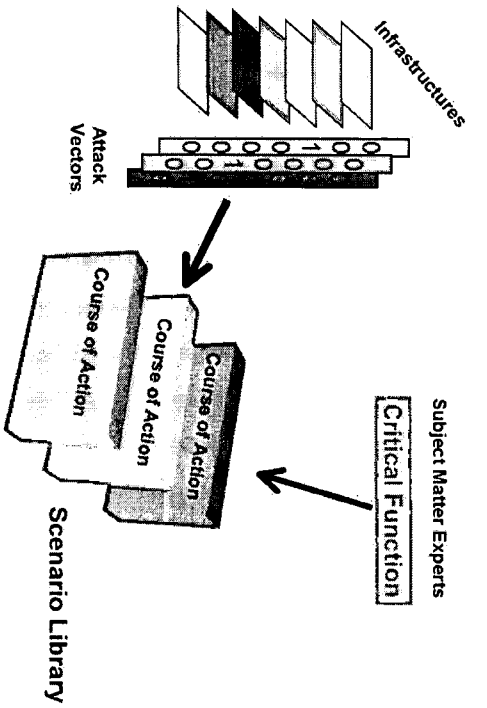

Figure 11: The Scenario Library

Figure 12: The Decision Making Process