Models for reducing the risk of critical networked infrastructures

Hugh Medal*, Stevenson J. Sharp, Ed Pohl and Chase Rainwater

Department of Industrial Engineering,
4207 Bell Engineering Centre,
University of Arkansas,
Fayetteville, AR 72701, USA
E-mail: hugh.medal@uark.edu
E-mail: sjsharp@uark.edu
E-mail: epohl@uark.edu
E-mail: cer@uark.edu
*Corresponding author

Scott J. Mason

Department of Industrial Engineering,
Clemson University,
124 Freeman Hall, Clemson, SC 29634, USA
E-mail: mason@clemson.edu

Abstract: In this paper, we review the literature studying how to reduce the disruption risk to critical networked infrastructures. This is an important area of research because huge consequences result from infrastructure disruptions. As a result, this research area has grown a lot in the last decade. In this review we discuss articles from the literature, place them into categories, and suggest topics for future research. Our review shows that although this area is growing in popularity, there are still many important opportunities for future work.

Keywords: risk; interdiction; fortification; protection; reliability; mitigation; critical infrastructure; disruptions; networks; risk assessment; risk management.

Reference to this paper should be made as follows: Medal, H., Sharp, S.J., Pohl, E., Rainwater, C. and Mason, S.J. (2011) 'Models for reducing the risk of critical networked infrastructures', *Int. J. Risk Assessment and Management*, Vol. 15, Nos. 2/3, pp.99–127.

Biographical notes: Hugh Medal is a PhD candidate in the Department of Industrial Engineering at the University of Arkansas. His primary research interests are disaster preparedness and mitigation, critical infrastructure protection, the design of resilient systems, and interdiction modelling.

Stevenson J. Sharp is a PhD candidate in the Department of Industrial Engineering at the University of Arkansas. His primary research interest is in dynamic resource allocation problems.

Ed Pohl is an Associate Professor in the Department of Industrial Engineering at the University of Arkansas. He received his PhD in Systems and Industrial

Engineering from the University of Arizona. His primary research interests are in repairable systems modelling, reliability, decision making under uncertainty, engineering optimisation, and probabilistic design. He is a senior member of IIE, ASQ and IEEE. He serves as an Associate Editor for the *Journal of Military Operations Research* and the *Journal of Risk and Reliability*.

Chase Rainwater is an Assistant Professor in the Department of Industrial Engineering at the University of Arkansas. He received his PhD in Industrial and Systems Engineering from the University of Florida. His primary research interests are in large-scale optimisation, integer programming and supply chain logistics. In addition, he is active in the areas of reliability, homeland security and healthcare planning. He is a member of IIE, INFORMS and MORS.

Scott J. Mason is the Fluor Endowed Chair in Supply Chain Optimisation and Logistics and a Professor of Industrial Engineering at Clemson University. He received his PhD in Industrial Engineering from Arizona State University after earning Bachelor and Master degrees from the University of Texas at Austin. His areas of focus include operations planning, scheduling, and control of capital project supply chains and large-scale systems modelling, optimisation, and algorithms, with domain expertise in semiconductor manufacturing. He is a senior member of the Institute for Industrial Engineers and a member of INFORMS.

1 Introduction

The Department of Homeland Security lists 18 infrastructures that are critical to the USA, including transportation and electrical power (Department of Homeland Security, 2002). Many of these infrastructures are made up of interconnected elements organised in a network as in transportation and electrical power networks. Almost all of these infrastructures are subject to the risk of being disrupted, leaving them unable to perform their intended function. In this survey paper we review articles that study how to reduce the disruption risk of critical networked infrastructures.

The risk of the disruption of critical infrastructure systems deserves the attention of researchers for several reasons. First, critical infrastructures are becoming more complex and more geographically dispersed, making them more difficult to analyse. Second, the function of these infrastructures is, by definition, critical.

Recent events demonstrate the consequences of disruptions in critical infrastructures. The 2004–2005 disruption of the rail network in the Powder River basin of Wyoming resulted in a shortage of coal and electricity price increases of up to 15% for certain regions of the USA (Rail Report: Rail Customer News and Information, 2005). Another more recent example is the 2010 eruptions of the volcano Eyjafjallajökull in Iceland, which disrupted air travel throughout northern and western Europe for about six days (Michaels et al., 2010). Another well-known example is the blackout that occurred in the Northeastern USA in 2003. The blackout was caused by the failure of power lines due to contact with trees and exacerbated by a software bug in the energy management system. The blackout ultimately impacted many other important networks such as water distribution, transportation, wireless communication, and the internet (United States-Canada Power System Outage Task Force, 2004).

There is a growing body of literature that is focused on developing ways to efficiently mitigate the risk of disruption in critical infrastructures. The purpose of this paper is to give an overview of this body of literature. In particular, we categorise each paper according to three characteristics. The categorisation should help the reader understand this field as well as highlight gaps where research needs to be done. In this paper we intend to show that while good work has been done in this research area, there are many important questions that have not yet been addressed.

There are a few other notable surveys related to this paper. Snyder et al. (2010) survey the literature relating to disruptions in supply chains, covering a broader array of topics than just networks. Brown et al. (2005) provide a tutorial on defending networks against attackers. Snyder et al. (2006) provide a survey and tutorial on disruptions to supply networks, covering both design and hardening models.

We consider our paper to be a complement to the paper by Snyder et al. (2006) because it discusses additional types of networks and presents additional risk reduction strategies besides hardening. It should be noted that most of the models presented in Snyder et al. (2006) use operations research/management science (OR/MS) techniques, primarily mathematical programming. However, the additional topics that we include in this paper have been studied by researchers with a diverse set of backgrounds (e.g., physics, economics, and geography), bringing different assumptions and problem solving techniques to the forefront. The diversity of backgrounds amongst researchers in the area of network disruptions can also be observed by the many different types of journals in which the papers in this review were published. We believe that the inclusion of the additional topics into this paper will help expose researchers from many different disciplines working on network disruption problems to different ways of approaching these problems.

The principal contributions of this review paper are:

1 a comprehensive review of network disruption problems, covering many different application areas with a focus on how researchers have modelled these problems

2 a helpful classification of this body of literature that includes work done by researchers from a diverse set of backgrounds

3 a discussion of the gaps in this body of literature

4 an identification of important areas for future research.

2 Definitions, classification scheme, and scope

2.1 Definitions

There are several definitions that we use often in this review. Our primary source for these definitions is a report by the Department of Homeland Security (The Department of Homeland Security Risk Steering Committee, 2008).

Before reading this review it is important to understand the terminology of what makes up a network and what happens to networks. An *element* is a network component such as an edge or node. The *state* of an element or network may be operating, failed, or some level in between. An *incident* is something that can change the state of an element. An incident caused by an antagonist is called an *attack*. An incident that cannot

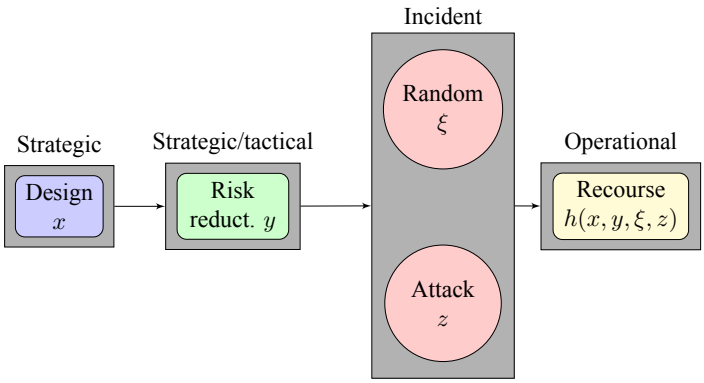
be predicted exactly, e.g., a natural disaster, is called a *random incident*. Each incident has a *likelihood* of occurring. An incident may cause the *failure* of an element.

There are several terms that we use to describe the effect that incidents and element failures have on a network. An *event* is an incident that degrades, causes the failure of, or destroys one or more elements. Not every incident is an event. Element *degradation* is the reduction in the performance of that element. A *disruptive event* is an event that reduces the performance of the network. The *consequence* of an incident is the amount of damage and performance decrease it causes. A consequence may be in regard to an element, element group, or in regard to the entire network. The *worst-case consequence* is the largest consequence possible. The term *recourse* refers to the decisions and actions taken in response to a disruptive event.

Several common terms exist to describe the performance of networks under the risk of disruptions. The *vulnerability* of an element or element group is its susceptibility to degradation or failure given that an incident occurs. The vulnerability of a network is its susceptibility to events. The *failure* probability of an element is the element vulnerability multiplied by the likelihood of an incident. The *risk* to a network is defined as the potential for a disruptive event and is a function of likelihood, vulnerability, and consequence. The *robustness* of a network is its capability to perform well under the occurrence of incidents. Network *reliability* is the probability that a network performs its intended function for a given amount of time under the occurrence of incidents. Network *survivability* is a measure of how many events a network can withstand before it cannot perform its intended function. The *resilience* of a network is its ability to be restored after an incident.

Some networks are subject to terrorist attacks. In this situation there are two players: the *defender*, who wishes to employ various risk reduction strategies, and the *attacker*, or *interdictor*, who seeks to inflict damage on the network. If the attacker's desired action depends on the defender's action, then the attacker is an *adaptive*, or *strategic attacker*.

Figure 1 Network problems with disruptions: problem stages (see online version for colours)



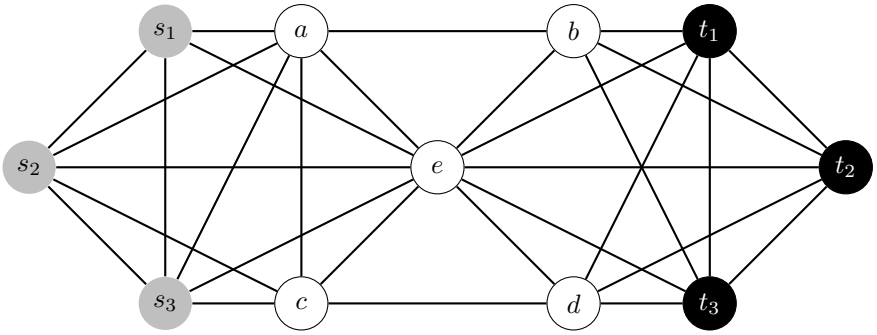
To aid the reader, we also provide a mathematical framework for studying disruption problems, shown in Figure 1. Consider a system characterised by a function h that measures its operational performance. Also, let ξ represent a random incident and z an incident due to an intentional attack. Before the disruption occurs, suppose the network

is designed by a defender. Let x be the design decisions. These decisions are typically long-term and are said to be strategic decisions. Similarly, rather than designing a new system, the defender may wish to use various risk-reduction strategies, such as hardening parts of the network or adding redundancy. Risk reduction strategies, denoted by y, may be strategic, such as adding redundancy, or tactical, such as some counter-terrorism decisions. The last stage is the recourse stage, where decisions are made to minimise the consequence of the disruption. These decisions are constrained by the state of the network resulting from the disruptive event in the previous stage. Often, the problems that occur in this stage are classic logistical optimisation problems such as the shortest path and maximum flow problems (see Ahuja et al., 1993). The expected recourse function $h(x, y, \xi, z)$ represents the expected post-disruption performance as a function of design and risk-reduction decisions. The decisions made in this stage are operational, such as choosing how goods should flow through the network.

2.2 Classification scheme

Papers in this survey are classified according to three characteristics: system type, risk measure, and risk reduction strategy. This section distinguishes between each of these types.

Figure 2 Source-sink network



2.2.1 System type

The four system types that we consider are sets of elements, graphs, source-sink networks with source failures (SSNSF), and source-sink networks with intermediate node or edge failures (SSNINF). The *set of elements* system is not a network but is a set of independent elements. These elements may represent a set of landmarks that a defender is interested in protecting against attacks. *Graphs* are made up of nodes and edges. Graphs are generic structures and are not suited for modelling features that are specific to a particular problem or application area. A *source-sink network* is different from a graph because it can better model application specific features. One characteristic that distinguishes a network from a graph is that a network usually has acommpanying data (e.g., edge weights) while a graph consists of generic nodes and edges. Figure 2 shows a source-sink network, which is composed of sources s_1, s_2, s_3, intermediate nodes a, b, c, d, e and sinks t_1, t_2, t_3. This structure is usually used to model flow from

sources to sinks through the intermediate nodes. Models may include the failure of sources or the failure of intermediate nodes. Table 1 shows the different types of systems that we include.

Table 1 System types considered in this review

System type	*What fails?*	*Number of intermediate edges*	*Application*
Set of elements	Elements	n/a	US national monuments
Graph	Nodes or edges	n/a	The internet
Source-sink network: source failures	Sources	1	Supply distribution network in which suppliers are subject to labour strikes
Source-sink network: intermediate node failures	Intermediate nodes or edges	many	Transportation network with unreliable infrastructure

2.2.2 Risk measure

A model's risk measure is how it captures risk. Choosing the most appropriate risk measure for a problem involves assessing the decision maker's preferences and the source of risk, e.g., random or intentional attacks.

Some models assume that disruptions occur randomly. When both the likelihood of incidents and the vulnerability of elements are known (i.e., the failure probability is known), a popular measure of risk is the *expected value* (EV) of the recourse function, or the expected consequence. When only the vulnerability of elements is known, then a common risk measure is the *conditional expected value*, which is the expected consequence given that an incident occurs. This measure does not require likelihood values. Other models measure risk as the worst case consequence out of all possible outcomes. We call this the *relative worst case* (RWC). This may capture the preferences of a risk averse decision maker. This approach is attractive because it does not require estimation of likelihoods, which is often difficult. Snyder and Daskin (2007) discuss other risk related modelling frameworks such as minimising expected cost while bounding the cost for a scenario, minimising absolute regret (Snyder and Daskin, 2006), and others.

Other models consider that disruptions occur due to attacks by an attacker. While an attacker can be modelled as a static threat, several researchers have argued that this is not the correct approach (Bier et al., 2009; Hausken, 2002). They argue that the attacker should be modelled as being adaptive to the defender's decisions, using game theory. Because the attacker searches for the strategy that results in the maximum damage, the attacker's disruption is the same as the worst case disruption. We refer to the risk measure used to represent an attacker as the *absolute worst case* (AWC) because it is the worst case disruption that can happen to the network given a constraint on the attacker's resources.

Several other risk measures have also been used. In this paper we also consider the *survivability* and *robustness* risk measures, which were both defined in Section 2.1. Some papers measure risk using a *risk metric*, which is a proxy for the true risk measure.

Each of the risk measures mentioned in this paper may either appear in the objective function or as a constraint. Additionally, some models measure risk as a combination of risk measures.

2.2.3 Risk reduction strategy

Finally, we classify papers by the risk reduction stragies that they employ. We classify these strategies into nine categories: vulnerability reduction, likelihood reduction, failure probability reduction, element consequence reduction, redundancy, rewiring, restoration, increasing attacker's cost, and informational measures.

Vulnerability reduction strategies attempt to reduce the likelihood that an incident becomes an event or a disruptive event. One common way of doing this is by *hardening* elements. The term *fortification* is synonymous with hardening in the literature. The hardening decision is typically represented as a binary variable and if a facility is hardened it cannot fail. Some authors have modelled the vulnerability of an element as a function of the amount of defense resources allocated. Related to this approach is the *contest success function* (Skaperdas, 1996), which is often used in the economics literature to model conflicts between players. Using a contest success function, the vulnerability of an element is expressed as a function of both the defender's allocation of protection resources and the attacker's allocation of resources. Contest success functions usually have some sort of contest intensity parameter that determines the form of the function.

Likelihood reduction strategies attempt to reduce the likelihood of an incident. Since it is difficult to affect the likelihood of natural disasters, these approaches usually involve preventing terrorist attacks and unintentional made-made incidents. Examples include investment in border defense, counter-terrorist operations, and intelligence (Powell, 2007b). Likelihood reduction has been modelled as a continuous function of the resource investment, which we call *continuous likelihood reduction*, as well as a discrete function, where elements are protected at different levels, which we call *discrete likelihood reduction*.

Another common approach is to model the reduction of the failure probability which we call *failure probability reduction*. This category includes *continuous failure probability reduction* and *discrete failure probability reduction*.

Several other strategies have also been modelled. One of these is *element consequence reduction*, or reducing the consequence of an incident. If failures are modelled as capacity degradation rather than complete failures, one approach is to invest resources to reduce the amount of degradation that occurs given a disruptive event. Adding *redundancy* to the network is another way to reduce the risk of the network and make it more robust. This can be done by adding new elements and increasing the capacity of existing components. *Rewiring* involves modifying the network without adding components to reduce the risk of the network. *Restoration* measures attempt to reduce the consequence of a disruptive event by allocating resources to increase network restoration capacity. Another method of reducing the risk of a network involves taking measures to *increase the cost* or effort required by the attacker to attack the network. *Informational* measures involve the use of information or the withholding of information to thwart would-be attackers. Strategies include secrecy, deception, signaling, the use of false targets, as well as increasing the accuracy of the defender's information. Finally, some papers consider combinations of the above approaches and several papers consider tradeoffs between approaches.

Figure 3 Classification diagram

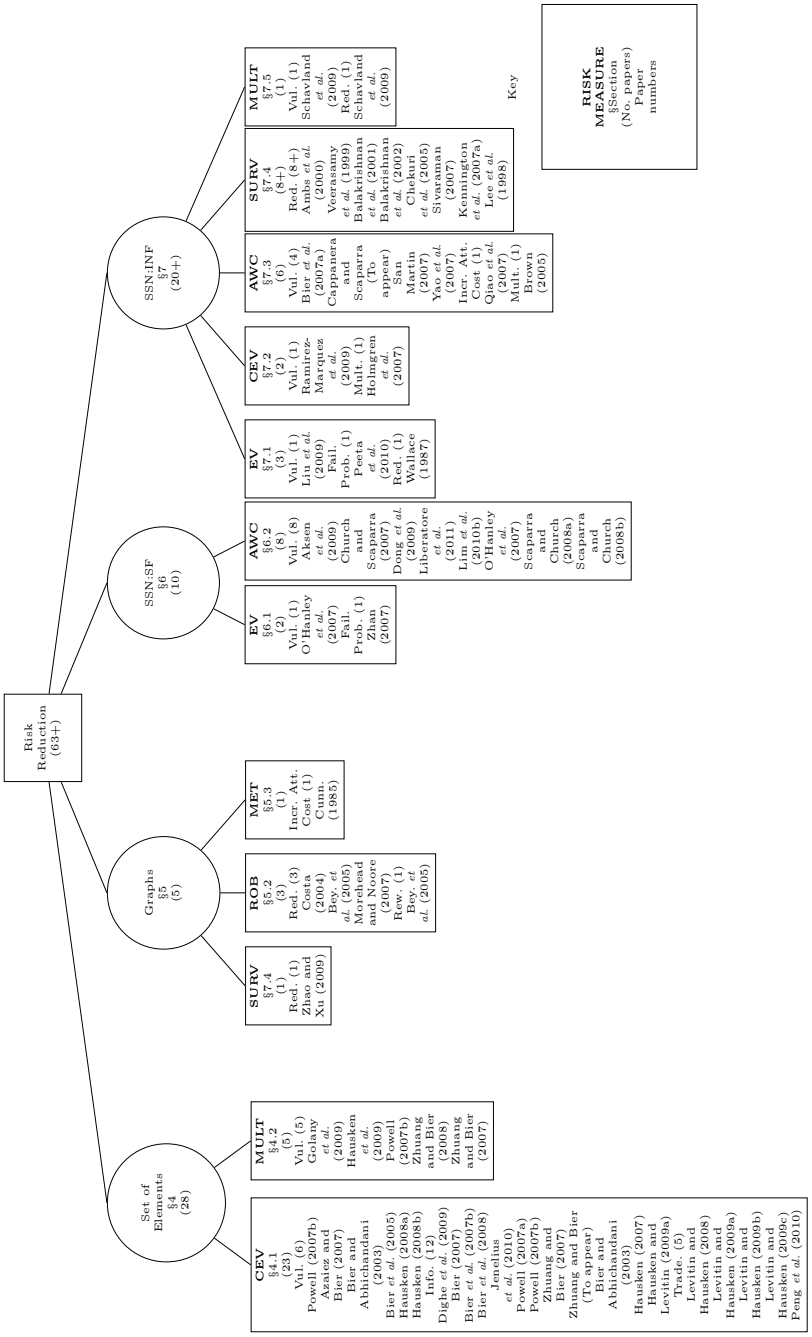


Figure 3 shows a tree diagram describing the organisation of this paper. The leaves of the tree represent the different categories into which the papers in this review are organised. The first row of the tree after the root node classifies papers by the type of network considered. The second row represents the risk measure considered in the paper; the risk measures listed are EV, conditional expected value (CEV), RWC, AWC, survivability (SURV), robustness (ROB), risk metric (MET), and multiple risk measures (MULT). The nodes in the second row after the root contain the number of papers in the category as well as the bibliographic entries of each of the papers in the category. The papers within the nodes in the second row are also categorised by the risk-reduction strategy taken in the paper. These strategies include failure probability reduction (fail. prob.), vulnerability reduction (vul.), redundancy (red.), increasing the cost of attack (incr. att. cost.), rewiring (rew.), multiple strategies (mult.), and a tradeoff between strategies (trade.) When papers consider multiple strategies separately in the same paper, we consider each strategy considered to be a separate paper for the purpose of counting the number of papers for each risk reduction strategy. However, we count it as one paper when counting the number of papers for each risk reduction measure. Again, we left out all of the categories that did not have any papers in them. A category may not have any papers because either the category is not relevant or because the category is truly a gap in the literature. The categories without any papers are discussed in Section 8.

2.3 Scope

The strategy of this paper is to review different approaches for mitigating against the risks to networks. All of the papers reviewed are analytical in nature and primarily deal with operations research models.

We also limited our search to articles that considered the system-wide impact of disruptions. That is, we consider systems of elements where the overall performance depends on the state of all of its elements. Thus, we did not review work that studies local consequences such as lives lost, repair costs, etc. There has been a lot of work done in areas such as risk analysis studying the local impacts of disruptions.

Finally, in this paper we consider large scale disruptions as opposed to disruptions due to wear and tear. However, we acknowledge that there is a fine line between these two sources of disruptions.

3 Descriptive models

In this section, we discuss descriptive models, or those that describe or analyse the changes in system performance that result from disruptions. Because of the existence of surveys and books on this topic, the purpose of this section is to raise key points that will be useful in the exposition of the remainder of this paper and to refer the reader to useful references.

3.1 Network vulnerability assessment

Many methods for assessing the risk and vulnerability of networks have been developed and refined. This work is relevant to this survey because an effective risk mitigation effort usually depends on an effective risk assessment. Sullivan et al. (2009) provide a helpful categorisation and discussion of the literature on network disruption

analysis, focusing on analysing network vulnerability and reliability. Murray et al. (2008) and Grubesic et al. (2008) categorise and survey approaches for assessing network vulnerability. They categorise vulnerability assessment into four approaches: scenario-specific, simulation, strategy-specific, and mathematical modelling.

3.2 Network science

A field called network science has recently been attracting many researchers from many disciplines. Alderson (2008) has written a helpful introduction into this area from an operations research perspective. The basic objective of this area is to develop models that describe the random and decentralised growth of networks. Prevalent models include random networks (Erdos and Renyi, 1959), small-world networks (Watts and Strogatz, 1998), and scale-free networks (Barabasi and Albert, 1999). Scale-free networks exhibit a hub-and-spoke structure, where a small number of nodes have a high degree. Small-world networks are characterised by a small average shortest path length between nodes and a high amount of node clustering.

There has been considerable interest in assessing the vulnerability of network science models to specific attack strategies. The vulnerability of these networks is measured as the change in a network efficiency measure, such as the length of the average shortest path, resulting from an event. In particular, researchers have found that scale-free networks, which model networks such as the world-wide web, have a high survivability or robustness against random incidents, but a low survivability and robustness against intentional attacks (Albert et al., 2000; DallAsta et al., 2006). The metrics for survivability and robustness typically involve some measure of network connectivity. This body of literature is discussed further in Grubesic et al. (2008).

3.3 Interdiction models

The AWC consequence is often measured using an interdiction model, where a strategic attacker seeks to inflict maximal damage on a network. Thus, models that prescribe an attacker's optimal strategy can also be used as descriptive models for measuring the AWC consequence. Models have been presented for the interdiction of facilities (Church et al., 2004), shortest path networks (Israeli and Wood, 2002), and maximum flow networks (Wood, 1993). Smith (2011) provides a basic introduction to interdiction models and Smith and Lim (2008) present a more extensive discussion. Church et al. (2004) categorise interdiction studies (see Table 1 in their paper).

3.4 Infrastructure interdependencies

Most of the existing work on critical infrastructure risk has studied isolated networks. However, many infrastructure networks are interdependent due to their physical proximity or because they depend on each other functionally (Zimmerman, 2004). Buldyrev et al. (2010) describe an interdependent network as a system of two or more networks where the failure of an element in one network may result in element failures in another network.

A phenomenon called cascading failures occurs when an element failure in one infrastructure system leads to an element failure in another infrastructure system. The consequences of the entire series of cascading failures is often much higher than the magnitude of the initial disruption (e.g., the 2003 Northeastern US blackout).

Zimmerman and Restrepo (2006) presented a metric to quantify the magnitude of cascading failures and applied their metric to several power grid disruptions.

A related research area focuses on developing infrastructure input-output models, which capture the inter-dependencies between infrastructures (see Santos (2006) for example). This differs from the topics that we cover in this survey because input-output models are concerned with economic infrastructure while we are more concerned with physical infrastructure.

3.5 Other

Church and Scaparra (2006) present a novel approach for graphically displaying the reliability of a system subject to an interdictor, called a reliability envelope. The reliability envelope is a plot of system efficiency after a disruptive event versus the magnitude of the event. For each system disruption magnitude, the decision maker can see the best case consequence, the worst case consequence, and the difference between the two, giving the decision maker a broader description of the risk to the system.

4 Set of elements

In this section we review papers that consider the set of elements system. Set of elements models usually mimic a simultaneous resource-allocation game between a defender and an attacker. Each element may be either operating or destroyed. The probability that an element is destroyed is a function of the resources that the defender invests towards protecting it and the attacker invests towards destroying it. If the element is destroyed the attacker receives a reward equal to the value of the element. The elements are modelled as a set and not separately because each player must decide how to allocate his or her resources amongst the entire group of elements.

Two objectives have been considered in these models. The first objective is to minimise the total reward received by the attacker. We refer to this objective as the *total reward* objective. Another type of objective considers that an attacker may also receive a reward for destroying the entire system. The system state (operating or destroyed) is a function of the states of its elements. Several system state functions have been examined. If a *series function* is used, the system is in the operating state if and only if all of its elements are in the operating state. When a *parallel function* is used, the system is in the operating state if at least one its elements are in the operating state. Other more complicated system state functions have also been used. Objectives that consider a reward for destroying the entire system are called *system state* objectives in this paper.

4.1 Conditional expected value risk measure

Almost all of the research on reducing the risk associated with a set of elements has considered the CEV risk measure. This is because set of elements models usually consider a game between a defender and attacker that takes place after the attacker has decided to make an attack. These models usually do not consider the likelihood that an attacker makes an attack.

4.1.1 Vulnerability reduction

The most popular risk reduction strategy is to reduce the vulnerability of elements in the set. The vulnerability of an element is usually modelled as a function of the resources invested by both the defender and the attacker.

Vulnerability reduction with total reward objectives has been modelled using contest success functions (Hausken et al., 2009; Levitin and Hausken, 2008, 2009a; Peng et al., 2010; Zhuang and Bier, 2008, to appear), a function of defense resources allocated (Bier et al., 2007b, 2008; Bier, 2007; Jenelius et al., 2010; Powell, 2007a; Zhuang and Bier, 2008), and hardening (Dighe et al., 2009). However, the purpose of most these papers is to examine the efficacy of other measures such as informational measures, rather than to examine the efficacy of vulnerability reduction. Thus, we also discuss these papers in other categories within this section.

Powell (2007b) takes an interesting look at vulnerability reduction using a total reward objective. He presents a model that allows the defender to allocate protection resources between counter-terrorism, which reduces the vulnerability of all elements, and the vulnerability reduction of specific sites.

Other papers have considered system state objectives. Bier and Abhichandani (2003) consider the defense of both series and parallel functions where the defender allocates protection resources to network elements to protect against an attacker that has the objective of maximising his success probability. Conversely, the defender has the objective of minimising the attacker's success probability. Bier et al. (2005) consider the same problem as in Bier and Abhichandani (2003) except that the attacker now wishes to maximise the expected damage of an attack, rather than the probability. These papers model vulnerability as a function of the defense resource allocation. The attacker attacks the element that has the largest attack utility, typically the one with the largest vulnerability. Azaiez and Bier (2007) extend the work of Bier and Abhichandani (2003) by modelling the protection of a combined series/parallel function where the defender allocates resources to maximise the cost to the attacker of the defender's worst case attack.

Hausken (2008a) tries to determine the type of system state objective preferred by the defender. He provides models for defense against a strategic attacker for both series and parallel functions using a contest success function to model vulnerability. Hausken (2008b) extends this work to an arbitrarily complex series/parallel network with the goal of determining whether the defender prefers a parallel-series network or a series-parallel network. He found that when everything else is equal, the defender prefers a series-parallel network.

4.1.2 Informational

Several articles have measured the effectiveness of informational strategies with total reward objectives such as hiding the defender's resource allocation from the attacker and intentionally giving the attacker wrong information. Dighe et al. (2009) present a model where the attacker knows how many allocations are made but does not know the particular allocations. They find that partial secrecy is preferable to full disclosure for the defender. Zhuang and Bier (to appear) examine three disclosure strategies: truthful disclosure, secrecy, and deception and find that all three strategies may be present at equilibrium. Other papers have modelled situations where the defender does not have perfect information about the attacker. Bier and others

(Bier, 2007; Bier et al., 2007b, 2008) present a model where a defender protects a collection of elements against an attacker who wishes to attack a single element. The defender only knows the probability distribution of the attacker's preferences. In this model, the authors find that the defender prefers his allocation to be made public. Most of the work on protection networks assumes that the attacker has perfect information. Jenelius et al. (2010) relax this assumption and provide a model that assumes that the attacker observes the utilities for attacking particular elements with random observation errors. They find that if the defender falsely assumes that the attacker has perfect information, the defender's allocations could yield significantly suboptimal results. Powell (2007b) also looks at this problem, assuming that the defender has uncertainty about which attacker he or she will face but knows that only two types of attackers are possible.

Another important problem characteristic relating to informational strategies with total reward objectives is the sequence in which the two agents act. The agents may play a simultaneous game where neither agent has any information about the other agent's actions. Also, a two-period game may take place where the attacker makes decisions after the defender. In this situation, the attacker may or may not have information about the defender's actions. Zhuang and Bier (2007) and Bier et al. (2007b) show that under certain assumptions, when the defender is able to hide information from the attacker, he or she has a first-move advantage in a sequential game. Powell (2007a) studies this same situation, focusing on the fact that the defender's allocation sends a signal to the attacker about which elements the defender values. This type of game is called a signaling game. This game is modelled using a mathematical model that analyses the tradeoff that the defender makes between protecting her most valuable elements and avoiding the sending of signals.

Other papers have considered informational strategies using system state objectives. Bier and Abhichandani (2003) and Hausken (2007) provide results that indicate that secrecy, deception, or both may be effective strategies for the defender. Hausken and Levitin (2009a) present a model where the defender allocates resources between protecting existing elements and deploying false elements.

4.1.3 Tradeoff between strategies

Naturally, some researchers have developed models that not only prescribe an allocation of resources but also prescribe an optimal tradeoff between multiple risk reduction strategies. Several papers have examined this tradeoff and share a number of common traits in how they model the problem (Levitin and Hausken, 2008, 2009b, 2009c; Peng et al., 2010). First, they each consider total reward objectives. The objective of the network is to meet a demand so that the reward received by the attacker is the cost of unmet demand. Second, it is assumed that the defender distributes her resources evenly amongst all or some of the elements. Third, the attacker chooses a subset of elements to attack and distributes his resources evenly amongst them. Fourth, a contest success function is then used to model the element vulnerability. Each of these papers models a different tradeoff between two or more risk-reduction strategies. Peng et al. (2010) present a model where the defender allocates resources between protecting existing elements and deploying false elements. They also consider that false elements can be detected to be false by the attacker with a specified probability. Levitin and Hausken (2009a) model the situation where a defender allocates resources between building new elements and protecting the built elements. Levitin and Hausken (2008, 2009b) allow the

defender to allocate resources between deploying genuine elements and deploying false elements. As a natural extension to the above tradeoffs, Levitin and Hausken (2009c) allow the defender to trade off between protection, redundancy, and deploying false elements.

4.2 Multiple risk measures

Researchers have begun to study how to allocate protection resources when multiple sources of risk are present. Specifically, they have looked at the difference between defending against random incidents (e.g., natural disasters) and strategic attacks.

Golany et al. (2009) compare the optimal policies for defending a network against probabilistic failures to the optimal policies for defending against a strategic attacker. For both models, the element vulnerabilities are a function of resources allocated by a defender. The objective in the probabilistic case is to minimise the expected value and the objective in the strategic attacker case is to minimise the worst case consequence. They found that the best protection solution against probabilistic attacks involves protecting the elements that received the greatest impact from protection. In contrast, in protecting against a strategic attacker, it is best to allocate protection resources to reduce the maximum vulnerability over all elements.

Several researchers have begun to develop models that prescribe optimal resource allocations while considering multiple risk measures. Hausken et al. (2009) present a model that allows the defender to tradeoff between investing in resources for protecting against terrorism, protecting against random failures, and protecting against both (all hazards protection). The objective of their model is to minimise the conditional expected value and they use a contest success function to model vulnerability. Zhuang and Bier (2007, 2008) present a model where a single defender chooses how to balances resources between defending against probabilistic failures and defending against strategic attacks.

The objective of their model is to minimise the CEV. They use a function similar to a contest success function to model vulnerability to strategic attacks and use a function of defender resource allocation to model probabilistic incident vulnerability. Powell (2007b) also studied how to allocate resources to protect against a threat that has both a strategic and a non-strategic component.

5 Graphs

Another area of research involves representing a system as a graph. These studies usually consider how to reduce the risk of disruptions in order to preserve graph theoretic properties such as connectivity and average shortest path. Overall, this work studies how to improve various measures of risk for descriptive growth models produced by network science researchers (see Section 3.2).

5.1 Survivability risk measure

Since survivability is an important risk measure that is studied using network science models (Albert et al., 2000), it makes sense to examine how to improve survivability. Zhao and Xu (2009) studied the effect of adding edges on the survivability of scale-free networks. Survivability is defined as the number of node removals that a network

can endure before it becomes disconnected. Two types of node removals are analysed: random removals and removals of the nodes with the highest degree.

5.2 Robustness risk measure

Researchers have also tried to find ways to improve the robustness of various descriptive models in network science. These studies share a common organisation. First, they usually define robustness as the effect that node removals have on the networks. Nodes are either removed randomly or according to a heuristic rule such as highest node degree. The effect of node removals is measured using some metric of connectivity (Costa, 2004; Beygelzimer et al., 2005; Morehead and Noore, 2007) or metric related to the shortest path distances between nodes (Beygelzimer et al., 2005). Second, these studies seek examine the benefit of various risk reduction strategies such as adding additional edges to the network (Beygelzimer et al., 2005; Costa, 2004; Morehead and Noore, 2007), called augmentation, and rearranging the placement of existing edges, called rewiring (Beygelzimer et al., 2005). Augmentation and rewiring are done randomly or according to a heuristic rule.

5.3 Risk metric

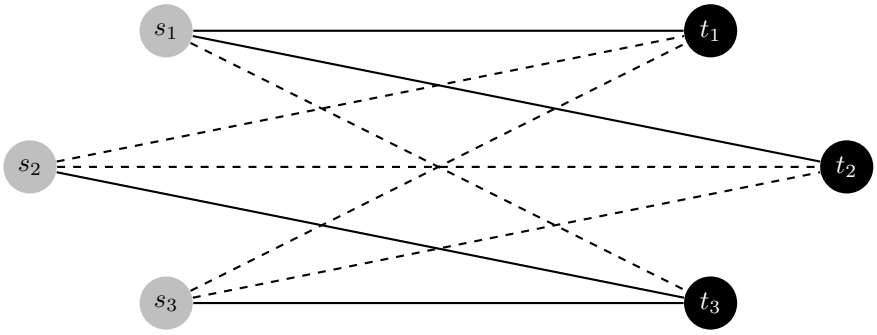
Another way to model the risk reduction of a graph is to use a risk metric, or a proxy for risk. Cunningham (1985) considers a risk metric called the 'strength' of a graph, which is a measure of the cost of edge removals over the number of disconnected subgraphs resulting from the edge removals. Two models are presented: one in which a defender maximises the strength of the graph by increasing the edge attack costs subject to a budget constraint and another where the defender minimises cost subject to a lower bound on the strength of the graph. In addition to edge removals, the problem of removing nodes is also considered. This study is applicable to any network and therefore does not require many of the assumptions made in the network science literature (e.g., graph is sufficiently large and sufficiently homogeneous).

6 Source-sink networks: source failures

In this section we review articles that model source-sink networks with node failures (SSNSF). These networks have a few characteristics that are important to modelling. First, when a source fails, a sink must be served by another source. Second, because intermediate nodes and edges do not fail, the shortest path of intermediate nodes and edges will always be taken from a source to a sink. Therefore, the path between a source and a sink may be represented by a single new edge between the source and sink, with length equal to the length of the shortest path between that source and sink. The resulting network is a bipartite graph. Figure 4 shows a hypothetical source-sink network with source failures. The solid lines represent assignments from sources to sinks. The dashed lines represent backup assignments. For example, if source s_1 fails, sink t_1 would be served by source s_2 or s_3.

Most of the articles in this section consider that the sources represent facilities and the sinks represent customers. Thus, in this section we use the term 'facility' instead of 'source'.

Figure 4 Source-sink network with source failures



6.1 Expected value

We only found two papers that study SSNSF with the EV risk measure; in fact, only one of them, O'Hanley et al. (2007), has appeared in a refereed journal.

6.1.1 Failure probability reduction

In a recent dissertation, Zhan (2007) presented two non-linear models for the p-median problem with unreliable facilities and fortification. The objective is to minimise the sum of the expected transportation cost and the unmet demand penalty cost. Zhan (2007) also presents a model for continuous failure probability reduction and shows that it is a special case of the generalised linear multiplicative programming problem (GLMP) (see Ryoo and Sahinidis (2003) for more details). To solve the model, the vertex enumeration method (Horst et al., 2000) is used. Zhan (2007) also presents a mixed-integer non-linear programming (MINLP) model for discrete fortification. Because the objective function of this model is monotonically non-decreasing, it can be solved by a monotonic branch-reduce-bound algorithm developed in Zhan (2007).

6.1.2 Vulnerability reduction

O'Hanley et al. (2007) study the hardening version of the maximum expected covering location problem (MEXCLP) (Daskin, 1983) in the context of biological conservation, which we denote as the maximum expected covering location problem with hardening (MEXCLPH). The problem is to choose a set of sites to denote as reserve sites, which is equivalent to hardening the sites. Each site contains a population of various wildlife species and has a nonidentical probability of failure. A reserve site cannot fail. A species is left unprotected (uncovered) and becomes extinct if all of the sites that it inhabits are disrupted. The objective is to minimise the expected weighted loss of species, equivalent to minimising the expected number of uncovered customers. They refer to their problem as the minimum expected coverage loss problem (ECL). The authors model this problem like the maximum covering location problem (MCLP) (Church and ReVelle, 1974) but add an additional weight (the probability of species survival) to the objective function, resulting in a model that has the same structure as the classic MCLP. The multi-period version of this problem is also studied, where the probability that a species is exterminated is a function of the number of periods it is left unprotected. This problem is modelled as an EV problem [see Birge and Louveaux (1997) for details].

6.2 AWC risk measure

Most of the work in source-sink networks with facility failures has considered the AWC risk measure. These models fall into the general defender-attacker-defender category of models (Brown et al., 2005).

6.2.1 Vulnerability reduction

A majority of the work relating to source failures has studied hardening. All of the papers in this section discuss a hardening extension of the r-interdiction median problem (RIM) (Church et al., 2004; see Section 3.3 of this paper) called the r-interdiction median problem with fortification (RIMF). If exactly q facilities can be fortified then the problem is the r-interdiction median problem with q-fortification (RIMQF). This model involves a game against an interdictor subject to a budget constraint that wishes to maximise the total cost of satisfying customer demand. It is assumed that both the defender and attacker have perfect information.

Church and Scaparra (2007) present a MIP model for the RIMQF that minimises the maximal cost over all possible interdiction scenarios, or all possible ways to interdict r out of p existing facilities. To reduce the size of their model, the authors utilise some properties of the problem to remove unnecessary variables and constraints. Additional variables are consolidated using ideas from the condensed Balinski constraints with the reduction of assignment variables (COBRA) formulation of the p-median problem (Church, 2003).

Scaparra and Church (2008b) reformulate the RIMQF model presented in Church and Scaparra (2007) as a maximum covering problem, which enables them to overcome some of the computational challenges of the previous model. Their model essentially tries to prevent the set of interdiction scenarios that result in the biggest impact. They then show how heuristics can be used to obtain bounds, which reduce the size of their model. The approach in this paper is flexible because it can handle any underlying model (e.g., covering problem) for which the evaluation of interdiction patterns can be done in polynomial time. This differs from the RIMQF model presented in Church and Scaparra (2007), which is tailored to the structure of the p-median problem.

Scaparra and Church (2008a) present a bilevel MIP formulation of the RIMQF. They provide an implicit enumeration (IE) algorithm to solve the problem and use properties of the problem to reduce the size of the IE tree. Since a RIM problem is solved at each node in the tree, the authors present a streamlined formulation of the RIM and utilise variable consolidation (see Church, 2003) and closest-assignment constraints. The results demonstrated computational improvements over the maximal covering approach in Scaparra and Church (2008b).

Several extensions have been made to the basic RIMQF. One of the limitations of the RIMQF is that it assumes that r, the number of disrupted facilities, is known. Liberatore et al. (2011) present a stochastic version of the RIMQF, where only the probability distribution of r is known to the defender. They present a maximum covering type formulation that is similar to the formulation in Scaparra and Church (2008b). Bounds are developed to reduce the size of the model and three heuristics are developed to solve the problem. Results show that when r is random it is important to model it as such. Aksen et al. (2009) study the RIMF with a knapsack budget constraint on the fortification resources. They also allow facilities to purchase extra capacity prior to an incident to accommodate customers who migrate from another failed facility. This

is termed ‘flexible capacity’. They present a bilevel MIP model with added closest assignment constraints. The model is solved using an IE algorithm. Dong et al. (2009) study a modified version of the RIMQF where the objective is to maximise the worst case minimal time satisfaction over all customers. The time satisfaction for a customer is assumed to be a linear, convex, or concave function of the distance to its assigned facility (Ma and Wu, 2006). They show that accounting for time satisfaction in the objective function results in significantly different solutions.

O’Hanley et al. (2007) also considered a worst-case version of the MEXCLPH. Rather than minimising the expected species loss, the objective is to minimise the worst case species loss. The interdiction budget is in the form of a constraint on the probability of the occurrence of the disruption. A bilevel MIP model is presented for this problem.

7 Source-sink networks: intermediate node failures

In this section we review papers that study source-sink networks with intermediate node failures (SSNINF). Because intermediate nodes fail, source-sink paths cannot usually be represented effectively by a single edge as with source-failure models. Rather, the entire network of intermediate nodes and arcs must usually be modelled explicitly as shown in Figure 2. As a result, problems with intermediate node failures are usually harder than problems with source failures. In this section we only refer to intermediate node failures because an intermediate node failure model can easily be transformed to a intermediate edge failure model (see Corley and Chang, 1974).

The literature on SSNINF networks is more developed than the research on SSNSF networks; however, there is also a lot of room for future research on SSNINF networks.

7.1 Expected value risk measure

Perhaps because SSNINF networks are more difficult to model than their source-failure counterparts, all of the papers in this section used two-stage stochastic programming models rather than single stage MIP models, which are common for SSNSF models.

7.1.1 Failure probability reduction

Peeta et al. (2010) presented a two-stage stochastic programming model for reducing the risk of transportation networks with bridges that are prone to failure. A discrete failure probability reduction approach is presented that reduces the failure probabilities for bridges in the network. The recourse problem is a capacitated minimum cost network flow problem. The Taylor series expansion of the objective function is used to reformulate it as a multi-linear function and sample average approximation approach [see Birge and Louveaux (1997) for details] is used to solve the reformulated model.

7.1.2 Vulnerability reduction

Liu et al. (2009) presented a two-stage stochastic programming model for the problem of hardening bridges within a transportation network discussed in Peeta et al. (2010) with the objective of minimising the expected travel time. Because of their assumption that the travel time for an arc depends on the flow through that arc, they model the second stage problem as a convex multicommodity flow problem. To account for the

non-linear second stage, they use an extension of the L-shaped method that utilises the concepts of generalised Bender's decomposition.

7.1.3 Redundancy

Wallace (1987) considered adding redundancy to networks to reduce their risk. Specifically, he presented a model for increasing the capacity of arcs in a network with the objective of maximising the expected maximum flow subject to random failures. It is demonstrated that this problem can be formulated as a two-stage stochastic programme with network recourse, for which specialised solution approaches exist (see Birge and Louveaux, 1997).

7.2 Conditional expected value risk measure

Two researchers have developed models for the failure of intermediate nodes that are similar to the models developed for sets of elements (see Section 4).

7.2.1 Vulnerability reduction

Ramirez-Marquez et al. (2009) presented a model for protecting a network against an attacker that distributes his resources evenly among all elements. The objective is to maximise the expected maximum flow. The defender chooses a subset of arcs to defend and then distributes his resources evenly amongst them. The vulnerability of each arc is modelled using a contest success function. Since the attacker allocates a positive amount to each arc, any unprotected arc fails. They use an evolutionary algorithm to identify protection allocation solutions and Monte Carlo simulation is used to evaluate candidate solutions.

7.2.2 Multiple strategies

Holmgren et al. (2007) presented a model that includes protection as well as restoration as strategies to reduce the risk to an electrical power grid. The recourse problem is a time-dependent maximum flow problem that captures the time to restore the network after a disruption. Thus, the consequence of a disruptive event is a function of its duration. In this problem, the vulnerability of an element is a function of the defender's allocation of protection resources. The defender may also allocate resources to recovery, affecting the repair time. A tradeoff is made between these two options. Three different attacker strategies are examined:

1 maximise expected negative consequences

2 maximise the probability that a negative consequence is above a threshold

3 choose targets randomly.

The model is used to generate the best protection strategy for each attack scenario. However, the authors do not suggest a way to generate protection strategies that perform well against several attack scenarios. The approach is demonstrated on a Swedish power network.

7.3 Absolute worst case risk measure

Like for source-failure models, a majority of the work on intermediate node failure models has used the worst case risk measure. These models also fit into the general defender-attacker-defender framework (Brown et al., 2005).

7.3.1 Vulnerability reduction

The vulnerability risk reduction strategy has so far been the most popular in the literature on intermediate node failures with the absolute case risk measure.

Two researchers have studied the problem of hardening a network to minimise the maximum shortest path. San Martin (2007) provides a specialised formulation and algorithm this problem. Computational results show that nested and reformulation-based decomposition algorithms to be twice as fast as direct decomposition. Cappanera and Scaparra (to appear) reformulate the hardening action as an attack cost increase action. They suggest an IE procedure to solve the problem.

Bier et al. (2007a) study the problem of defending a power network against a strategic attacker. When choosing a new element to attack, the attacker chooses the arc with the largest load. The defender and attacker are subject to a constraint on the maximum number of hardened edges and attacked edges, respectively. The defender's recourse problem is to minimise the total cost of distribution (load generation) and unmet demand (load shedding). A greedy algorithm is presented where the recourse problem, the attacker's problem, and the defender's problem are solved sequentially in a loop for a pre-specified number of iterations. In the attacker phase, the element with the largest flow is interdicted. In the defense phase, the defender hardens the elements that are most desirable to the attacker. The algorithm is demonstrated on the IEEE reliability test system one and two area networks (Grigg et al., 1999).

Yao et al. (2007) present an exact algorithm for a similar problem to that studied in Bier et al. (2007a). They use a delayed cut generation approach similar to Bender's decomposition. They also test their approach on the one area network used in Bier et al. (2007a).

7.3.2 Increase attack cost

Qiao et al. (2007) study the problem of allocating resources to a water supply network that is subject to an adversarial attack. The resource allocation increases the cost an attacker incurs to attack an element. They develop a model that maximises the minimal value of a risk metric over a set of element groups. The risk metric for an element group is defined as the cost incurred by the attacker to attack the element group divided by the consequence of the disruptive event associated with that element group. The set of element groups considered is the set of all subsets less than a predetermined maximum cardinality, which is the maximum number of arcs that an attacker may attack simultaneously. Due to the hydraulic constraints inherent in a water supply network, a simulation model is used to estimate the consequence of a component's failure. A genetic algorithm is used to solve the model.

7.3.3 Multiple strategies

Brown (2005) presents a time-indexed model for hardening and expanding the capacity of the links of an oil pipeline network against a strategic attack. The recourse problem

for each time period is essentially a maximum flow problem. In addition, attacks are also time-indexed.

7.4 Survivability risk measure

Another line of research has studied how to allocate spare capacity resources to an existing network to ensure its survivability in the presence of failures. This work is motivated by applications in the telecommunications industry. Problems in this area have been typically modelled as an MIP model with the objective of minimising the cost of spare capacity allocation subject to a constraint requiring that enough spare capacity exists so that flow can be rerouted in single-edge failure scenarios. Because this is a well established area, instead of listing all of the work done we refer the reader to a survey by Kennington et al. (2007b). Important articles in this area include: Ambs et al. (2000), Veerasamy et al. (1999), Balakrishnan et al. (2001, 2002), Sivaraman (2007), Kennington et al. (2007a) and Lee et al. (1998).

7.5 Multiple risk measures

A model developed by Schavland et al. (2009) included two risk reduction strategies and two risk measures. The authors consider both hardening and component capacity increases in protecting a network against an attacker using a multiobjective game theoretic model. The two objectives are to maximise network reliability as well as the worst case expected maximum flow.

8 Future work

We divide our discussion of possible areas of future work into three categories. First, we discuss areas of our classification that had few or no papers. Second, we identify important opportunities for integrating existing approaches. Third, we discuss new areas of research.

8.1 More work needed

To start, we mention the categories of our survey in which we did not find any papers. In our opinion all of the categories that did not have any papers in this review are worthy of some further thought.

Table 2 shows the number of papers studying various combinations of the system types and risk measures. The following risk measures are listed: EV, CEV, RWC, AWC, survivability (SURV), robustness (ROB), risk metric (METRIC), and multiple risk measures (MULT). The numbers show that the CEV risk measure is the most popular. The table also shows that few papers have considered multiple risk measures. More work is needed in this area because most real-world networks are subject to multiple types of risk. Of particular importance is the simultaneous consideration of random failures and strategic attacks.

Table 2 Risk measures used for each system type

	EV	*CEV*	*RWC*	*AWC*	*SURV.*	*ROB.*	*METRIC*	*MULT.*	*Total*	*%*
SofE	0	23	0	0	0	0	0	5	28	46%
Graph	0	0	0	0	1	5	0	0	6	10%
SSN:SF	2	0	0	8	0	0	0	0	10	16%
SSN:INF	3	2	0	6	4	0	0	2	17	28%
Total	5	25	0	14	5	5	0	7		
%	8%	41%	0%	23%	8%	8%	0%	11%		

Table 3 shows the number of papers studying various combinations of the system types and risk reduction strategies. The risk reduction strategies included are vulnerability reduction (VUL), likelihood reduction (LI), failure probability reduction (FP), element consequence reduction (ECR), redundancy (RED), restoration capacity (REST), rewiring (REW), increasing the attacker's cost (INCR), and informational measures (INFO). The last two columns represents papers that consider multiple approaches (MULT), or a tradeoff (TRADE) between multiple approaches, respectively. The statistics show that vulnerability reduction is the strategy of choice for a majority of papers. Many of the other strategies have received little attention. Because these strategies are viable for most problems, they are deserving of more study. The consideration of tradeoffs between multiple strategies has received little attention outside of the study of a set of elements. Because most decision makers have several strategies to consider when trying to reduce the risk of a network, tradeoff studies are an important area of future work.

Table 3 Risk reduction strategies used for each system type

	VUL	*LI*	*FP*	*ECR*	*RED*	*REST*	*REW*	*INCR*	*INFO*	*MULT*	*TRADE*
SofE	11	0	0	0	0	0	0	0	12	0	5
Graph	0	0	0	0	4	0	1	1	0	0	0
SSN:SF	9	0	1	0	0	0	0	0	0	0	0
SSN:INF	7	0	1	0	6	0	0	1	0	2	0
Total	27	0	2	0	10	0	1	2	12	2	5
%	44%	0%	3%	0%	16%	0%	2%	3%	20%	3%	8%

8.2 Integrating existing approaches

It may be possible to incorporate the work done in the risk analysis community on risk and vulnerability assessment into the risk mitigation methods reviewed in this paper. Also, in risk analysis and vulnerability assessment, the mitigation is done after the risk assessment, in sequence. However, since mitigation activities change the risk assessment, it may be beneficial to integrate these two activities.

Another interesting area of future work is to integrate the design and risk reduction decisions. In the context of locating unreliable facilities, Snyder and Daskin (2005) and Cui et al. (to appear) include perfectly reliable locations in their models, which can be though of as 'fortified' facilities. However, it is determined exogenously, or prior to solving the model, which facilities are perfectly reliable and hence risk reduction is prescribed by the model. Lim et al. (2010a) present a model where the decision maker chooses between locating unreliable facilities and reliable 'backup' facilities, which cost more. However, their model assumes that if a demand point's primary facility fails,

the demand point is then assigned to its perfectly reliable backup. There are two ways in which this assumption may not hold in reality. First, it is likely that if a demand point's primary facility fails it will then be assigned to the next closest open facility, rather than going directly to a reliable backup. Second, this assumption allows for a facility to be assigned as one demand point's unreliable primary facility and another demand point's perfectly reliable backup. In some situations this may not be a satisfactory assumption, especially if the demand points require the same commodity type. Thus, this paper takes an approach to risk reduction that is different to the papers mentioned in Section 6.

Finally, it would be interesting to see if the insights generated from set of elements models also apply to the source-sink networks. For example, is secrecy still valuable to the defender when defending a source-sink network?

8.3 New research areas

Many of the models in this paper consider random incidents. The drawback of the random incident approach is that its results are dependent on likelihood and vulnerability information, which is often difficult to obtain. As a result, it would be useful to know how sensitive these models are to the likelihood and vulnerability estimates. If these models are indeed sensitive to their inputs, it would be useful to have models that produce solutions that are robust to likelihood and vulnerability inputs.

In addition, more work is needed that considers correlated random failures. All of the random incident models that we found considered element failures to be independent. This assumption is not realistic in modelling natural disaster risk because multiple elements are affected by a single incident, making element failures correlated.

The papers that study risk reduction of an independent set of elements in Section 4 consider several aspects in their model that have not been studied for source-sink networks. These aspects include:

1 the attacker's resources are known with certainty to the defender

2 attacks are successful 100% of the time

3 elements are either completely protected or not protected at all.

While Liberatore et al. (2011) addressed (1), it would be useful if assumptions (2) and (3) were considered in more complicated systems such as source-sink networks.

Also, models that consider multiple decision makers are needed. Most of the papers in this survey assume a single decision maker such as a private company. However, the management of most public infrastructures involves multiple stakeholders. It is possible that the decisions generated by single-decision-maker models are not satisfactory for all of the stakeholders involved.

In addition, more multi-objective models are needed. Most of the papers that we reviewed considered only one objective. However, many decision makers are interested in multiple objectives, e.g., risk and cost. Models that are able to develop Pareto efficient curves of multiple objectives would be useful to decision makers.

Because most of the studies included in this review paper assume risk to be static, work is needed that considers risks that change over time. For instance, strategic attackers may change their strategies over time. Therefore, it would be useful to have models that helped decision makers make strategic decisions to mitigate against time-varying risks.

There are a few system types that have not yet been studied. First, no one has studied how to reduce the risk of source-sink networks with both source and intermediate node failures. Second, there is a class of networks where only n edges can exist on the source-sink path. One example of this is hub-and-spoke networks, where at most two hubs may be visited along the way from source to sink. These networks are prevalent in air transportation. However, no one has investigated how to reduce the risk of these networks.

The problem of reducing the disruption risk of interdependent infrastructure systems has not been studied much. As the understanding of these interdependencies increases, researchers should begin to include interdependencies into models for protecting interdependent infrastructures. Vespignani (2010) states that a limitation of existing models is that they only model network connectivity and do not model flow through the network. The field of operations research, in which network flow is well studied, appears to be poised to address this extension. systems has not been studied much. As the understanding of these interdependencies increases, researchers should begin to include interdependencies into models for protecting interdependent infrastructures. Vespignani (2010) states that a limitation of existing models is that they only model network connectivity and do not model ow through the network. The field of operations research, in which network ow is well studied, appears to be poised to address this extension. Chang (2009) points out that interdependent networks are usually composed of many types of systems and suggests that inter-disciplinary research (e.g., engineering and social science) is important to make advances in this area of study.

9 Conclusions

In this survey paper, we reviewed models for reducing the disruption risk of networks. We also briefly discussed descriptive models, which seek to assess the vulnerability and risk of networks with respect to disruptions. During the course of our discussion we classified the literature by the system type, risk reduction measure, and risk reduction strategy. At the end of our review we pointed out areas of future work.

Our discussion showed that there are several avenues of future work. First, a researcher may wish to address some of the categories that did not contain very many papers. Second, a researcher may want to try integrating some of the approaches that were reviewed in this paper. Third, we suggested several new areas of research.

This is an important area of research because infrastructures are complex, critical, and vulnerable. Because of this, researchers should address the many opportunities for future work.

Acknowledgements

The authors would like to thank the US Department of Homeland Security (DHS) for sponsoring this work through the Mack-Blackwell Rural Transportation Centre at the University of Arkansas through Grant Number DHS-1101. However, the views expressed in this paper do not represent those of DHS, but rather those of the authors. Finally, the authors wish to thank the anonymous reviewers for their comments.

References

Ahuja, R., Magnanti, T. and Orlin, J. (1993) *Network Flows: Theory, Algorithms, and Applications*, Prentice-Hall, Englewood Cliffs, NJ.

Aksen, D., Piyade, N. and Aras, N. (2009) 'The budget constrained r-interdiction median problem with capacity expansion', *Central European Journal of Operations Research*, pp.1–23.

Albert, R., Jeong, H. and Barabasi, A. (2000) 'Error and attack tolerance of complex networks', *Nature*, Vol. 406, No. 6794, pp.378–382.

Alderson, D.L. (2008) 'Catching the 'network science' bug: insight and opportunity for the operations researcher', *Operations Research*, Vol. 56, No. 5, pp.1047–1065.

Ambs, K., Cwilich, S., Deng, M., Houck, D., Lynch, D. and Yan, D. (2000) 'Optimizing restoration capacity in the AT&T network', *Interfaces*, Vol. 30, No. 1, pp.26–44.

Azaiez, M. and Bier, V. (2007) 'Optimal resource allocation for security in reliability systems', *European Journal of Operational Research*, Vol. 181, No. 2, pp.773–786.

Balakrishnan, A., Magnanti, T. and Sokol, J. (2001) 'Telecommunication link restoration planning with multiple facility types', *Annals of Operations Research*, Vol. 106, pp.127–154.

Balakrishnan, A., Magnanti, T.L., Sokol, J.S. and Wang, Y. (2002) 'Spare-capacity assignment for line restoration using a single-facility type', *Operations Research*, Vol. 50, No. 4, pp.617–635.

Barabasi, A-L. and Albert, R. (1999) 'Emergence of scaling in random networks', *Science*, Vol. 286, No. 5439, pp.509–612.

Beygelzimer, A., Grinstein, G., Linsker, R. and Rish, I. (2005) 'Improving network robustness by edge modification', *Physica A: Statistical Mechanics and its Applications*, Vol. 357, Nos. 3–4, pp.593–612.

Bier, V. and Abhichandani, V. (2003) 'Optimal allocation of resources for defense of simple series and parallel systems from determined adversaries', in *Risk-based Decision Making in Water Resources X: Proceedings of the Tenth Conference*, American Society of Civil Engineers, Santa Barbara, California, 3–8 November, p.59.

Bier, V. M., Nagaraj, A. and Abhichandani, V. (2005) 'Protection of simple series and parallel systems with components of different values', *Reliability Engineering and System Safety*, Vol. 87, No. 3, pp.315–323.

Bier, V., Cox, L. and Azaiez, M. (2009) 'Why both game theory and reliability theory are important in defending infrastructure against intelligent attacks', in *Game Theoretic Risk Analysis of Security Threats*, Springer.

Bier, V., Gratz, E., Haphuriwat, N., Magua, W. and Wierzbicki, K. (2007a) 'Methodology for identifying near-optimal interdiction strategies for a power transmission system', *Reliability Engineering and System Safety*, Vol. 92, No. 9, pp.1155–1161.

Bier, V., Oliveros, S. and Samuelson, L. (2007b) 'Choosing what to protect: strategic defensive allocation against an unknown attacker', *Journal of Public Economic Theory*, Vol. 9, No. 4, p.563.

Bier, V.M. (2007) 'Choosing what to protect', *Risk Analysis*, Vol. 27, No. 3, pp.607–620.

Bier, V.M., Haphuriwat, N., Menoyo, J., Zimmerman, R. and Culpen, A.M. (2008) 'Optimal resource allocation for defense of targets based on differing measures of attractiveness', *Risk Analysis*, Vol. 28, No. 3, pp.763–770.

Birge, J.R. and Louveaux, F. (1997) *Introduction to Stochastic Programming*, Springer-Verlag, New York.

Brown, G., Carlyle, M., Salmerffon, J. and Wood, K. (2005) 'Analyzing the vulnerability of critical infrastructure to attack and planning defenses', in J.C. Smith (Ed.): *INFORMS Tutorials in Operations Research*, pp.102–123, INFORMS, Baltimore, MD.

Brown, P. (2005) 'Optimizing the long-term capacity expansion and protection of Iraqi oil infrastructure', Master thesis, Naval Postgraduate School.

Buldyrev, S., Parshani, R., Paul, G., Stanley, H. and Havlin, S. (2010) 'Catastrophic cascade of failures in interdependent networks', *Nature*, Vol. 464, No. 7291, pp.1025–1028.

Cappanera, P. and Scaparra, M. (to appear) 'Optimal allocation of protective resources in shortest-path networks', *Transportation Science*.

Chang, S.E. (2009) 'Infrastructure resilience to disasters', *The Bridge*, Vol. 39, No. 4, pp.36–41.

Chekuri, C., Gupta, A., Kumar, A., Naor, J. and Raz, D. (2005) 'Building edge-failure resilient networks', *Algorithmica*, Vol. 43, Nos. 1–2, pp.17–41.

Church, R. (2003) 'COBRA: a new formulation of the classic p-median location problem', *Annals of Operations Research*, Vol. 122, No. 1, pp.103–120.

Church, R. and ReVelle, C. (1974) 'The maximal covering location problem', *Papers in Regional Science*, Vol. 32, No. 1, pp.101–118.

Church, R. and Scaparra, M. (2007) 'Protecting critical assets: the r-interdiction median problem with fortification', *Geographical Analysis*, Vol. 39, No. 2, pp.129–146.

Church, R.L. and Scaparra, M.P. (2006) 'Analysis of facility systems reliability when subject to attack or a natural disaster', in A.T. Murray and T.H. Grubesic (Eds.): *Critical Infrastructure: Reliability and Vulnerability*, pp.221–241, Chapter 11, Springer-Verlag, Berlin, Germany.

Church, R., Scaparra, M. and Middleton, R. (2004) 'Identifying critical infrastructure: the median and covering facility interdiction problems', *Annals of the Association of American Geographers*, Vol. 94, No. 3, pp.491–502.

Corley, H.W., Jr. and Chang, H. (1974) 'Finding the n most vital nodes in a flow network', *Management Science*, Vol. 21, No. 3, pp.362–364.

Costa, L.D. (2004) 'Reinforcing the resilience of complex networks', *Phys. Rev. E*, Vol. 69, No. 6, pp.066127–1–066127–7.

Cui, T., Ouyang, Y. and Shen, Z. (to appear) 'Reliable facility location under the risk of disruptions', *Operations Research*.

Cunningham, W. (1985) 'Optimal attack and reinforcement of a network', *Journal of the Association for Computing Machinery*, Vol. 32, No. 3, pp.549–561.

DallAsta, L., Barrat, A., Barthelemy, M. and Vespignani, A. (2006) 'Vulnerability of weighted networks', *Journal of Statistical Mechanics: Theory and Experiment*, Vol. 2006, No. 4, p.04006.

Daskin, M. (1983) 'A maximum expected covering location model: formulation, properties and heuristic solution', *Transportation Science*, Vol. 17, No. 1, pp.48–70.

Department of Homeland Security (2002) *National Strategy for Homeland Security*.

Dighe, N., Zhuang, J. and Bier, V. (2009) 'Secrecy in defensive allocations as a strategy for achieving more cost-effective attacker deterrence', *International Journal of Performability Engineering*, Vol. 5, No. 1, pp.31–43.

Dong, L., Xing-hua, K. and Xiang-tao, Y. (2009) 'A model for supply chain critical facility protection planning based on time satisfaction', in *Proceedings of the 2009 Second International Conference on Intelligent Computation Technology and Automation*, EEE Computer Society, Vol. 3, pp.903–906.

Erdos, P. and Renyi, A. (1959) 'On random graphs', *Publicationes Mathematicae Debrecen*, Vol. 6, Nos. 290–297, p.156.

Golany, B., Kaplan, E., Marmur, A. and Rothblum, U. (2009) 'Nature plays with dice–terrorists do not: allocating resources to counter strategic versus probabilistic risks', *European Journal of Operational Research*, Vol. 192, No. 1, pp.198–208.

Grigg, C., Wong, P., Albrecht, P., Allan, R., Bhavaraju, M., Billinton, R., Chen, Q., Fong, C., Haddad, S., Kuruganty, S. et al. (1999) 'The IEEE reliability test system-1996. A report prepared by the reliability test system task force of the application of probability methods subcommittee', *IEEE Transactions on Power Systems*, Vol. 14, No. 3, pp.1010–1020.

Grubesic, T., Matisziw, T., Murray, A. and Snediker, D. (2008) 'Comparative approaches for assessing network vulnerability', *International Regional Science Review*, Vol. 31, No. 1, p.88.

Hausken, K. (2002) 'Probabilistic risk analysis and game theory', *Risk Analysis*, Vol. 22, No. 1, pp.17–27.

Hausken, K. (2007) 'Protecting infrastructures from strategic attackers', in *Proceedings of the 2007 European Safety and Reliability Conference*, Stavanger, Norway, Vol. 1, pp.881–887.

Hausken, K. (2008a) 'Strategic defense and attack for series and parallel reliability systems', *European Journal of Operational Research*, Vol. 186, No. 2, pp.856–881.

Hausken, K. (2008b) 'Strategic defense and attack for reliability systems', *Reliability Engineering and System Safety*, Vol. 93, No. 11, pp.1740–1750.

Hausken, K. and Levitin, G. (2009a) 'Protection vs. false targets in series systems', *Reliability Engineering and System Safety*, Vol. 94, No. 59, pp.73–81.

Hausken, K., Bier, V. and Zhuang, J. (2009) 'Defending against terrorism, natural disaster, and all hazards', *Game Theoretic Risk Analysis of Security Threats*, Springer, New York, pp.65–97.

Holmgren, A.J., Jenelius, E. and Westin, J. (2007) 'Evaluating strategies for defending electric power networks against antagonistic attacks', *IEEE Transactions on Power Systems*, Vol. 22, No. 1, pp.76–84.

Horst, R., Pardalos, P. and Van Thoai, N. (2000) *Introduction to Global Optimization*, Springer.

Israeli, E. and Wood, R. (2002) 'Shortest-path network interdiction', *Networks*, Vol. 40, No. 2, pp.97–111.

Jenelius, E., Westin, J. and Holmgren, J. (2010) 'Critical infrastructure protection under imperfect attacker perception', *International Journal of Critical Infrastructure Protection*, Vol. 3, No. 1, pp.16–26.

Kennington, J., Nair, V. and Spiride, G. (2007a) 'A decomposition approach for spare capacity assignment for path restorable mesh networks', *International Journal of Computers and Applications*, Vol. 29, No. 2, pp.170–179.

Kennington, J., Olinick, E. and Spiride, G. (2007b) 'Basic mathematical programming models for capacity allocation in mesh-based survivable networks', *Omega*, Vol. 35, No. 6, pp.629–644.

Lee, K., Park, K., Park, S. and Lee, H. (1998) 'Economic spare capacity planning for DCS mesh-restorable networks', *European Journal of Operational Research*, Vol. 110, No. 1, pp.63–75.

Levitin, G. and Hausken, K. (2008) 'Protection vs. redundancy in homogeneous parallel systems', *Reliability Engineering and System Safety*, Vol. 93, No. 10, pp.1444–1451.

Levitin, G. and Hausken, K. (2009a) 'Meeting a demand vs. enhancing protections in homogeneous parallel systems', *Reliability Engineering and System Safety*, Vol. 94, No. 11, pp.1711–1717.

Levitin, G. and Hausken, K. (2009b) 'False targets vs. redundancy in homogeneous parallel systems', *Reliability Engineering and System Safety*, Vol. 94, No. 2, pp.588–595.

Levitin, G. and Hausken, K. (2009c) 'Redundancy vs. protection vs. false targets for systems under attack', *IEEE Transactions on Reliability*, Vol. 58, No. 1, pp.58–68.

Liberatore, F., Scaparra, M. and Daskin, M. (2011) 'Analysis of facility protection strategies against uncertain numbers of attacks: the stochastic r-interdiction median problem with fortification', *Computers and Operations Research*, Vol. 38, No. 1, pp.357–366.

Lim, M., Daskin, M., Chopra, S. and Bassamboo, A. (2010a) 'A facility reliability problem: formulation, properties, and algorithm', *Naval Research Logistics*, Vol. 57, No. 1, pp.8–70.

Lim, M., Daskin, M., Chopra, S. and Bassamboo, A. (2010b) 'Solving interdictor-defender bilevel optimization: a two population genetic algorithm approach', Technical report, University of Illinois.

Liu, C., Fan, Y. and Ordonez, F. (2009) 'A two-stage stochastic programming model for transportation network protection', *Computers and Operations Research*, Vol. 36, No. 5, pp.1582–1590.

Ma, Y. and Wu, H. (2006) 'Definitions and curve fitting of time satisfaction functions in facility location problems', in *Proceedings of the 2006 International Conference on Management Science and Engineering*, Piscataway, NJ, USA, Vol. 1, pp.429–433.

Michaels, D., McGrath, S. and Pasztor, A. (2010) 'Airports reopen, safety debate lingers', *Wall Street Journal*, available at http://online.wsj.com.

Morehead, R. and Noore, A. (2007) 'Novel hybrid mitigation strategy for improving the resiliency of hierarchical networks subjected to attacks', *Physica A*, Vol. 378, No. 2, pp.603–612.

Murray, A., Matisziw, T. and Grubesic, T. (2008) 'A methodological overview of network vulnerability analysis', *Growth and Change*, Vol. 39, No. 4, pp.573–592.

O'Hanley, J.R., Church, R.L. and Gilless, J.K. (2007) 'Locating and protecting critical reserve sites to minimize expected and worst-case losses', *Biological Conservation*, Vol. 134, No. 1, pp.130–141.

Peeta, S., Salman, F.S., Gunnec, D. and Viswanath, K. (2010) 'Pre-disaster investment decisions for strengthening a highway network', *Computers & Operations Research*, Vol. 37, No. 10, pp.1708–1719.

Peng, R., Levitin, G., Xie, M. and Ng, S. (2010) 'Defending simple series and parallel systems with imperfect false targets', *Reliability Engineering and System Safety*, Vol. 95, No. 6, pp.679–688.

Powell, R. (2007a) 'Allocating defensive resources with private information about vulnerability', *American Political Science Review*, Vol. 101, No. 4, pp.799–809.

Powell, R. (2007b) 'Defending against terrorist attacks with limited resources', *American Political Science Review*, Vol. 101, No. 3, pp.527–541.

Qiao, J., Jeong, D., Lawley, M., Richard, J-P., Abraham, D. and Yih, Y. (2007) 'Allocating security resources to a water supply network', *IIE Transactions*, Vol. 39, No. 1, pp.95–109.

Rail Report: Rail Customer News and Information (2005) 'Rails cause utility fuel shortages, electricity rate hikes', available at http://www.railcure.org/pdf/newsletter0805.pdf (accessed on 8 October 2010).

Ramirez-Marquez, J.E., Rocco, C.M. and Levitin, G. (2009) 'Optimal protection of general source-sink networks via evolutionary techniques', *Reliability Engineering and System Safety*, Vol. 94, No. 10, pp.1676–1684.

Ryoo, H-S. and Sahinidis, N.V. (2003) 'Global optimization of multiplicative programs', *Journal of Global Optimization*, Vol. 26, No. 4, pp.387–418.

San Martin, P. (2007) 'Tri-level optimization models to defend critical infrastructure', Master thesis, Naval Postgraduate School.

Santos, J. (2006) 'Inoperability input-output modeling of disruptions to interdependent economic systems', *Systems Engineering*, Vol. 9, No. 1, pp.20–34.

Scaparra, M. and Church, R. (2008a) 'An exact solution approach for the interdiction median problem with fortification', *European Journal of Operational Research*, Vol. 189, No. 1, pp.76–92.

Scaparra, M.P. and Church, R.L. (2008b) 'A bilevel mixed-integer program for critical infrastructure protection planning', *Computers and Operations Research*, Vol. 35, No. 6, pp.1905–1923.

Schavland, J., Chan, Y. and Raines, R.A. (2009) 'Information security: designing a stochastic-network for throughput and reliability', *Naval Research Logistics*, Vol. 56, pp.625–641.

Sivaraman, R. (2007) 'Capacity expansion in contemporary telecommunication networks', PhD thesis, Massachusetts Institute of Technology.

Skaperdas, S. (1996) 'Contest success functions', *Economic Theory*, Vol. 7, No. 2, pp.283–290.

Smith, J.C. (2011) *Wiley Encyclopedia of Operations Research and Management Science*, chapter Basic Interdiction Models.

Smith, J.C. and Lim, C. (2008) *Pareto Optimality, Game Theory and Equilibria*, chapter Algorithms for Network Interdiction and Fortification Games, Springer New York, pp.609–644.

Snyder, L. and Daskin, M. (2007) 'Models for reliable supply chain network design', in A.T. Murray and T.H. Grubesic, (Eds.): *Critical Infrastructure: Reliability and Vulnerability*, pp.257–289, Chapter 13, Springer-Verlag, Berlin, Germany.

Snyder, L. and Daskin, M. (2005) 'Reliability models for facility location: the expected failure cost case', *Transportation Science*, Vol. 39, No. 3, pp.400–416.

Snyder, L., Scaparra, M., Daskin, M. and Church, R. (2006) *Planning for Disruptions in Supply Chain Networks*, Baltimore, MD.

Snyder, L.V. and Daskin, M.S. (2006) 'Stochastic p-robust location problems', *IIE Transactions*, Vol. 38, No. 11, pp.971–985.

Snyder, L.V., Atan, Z., Peng, P., Rong, Y., Schmitt, A.J. and Sinsoysalk, B. (2010) 'OR/MS models for supply chain disruptions: a review', Submitted draft, Lehigh University, available at http://papers.ssrn.com/sol3/papers.cfm?abstract id=1689882.

Sullivan, J.L., Aultman-Hall, L. and Novak, D.C. (2009) 'A review of current practice in network disruption analysis and an assessment of the ability to account for isolating links in transportation networks', *Transportation Letters*, Vol. 1, pp.271–280.

The Department of Homeland Security Risk Steering Committee (2008) 'DHS risk Lexicon', Technical report, Department of Homeland Security, Washington, DC.

United States-Canada Power System Outage Task Force (2004) Final report on the August 14th blackout in the United States and Canada.

Veerasamy, J., Venkatesan, S. and Shah, J.C. (1999) 'Spare capacity assignment in telecom networks using path restoration and further improvement using traffic splitting', *Journal of Systems and Software*, Vol. 47, No. 1, pp.27–33.

Vespignani, A. (2010) 'The fragility of interdependency', *Nature*, Vol. 464, No. 7291, pp.984–985.

Wallace, S. (1987) 'Investing in arcs in a network to maximize the expected max flow', *Networks*, Vol. 17, No. 1, pp.87–103.

Watts, D. and Strogatz, S. (1998) 'Collective dynamics of 'small-world' networks', *Nature*, Vol. 393, No. 6684, pp.440–442.

Wood, R. (1993) 'Deterministic network interdiction', *Mathematical and Computer Modelling*, Vol. 17, No. 2, pp.1–18.

Yao, Y., Edmunds, T., Papageorgiou, D. and Alvarez, R. (2007) 'Trilevel optimization in power network defense', *IEEE Transactions on Systems Man and Cybernetics Part C*, Vol. 37, No. 4, p.712.

Zhan, R. (2007) 'Models and algorithms for reliable facility location problems and system reliability optimization', PhD thesis, University Of Florida.

Zhao, J. and Xu, K. (2009) 'Enhancing the robustness of scale-free networks', *Journal of Physics A: Mathematical and Theoretical*, Vol. 42, p.195003.

Zhuang, J. and Bier, V. (2008) 'Katrina vs. 9/11 how should we optimally protect against both? in H. Richardson, P. Gordon and J. Moore II (Eds.): *Post-Katrina: Economics, Social Aspects, and Risk*, pp.71–83, Chapter 4, Edward Elgar Publishing.

Zhuang, J. and Bier, V. (to appear) 'Secrecy and deception at equilibrium, with applications to anti-terrorism resource allocation', *Defence and Peace Economics*.

Zhuang, J. and Bier, V.M. (2007) 'Balancing terrorism and natural disasters-defensive strategy with endogenous attacker effort', *Operations Research*, Vol. 55, No. 5, pp.976–991.

Zimmerman, R. (2004) 'Decision-making and the vulnerability of interdependent critical infrastructure', in *Proceedings of the 2004 IEEE International Conference on Systems, Man and Cybernetics*, IEEE, Vol. 5, pp.4059–4063.

Zimmerman, R. and Restrepo, C. (2006) 'The next step: quantifying infrastructure independencies to improve security', *International Journal of Critical Infrastructures*, Vol. 2, No. 2, pp.215–230.