IISE Transactions

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uiie21

Homeland security research opportunities

Laura A. Albert, Alexander Nikolaev & Sheldon H. Jacobson

To cite this article: Laura A. Albert, Alexander Nikolaev & Sheldon H. Jacobson (2022): Homeland security research opportunities, IISE Transactions, DOI: 10.1080/24725854.2022.2045392

To link to this article: https://doi.org/10.1080/24725854.2022.2045392

Published online: 12 Apr 2022.

IISE TRANSACTIONS
https://doi.org/10.1080/24725854.2022.2045392

Homeland security research opportunities

Laura A. Albert[a], Alexander Nikolaev[b], and Sheldon H. Jacobson[c]

[a]Department of Industrial and Systems Engineering, University of Wisconsin-Madison, Madison, WI, USA; [b]Department of Industrial and Systems Engineering, University at Buffalo, Buffalo, NY, USA; [c]Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, IL, USA

ABSTRACT

Homeland security research has gone through a significant transformation since the events of September 11, 2001, and continues to evolve. This article identifies opportunities that the industrial engineering and operations research communities can seize. By drawing together insights from thought leaders in these communities, a path outlining research problems and discovery is provided that will serve to guide industrial engineering and operations research innovations and help move homeland security research forward over the next decade.

ARTICLE HISTORY
Received 28 December 2021
Accepted 11 February 2022

KEYWORDS
Counterterrorism; infrastructure security; interdiction; cybersecurity; risk analysis

1. Introduction

Security was, is, and is likely to continue to be, an area with widespread public interest, concern, discussion, and research. Prior to the events of September 11, 2001, security was something that most United States (US) residents felt was someone else's problem, usually managed by businesses and corporations, or at the national scale, government. The concepts of protection and security were often considered military issues, with the US Department of Defense responsible for such activities. The events of September 11, 2001, changed that perspective, broadening security to include civilian targets such as commercial aviation, propelling security into a new light, effectively making it an area that touched everyone's life.

The creation of the Department of Homeland Security launched a new era of national security, with modeling and analytics needed to address security issues focusing on deterrence, interdiction, protection, and response across a wide swath of society. The goal was to protect both lives and assets by allocating resources to secure systems. Given the limited resources available for security, Industrial Engineering and Operations Research (IE/OR) provided useful models and methods to design enhanced security systems, make interconnected decisions to support security efforts, and to deploy and use security resources (Larson, 2004; Wright *et al.*, 2006).

Operations Research (OR) is rooted in military applications. Some of the earliest applications of OR addressed military patrols for security (Morse and Kimball, 1946). Over the years, the breadth of security domains addressed using OR methods has grown across the private and public sectors. Areas where IE/OR have had an impact to date include aviation security (Albert *et al.*, 2020), securing critical infrastructure (Brown *et al.*, 2006; Zhuang and Bier, 2007), emergency preparedness (Jia *et al.*, 2007; Mete and Zabinsky, 2010), and disaster management (Caunhye *et al.*, 2012, Galindo and Batta, 2013). IE/OR has also shed light on appropriate models for adaptive adversaries (Brown and Cox, 2011). Several specific examples of where OR models have been used include interdicting smuggled nuclear material (Morton *et al.*, 2007), scheduling Federal Air Marshals (Jain, Tsai, Pita, Kiekintveld, Rathi, Tambe and Ordonez, 2010), strategically allocating defensive resources (Bier *et al.*, 2007), and protecting food supply chains (Wein and Liu, 2005).

The homeland security landscape continues to evolve, as targets become more lucrative and new vectors of attack become ubiquitous. Physical security at travel hubs and around public assets continue to provide outlets for bad actors to target. With the advent of the Internet and widespread digitization across commerce, industry, and government, and the ubiquity of cyber components in various systems and infrastructure, cyber assets have taken the lead as the primary target requiring protection, e.g., including that against malware, phishing, and ransomware (Enayaty-Ahangar *et al.*, 2020). What is most apparent is that IE/OR methodologies are well-suited to influence homeland security over the next decade.

The objective of this article is to synthesize thoughts on future research directions for IE/OR within the realm of security, with an eye on identifying where the IE/OR research community can take the next steps forward. Ideally, these thoughts will facilitate quantum leaps in methodology and application that will address existing and future threats, as well as inform policy. We hope to inspire new research thrusts that will foster methodological innovations (so as to overcome current stumbling blocks and/or directions to

CONTACT Sheldon H. Jacobson shj@illinois.edu

overcome them), tap new data sources, and provide inspiration for yet-to-be-identified novel problem formulations.

This article is organized as follows. Section 2 provides a brief overview of the problem domains and methods where IE/OR has been at the forefront of innovation. Section 3 provides commentaries by several thought leaders in the field as to the areas of immediate and future need. Section 4 provides a summarizing discussion.

2. IE/OR footprint in today's homeland security

The IE/OR research that addresses critical issues in homeland security has encompassed a broad range of homeland security issues and decisions. In this section, we mainly focus on the past two decades' work in three areas where IE/OR research had the most impact on the research community and policy: aviation security, network interdiction, and critical infrastructure protection.

2.1. Aviation security

The events of September 11, 2001, transformed aviation security. Shortly after that day, the Aviation and Transportation Security Act created the Transportation Security Administration (TSA), which launched a new era for airport security screening strategies and tactics (Jacobson *et al.*, 2003; Barnett, 2004; Martonosi and Barnett, 2006). Aside from the TSA assuming control of airport security checkpoint operations, the newly created TSA meant that transportation security would be viewed as a system. This created an opportunity and natural setting for IE/OR methods to improve their design and optimize their performance.

Given that airport security checkpoint design and operations was a topic that was being rethought, the optimal allocation of security resources at airport security checkpoints, such as screening device technologies, was an open area for investigation. A stream of papers in the literature studied how to select screening procedures and devices, as well as how to assign passengers to screening procedures. McLay *et al.* (2006) conceptualized a multi-level screening approach that lifts the assumption that all passengers pose the same level of risk. Early research contributed linear and integer programming models to determine optimal security checkpoint configurations (McLay *et al.*, 2007; Nie *et al.*, 2009). Nikolaev *et al.* (2007) merged the design and real-time allocation decisions in an aviation security resource allocation problem. Subsequent efforts analyzed dynamical routing of passengers to security classes, using Markov decision processes (McLay *et al.*, 2009; McLay *et al.*, 2010), control theory (Lee *et al.*, 2009), and queueing theory (Lee and Jacobson, 2011).

It quickly became apparent that IE/OR methods provide useful tools for analyzing and improving tactical airport security operations. However, it took time for these tools to contribute to the strategic design of airport security checkpoints. A fundamental, research-originated paradigm shift for aviation security was the introduction of risk-based security (Nikolaev *et al.*, 2007; McLay *et al.*, 2010). Indeed, for the first 10 years after September 11, 2001, U.S. airport security operations were designed under the flawed assumption that all passengers posed the same level of risk to the air system. This means that from the security operations perspective, all air passengers were treated the same way, even though airport security policy-makers knew that was not ideal. The challenge was to provide sufficient evidence to support differential screening that would satisfy lawmakers and the flying public. Risk-based security transformed such thinking, allowing for the flexibility of aligning security resources and their benefits with security risk. The breakout from the one-size-fits-all security paradigm in practice took place in November 2011 with the launch of TSA PreCheck (Albert *et al.*, 2020). PreCheck offers passengers the opportunity to qualify for expedited physical screening at airports in exchange for voluntarily undergoing a background check to assess their risk.

This strategic paradigm shift permitted higher passenger throughput rates while providing higher levels of security to the air system. PreCheck-expedited screening lanes require lower levels of TSA officer attention, permitting more security attention be focused on the remaining passengers. As passenger throughput ramped up over the ensuing decade, PreCheck lanes maintained low passenger waiting times, helping to maintain good overall airport security checkpoint throughput performance.

Passenger screening is the most visible activity in a layered aviation security system. IE/OR literature contributed to its other aspects as well. For example, research has examined how to strategically allocate Federal Air Marshals (FAMs) on certain high-risk flights. The role of FAMs is to thwart attacks if an attacker bypasses security operations. Jain, Tsai, Pita, Kiekintveld, Rathi, Tambe and Ordonez (2010) introduced a large-scale Stackelberg game model that creates randomized schedules for placing FAMs on international flights. Fast algorithms based on column-generation algorithms were developed to find optimal randomized schedules to allocate FAMs (Jain, Kardes, Kiekintveld, Ordonez and Tambe, 2010). Other research has examined ways to protect commercial airplanes against surface-to-air missile attacks using a decision tree analysis (Von Winterfeldt and O'Sullivan, 2006).

Broadening the research on securing checkpoints, the IE/OR community recommended ways to systemically manage limited security resources when securing borders, and ports of entries beyond airports. Indeed, checkpoint operations challenges often involve sequential screening for threats (Boros *et al.*, 2009; Boros *et al.*, 2011), deploying new screening devices within existing screening operations (Gaukler *et al.*, 2011), and evaluating the impact of risk assessments on screening and inspection processes (Gaukler *et al.*, 2012; McLay and Dreiding, 2012). Many checkpoint inspection decisions require the analyses of the tradeoff between detection rates and speed, and inspection protocols can often be applied only sparingly to avoid long queues (Bakshi *et al.*, 2011). Randomized, software-assisted security solutions made tangible impact on surveillance operations

for both the FAM Service and police road patrol (Jain, Tsai, Pita, Kiekintveld, Rathi, Tambe and Ordonez, 2010).

2.2. Network interdiction

Homeland security applications motivated the need to understand how a system can perform in the presence of worst-case and/or cascading failures, as well as how to design a system to be resilient to such failures. This led to the proliferation of network interdiction modeling approaches for studying system vulnerability, with the aim to ensure or enhance system-level protection from "attacks" (Smith and Song, 2020). This line of research on network interdiction is thus a counterpart of the work on system reliability to random component failures.

Network interdiction models capture the strategic interactions between an attacker and a defender on a graph, where the dynamics are typically those of a Stackelberg game (Casorrán *et al.*, 2019). This is a game where a "leader"/defender acts first by interdicting components (e.g., lengthening arcs), and a "follower"/adversary has recourse decisions based on the leader's interdiction decisions. In a "system interdiction problem" (Israeli and Wood, 2002), a leader disrupts an adversary's "economy" through interdiction, which may represent compromising the follower's key components or activities, such as power generators, transportation, and smuggling. The core of these problems is typically a variant of a network flow problem, focusing on maximum flows (Wood, 1993), shortest paths (Israeli and Wood, 2002), or maximum-reliability paths (Morton *et al.*, 2007).

IE/OR methods and approaches for network interdiction have been instrumental in a variety of application areas. Brown *et al.* (2009) showed that max-min optimization, in conjunction with a project-management model, can be suited to tactically delay an adversary's nuclear weapons project. Morton *et al.* (2007) exercised creative use of linear programming duality in the problem of thwarting the transport of illicit nuclear materials. Dimitrov *et al.* (2011) considered radiation detection equipment specifications in positioning sensors so as to minimize the evasion probability for a nuclear smuggler that can be detected only with some probabilities when traversing the arcs of a transportation network. Other applications of IE/OR include disrupting drug transportation networks. Pan and Morton (2008) analyzed ways to disrupt drug transportation networks by developing step-inequalities that, used in mixed-integer program L-shaped decomposition, speed up stochastic interdiction algorithms. Zheng and Albert (2019) adapted physical network interdiction methods toward securing cyber-infrastructure. Church and Scaparra (2007) used those methods to propose a plan to fortify critical infrastructure (supply chain facilities) to withstand the impact of an intentional strike on system resilience. Smith *et al.* (2007) took a generalized view on survivable network design problems, relaxing the assumption of the rational behavior of an adversary that aims to destroy a network or disrupt its functionality.

2.3. Critical infrastructure protection

IE/OR has a long history of contributing to the planning, design, and operation of critical infrastructure. The recent history's large-scale terrorist attacks on public infrastructure led to a renewed interest in the *protection* of such critical infrastructure. The IE/OR community contributed to systems-level decisions by identifying vulnerabilities in interconnected systems, allocating scarce resources, and enhancing resilience in response to component failures (Greenberg *et al.*, 2012). The seminal paper by Brown *et al.* (2006) introduced a modeling framework for identifying vulnerabilities in an interconnected system and identify how to mitigate these vulnerabilities. They applied their modeling framework to examples for bolstering the US Strategic Petroleum Reserve, protecting the US border, and securing an electrical transmission system. A number of studies developed mathematical models to connect infrastructure operations to measures of system-level resilience (Alderson *et al.*, 2015).

Game theory emerged as a tool for providing insight into how to allocate scarce security resources in a system. Zhuang and Bier (2007) took a strategic perspective on resource allocation for countering terrorism and natural disasters and analyzed equilibrium solutions in multiple defender–attacker game types. A challenge in this area is understanding how to protect multiple targets by allocating limited resources. The literature contributed resource allocation approaches toward protecting potential targets (Willis, 2007; Bier *et al.*, 2008), and supported the development of strategies for hardening targets (Haphuriwat and Bier, 2011; Wang and Bier, 2011).

Overall, the IE/OR community engaged in a robust exploration of approaches to model terrorism risks (Cox, 2008) and alternatives to classic methods such as probabilistic risk analysis (Golany *et al.*, 2009; Brown and Cox, 2011). New models and analyses were introduced to support the allocation of scarce resources in response to risks introduced by adaptive adversaries (Ezell *et al.*, 2010). Prioritizing and balancing agendas of the research on risk assessment versus resilience has been a topic of active discussion in recent years (Greenberg *et al.*, 2020).

The papers reviewed in this section represent just a slice of research by the IE/OR community that has have demonstrated impact for the discipline. The next section discusses new opportunities proposed by a group of IE/OR thought leaders.

3. Thought leader perspectives

To provide a broad scope of insights, we engaged with several IE/OR thought leaders who provided their candid views on the future of homeland security and how IE/OR can play a key role.

3.1. Dr. Edward Kaplan

Dr. Edward Kaplan, a William N. and Marie A. Beach Professor of Operations Research at the Yale School of

Management, Professor of Public Health at the Yale School of Medicine, and Professor of Engineering in the Yale School of Engineering and Applied Science, has made numerous seminal contributions on problems related to homeland security.

Dr. Kaplan began by pointing out that, with homeland security, it helps to distinguish between natural threats and deliberate (or man-made) threats. The former include floods, hurricanes, earthquakes, epidemics, and other large-scale crises. The latter are due to the activity of (non-state) terrorist actors. There may exist some overlap of these two groups of threats, as is the case with biological terrorism. In this regard, the COVID-19 pandemic has demonstrated that the resulting threat/damage to the homeland from a naturally occurring outbreak can be severely exacerbated by deliberate human and political behavior and interference. For example, anti-masking and vaccination resistance during the COVID-19 pandemic are phenomena that bring to the forefront the challenges associated with the implementation of what could be controversial policies (to some), in addition to just sorting out the most effective public health policies. In the same vein, see an opinion paper by Lawson (2021) that discusses the new type of threat to the homeland that pandemics in general present.

In line with Dr. Kaplan's mainstream line of work, he offered several ideas in the realm of intentional threats to security, deliberating on two big issues that have (re-) emerged at the forefront in the last few years. The first one is the problem of identifying the source of the threat. Dr. Kaplan's own highly-cited work on such problems was overwhelmingly devoted to Jihadi terrorism and the figures of groups such as Al Qaeda/ISIS/Hezbollah/Hamas (Kaplan and Kress, 2005; Kaplan, 2010). Today, a reasonable argument can be made that domestic terrorism, which can be described as extremism, is now recognized as the bigger threat to the homeland.

Mass shooting events and their aftermath, as well as news-sparked and politics-related riots, with the January 2021 United States Capitol attack as one example, bear significant consequences for the preponderance of peaceful citizens. Importantly, the surveillance and intelligence gathering "rules" are different for foreign versus domestic threats, as the US Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) (as well as the National Security Agency) operate under different regulations. Yet, on both these playing fields, the basic goal is the same: identify threats so they can be preempted before they are realized. How to apply intelligence collection and analysis to domestic threats is a growing issue where IE/OR could be instrumental.

Another issue that Dr. Kaplan offered is that in today's world, much and perhaps most of the organizing activity for domestic and foreign threats takes place online over the Internet. This makes determining how to monitor and analyze social network data an important set of problems. Tauhid Zaman has been conducting innovative work on these problems. See, for example, the recent papers on finding online extremists and analyzing their social networks to identify community shaping-type ties (Klausen *et al.*, 2018) and on detecting bots and assessing their impact (Des Mesnards *et al.*, 2021). Attacks on financial institutions, similar to such long-standing threats as attacks on water supplies, traffic networks, continue to offer targets of opportunity for IE/OR research.

Search theory is a classic OR success story. Larry Stone's search algorithms (Stone, 1976) are still used by the Coast Guard and others when searching for people lost at sea (as well as downed airplanes). What extensions of these ideas, as well new models, are needed to enable efficient search for online actors and events? For example, Larry Stone worked with another Metron scientist, Jim Ferry, on search theory for fused physical and online location data (Popp and Yen, 2006). We note that data fusion methods and event representation models (e.g., using networks (Jenkins *et al.*, 2015; Farasat *et al.*, 2016)) are likely to be useful research directions in such efforts as well.

3.2. Dr. Cole Smith and Dr. David Morton

Dr. Cole Smith, Dean of the College of Electrical Engineering and Computer Science at Syracuse University, and Dr. David Morton, the David A. and Karen Richards Sachs Professor of Industrial Engineering and Management Sciences at Northwestern University, are authorities on network interdiction research. They provided their thoughts on future advances and IE/OR research opportunities in this domain.

Dr. Smith first pointed out that many efforts in security research seek to assess the vulnerability of a system (whether it is a network or not) to failure. This means that the objective may be to limit the scope of damage inflicted on a system when it is infiltrated by terrorist activities.

However, what does a failure mean in this context? It is typically defined as malicious intent: indeed, failures may be caused by "attackers" in attacker–defender models. In such models, attackers need not be sentient, and failures could be accidents that are sufficiently likely to occur. For example, in network problem formulations where an attacker is limited to interdicting at most k arcs, it is because the probability that more than k arcs fail may be sufficiently small. Alternatively, when using a more general budget-constrained adversary, it is common to equate a high budget to interdict the arc with a low probability that the arc could accidentally fail. So far, from a mathematical modeling perspective, one can thus equate a sentient attacker with an accidental failure, and then say in the latter case that the strategy is to mitigate a worst-case attack, i.e., discovering vulnerabilities in the system. In Dr. Smith's view, the next several decades of research in this area will more often need to explicitly address intent.

To this end, the IE/OR community is well-positioned to make the effort and step away from creating interdiction models that are "clean" (i.e., easy to treat from a mathematical optimization point of view). More realistic games are those that are played in turn between two agents (as in a Stackelberg game). Note that attacker–defender models are

(usually) NP-hard, and defender–attacker–defender models are (almost always) even more difficult. Naturally, addressing games with repeated turns is much more difficult and presents a research opportunity to fill a void in the literature. These problems may invite artificial intelligence approaches augmented with hard-earned knowledge on how to play two-stage interdiction games—an area in which IE/OR has excelled.

Along these lines, repeated games can be viewed in another way, in response to another simplification that has been the hallmark of interdiction studies. We tend to think of games as being one-shot games with all information being (symmetrically) available to both players. When the game is played once and information is asymmetric, there are some interesting studies available (Sefair and Smith, 2016; Smith and Song, 2020). Pay *et al.* (2019) consider stochastic network interdiction problems where the defender has incomplete (ambiguous) preferences that require modeling. However, suppose one takes the next natural step, namely, to play the game many times, with one player not seeing all of the network data. That player infers some information about the data and learns to play what we label as "blind." A further extension is for both players to be "blind." Assessing what happens in this case would be a fruitful direction of research.

Dr. Smith noted that the quantum leap that has yet to occur is due in part to optimizers and mathematical programmers (like many interdiction researchers in the IE/OR community) staying in the realm of problems that can be solved by mathematical programming. The more complicated games will be taken up by non-mathematical programmers. However, they may be handicapped by lack of awareness of the rich findings by the mathematical programming contributors. As such, they may apply inferior algorithms without the benefit of the decades of experience accumulated about network interdiction problems. This presents a unique opportunity for cross disciplinary collaborations, to expand the toolkit of methodologies if the IE/OR communities wishes to address the "messy" problems that would be more pertinent to actual homeland security deployment applications.

Dr. Smith concluded his discussion by noting that after urging the research community to reconsider making "clean" assumptions on the dynamics of the analyzed games, we must continue to pay special attention to the adopted objectives. The process of inferring adversarial intent is extremely difficult, and that is a field of study unto itself with its own literature and with its own set of researchers who have devoted their careers to its study. However, there is very little literature on intent in most IE/OR applications. Here, a typical choice is to work with a utility function, usually in a zero-sum game, where the attacker's intent is simply the opposite of the defender's intent. If not, perhaps bi-level optimization problems rather than interdiction problems can be formulated to provide insightful analysis and insights. At the end of the day, what matters is that such problems can be solved. The takeaway from this point is that the IE/OR community could learn much from delving into the literature of assessing intent, and perhaps studying problems in which the defender and attacker play several "rounds" of a game first, with the defender seeking to not only defend its infrastructure but also to learn what the attacker seeks to accomplish. Similarly, the attacker may first do reconnaissance only and seek to infer what object or area the defender is protecting.

Dr. Morton expanded on the need to define more creative uses of existing technical approaches to capture resiliency valuation, as well as the need to conceptualize new approaches. He begins with an important observation: the IE/OR community excels in building operational models, including systems models of key infrastructure (Alderson *et al.*, 2015). With such an operational model in hand, researchers can query system performance with some subset of components disabled. The ability to answer such "what if" questions naturally leads to families of models in which an adversary optimally degrades performance. This, in turn, allows one to inform hardening of infrastructure systems to improve resilience. From this premise, Dr. Morton makes two key points.

The first point concerns the mathematics behind those models of system security, and game-theoretic models in particular, that exploit the role of duality in optimization. These models continue to have important connections to recent advances in robust optimization, distributionally robust optimization, and adversarial models in machine learning.

The second point concerns opportunities and challenges in cybersecurity, which have been known to be significant for quite some time. There has been important work in this area, e.g., by Khouzani *et al.* (2019); also, see the review by Enayaty-Ahangar *et al.* (2020). At the same time, the mental model of building a high-fidelity mathematical model of an operational system and then querying it to understand its vulnerabilities is challenged by the systems involving cybersecurity. In Dr. Morton's view, principled approaches to cybersecurity using the IE/OR tools have been elusive but represent a breakthrough opportunity.

3.3. Dr. Fred Roberts

Dr. Fred Roberts, a Distinguished Professor of Mathematics at Rutgers University, provided his thoughts on issues centered around an array of areas, including the challenges in supply chain management in the traditional post-disaster recovery context and delving further toward the needs for the exploration of the Arctic. He also provided some stretch thoughts on other areas of importance for homeland security.

Dr. Roberts began by noting that infrastructure systems such as the power grid, road networks, and airports are ideal venues where IE/OR research can have an impact. Dr. Roberts argues that in setting problem objectives, the scientific community should be more explicit about the trade-off between resiliency and efficiency. Indeed, building resilient systems is not so much about avoiding damage, but instead about being able to withstand disruptions without breaking

and continuing to function in spite of damage. This issue has been discussed during the COVID-19 pandemic, where the objectives of optimality versus robustness come into play. Likewise, election security may also benefit from such consideration through the design of voting audit trail systems and incorporating controlled redundancy into vote collection procedures to enhance voter security, while also meeting other election performance objectives.

Research that enhances detection capabilities provides a rich direction for investigation in a variety of application areas. Given the proliferation of sensors, knowing where they should be placed and what information they should collect presents new IE/OR research opportunities. Such investigations would be highly application-dependent, though general principles may be extracted during the research process. For example, in the area of border crossings, ports, and customs, sensors could be embedded in inspection procedures that minimize delays, where they are possibly used by robots and intelligent machines during inspection. Sensors could be used in a more broad sense in diverse applications ranging from inspecting counterfeit parts in supply chains, to border surveillance, to monitoring the spread of a pandemic along with its different containment procedures (e.g., contact tracing, face masks, quarantine), to suppressing the spread of disinformation.

Given the adversarial role of terrorists, sequential games with mixed policies provide new methodological research opportunities, as also noted by Dr. Smith. This can be applied in a variety of settings, such as security patrols and public safety. Combating terrorism is more than identifying threat items; it is also about the people who engage in terrorist activity. Modeling human behavior or incorporating human behavior into IE/OR models can advance counterterrorism strategies. Collaborations between human factor researchers and operations researchers could facilitate such advances. This issue is salient in the area of large venue security, for example, when designing and redesigning venues to optimize evacuations (this would involve modeling high volume and speed crowd movements) and identifying inspection procedures and the role of randomization at different stages of the procedures.

Dr. Roberts further offered a potpourri of thoughts on homeland security research that would benefit from IE/OR methods. He recognizes opportunities for IE/OR innovation in supply chain resiliency, pandemic preparedness, disaster response, climate change, logistics in the Arctic region, and controlling the spread of misinformation. The takeaway from Dr. Robert's thoughts is that there exists a broad range of problems for IE/OR researchers to address, and stepping into new domains for the IE/OR community may be beneficial for both the research community and their collaborative partners.

3.4. Dr. Vicki Bier

Dr. Bier, a Professor Emeritus at the University of Wisconsin-Madison, provided thoughts along the lines of policy-making and the nature of risks that may have been dormant but are approaching serious magnitudes.

Dr. Bier noted that the Department of Homeland Security was established "to secure the nation from the many threats we face." Over time, however, as the agency became a more effective "machine bureaucracy," she argues that the agency has become less focused on the few most severe threats and more focused on determining priorities and budget allocations among a large number of risks, some of which are far less than catastrophic in nature.

Dr. Bier argues that research should not only emphasize "existential" risks; after all, September 11, 2001 and Hurricane Katrina were both quite traumatic enough for the US to merit significant attention, even though they did not lead to the demise of New York City or New Orleans, respectively. However, she encourages academic researchers to emphasize the study of hazards that have the potential for catastrophic impacts. After all, a small reduction in risk or technological improvement with regard to a catastrophic risk is likely to have a greater impact on society than an incremental advance in dealing with a risk that society is already able to manage.

Dr. Bier also argues that nearly all of these potentially catastrophic risks either are natural disasters or leverage the power of nature. It is simply difficult for terrorists to unleash as much power as can nature. For example, Hurricane Katrina caused more damage overall than the attacks of September 11, 2001.

In thinking about potential catastrophic risks that merit further research, Dr. Bier noted the release of a biological agent such as smallpox, which could start as an accident or an act of terrorism, can quickly become catastrophic through natural transmission. (We note that this point makes a connection with some earlier works due to Kaplan *et al.* (2002) and Wein *et al.* (2003).) Another example is forest fires, which (whether caused by climate change or poor forest management) are becoming increasingly catastrophic in the western US and around the world. More generally, climate change could make large parts of the world unlivable due to rising sea levels, inland flooding, and in some areas lack of available drinking water. As a result, climate-induced migration is another topic that is worthy of future study. Note that many of these are inherently multidisciplinary, and involve not only mathematical modeling (e.g., epidemiological models or agent-based models of flood response), but also social science and sociotechnical systems to address the human aspects involved in both disaster prevention and disaster response.

4. Discussion

There are several common themes that are woven through the perspective of the thought leaders, providing a picture of the landscape for IE/OR research opportunities. This section synthesizes such thought and adds opportunities for IE/OR researchers to engaging when the goal is to protect an asset from a threat.

Many existing IE/OR research efforts that have focused on homeland security have considered "attacks" to occur at a discrete point in time. The proliferation of data and social networks provides opportunities for IE/OR modeling to reduce risk across time. This opens up opportunities to gather information, gain knowledge from that information (e.g., identify terrorist groups and their social networks), and use this knowledge to not only prevent attacks but also to prevent adversarial groups from attracting others and advancing attack plans (as outlined by Dr. Kaplan). Likewise, IE/OR models could be used after an attack to complement forensics efforts by attributing the responsibility for the attack. In both examples, limited information regarding an attack (or plans for an attack), data analytics, and social network models could shed light on the "inverse problem" of who did the planning, their origin, and their goals. Given the growth of data, issues related to what kind of data should be collected and how it should be collected are much needed research directions.

Historically, many of the IE/OR efforts to support homeland security and protect critical infrastructure have focused on physical systems and assets. Dr. Kaplan made several points on the subject of online activity, namely, cyber security, which is the domain whose goals include protecting critical infrastructure from cyberattacks. Over the recent years, cyber targets have become more attractive and accessible, and hence, cyber security represents the most significant threat today (Biden, 2021). Prior to the advent of the Internet, physical security was the primary concern, with the goal of protecting people and their assets from attack. Since then, with widespread digitization across commerce, industry, and government and the ubiquity of cyber components in various systems and infrastructure, cybersecurity has taken the lead as the primary target requiring protection, including malware, phishing, and ransomware (Enayaty-Ahangar *et al.*, 2020). Machine learning-based methods have been largely unable to prevent damage due to fake reviews on key e-commerce platforms (Paul and Nikolaev, 2021) and this presents serious risks to self-regulation of open markets, a cornerstone of a capitalist economy. As for finding solutions to cybersecurity problems, a recent article in "*OR/MS Today*" discusses the propagation of fake news during natural disasters and the difficulties associated with debunking rumours and otherwise fighting the spread of large-scale misinformation (Hunt *et al.*, 2020). Other recent research has focused on supply chain investments (Zheng *et al.*, 2019; Simon and Omar, 2020).

Much of the modeling efforts in the IE/OR research community have been to find optimal solutions. As has been observed during the COVID-19 pandemic, resiliency rather than optimality has been more critical when analyzing complex systems. Methods for capturing resiliency, and discovering the resiliency/optimality nexus would provide valuable approaches for addressing security problems (as noted by Dr. Roberts). Resilience in critical infrastructure has been a strength of IE/OR models, since our tools model interconnected systems and can evaluate the performance of systems based on how their components operate and perform (Alderson *et al.*, 2015). A recent work by Baroud (2021) discusses the existing and desirable approaches to resilience modeling with a special focus on critical infrastructures preparedness applications. As Dr. Smith and Dr. Morton outlined, network interdiction models are adept at predicting performance given multiple component failures. The COVID-19 pandemic has highlighted the need to consider models of resilience for critical infrastructure systems under new types of disruptions over different time periods. Likewise, network interdiction models can reflect the structure of supply chains. The COVID-19 pandemic has also accentuated the need to consider equity in addition to resilience measures and efficiency in evaluating performance in response to large-scale disruptions.

Artificial Intelligence (AI) has become a mainstay IE/OR methodology. Methodologies that support moving from data to decision will continue to be important for managing security risks in the future. Traditional IE/OR models such as integer programming that are solved using branch-and-bound algorithms can be classified within the AI footprint. Machine Learning methods that employ neural networks offer more current AI techniques. Many of the opportunities for advancing security resides in finding new ways to use AI to deter, detect, and recover from security attacks. The advantage offered by AI is that it can transform large data sets into useful information. Security data is often incomplete, and AI researchers have long been pursuing innovations in unsupervised machine learning when data is incomplete. Achieving unbiased insights in such domains presents an opportunity for the IE/OR research community. Additionally, imbalance arises since security breaches are rare and their records are generally not made public, and hence, in security data sets the amount of the normalcy data is much greater than that of the anomaly data. Our unawareness of new types of attacks, before they are identified as such, amounts to data incompleteness. Additionally, when analyzing data to uncover security vulnerabilities, it is often easy to confuse causal insight with correlation and association. New methods are needed to unravel the dependence/causality nexus. Such contributions will reduce false alarms and false clears when attempting to identify and thwart security threats.

Infrastructure systems are highly connected. The connectedness of infrastructure systems means that a natural or anthropogenic hazard can lead to cascading events that are even more hazardous than the original event. As outlined by Dr. Bier, there is a need to manage catastrophic risks in interconnected systems, where the catastrophic risks can include slow-moving disasters such as climate change. Engineered systems that can prevent the worst outcomes can be prohibitively expensive to build, for example, which may motivate new strategies for reducing risk (e.g., migration strategies). Understanding the connections and their implications are crucial for identifying mitigating actions. In addition, the performance of infrastructure systems relies in human behavior in various ways, including automation and public participation. Infusing IE/OR research with sociotechnical systems could lead to important research contributions to identify incentives and policies for managing hazards in complex systems.

It is worth including several related forward-looking manuscripts that prescribe directions for future research. Lim *et al.* (2018) review research on securing waterways, ports and other maritime assets against terrorist attacks and piracy events, among others, indicating the need for IE/OR contributions in these areas. Konrad *et al.* (2017) highlight how the IE/OR community can help address the growing issue of human trafficking, which is a complex transnational problem for society and the global economy, but to date, has almost exclusively received attention from the criminology, sociology, and clinical research scientific communities. Su and Nwafor (2021) formulate the problem of intrusion detection in the emerging Internet of Things systems, which the IE/OR community could help advance.

Overall, since 2015, we observe the paucity of published basic research on homeland security. It appears that many researchers who contributed to the wave of creative thinking in the years following September 11, 2001 have moved on to other research applications. This research was supported by basic scientific research funding agencies, including DHS university centers of excellence such as Center for Risk and Economic Analysis of Threats and Emergencies (CREATE) at the University of Southern California that assesses strategies to mitigate risks from intentional and natural disasters, as well as grants from a partnership between National Science Foundation (NSF) and DHS's Domestic Nuclear Detection Office (DNDO), that encouraged long-term, transformational advances in nuclear detection technology. These funding initiatives were instrumental in stimulating innovative and impactful research in IE/OR. With the field maturing and with government agencies providing support for mission-driven research, innovative research that addresses homeland security in IE/OR has reduced. However, this article sheds light on the many fruitful opportunities that remain and suggests the need for scientific funding to support basic scientific research to enable the next major breakthroughs in this area.

In conclusion, the last two decades saw many important research contributions from the IE/OR community that supported and shaped homeland security. Several thought leaders outline the many challenges that remain. The takeaway from this discussion is that numerous opportunities exist for IE/OR researchers to contribute to enhancing homeland security, both tactically and strategically. Whether this involves relaxing simplifying assumptions, creating new models, or collaborating with those in nontraditional areas, IE/OR researchers can make a difference today for many years into the future. We hope this article inspires our community to take the next steps—and possibly quantum leaps—forward to make our world more safe and resilient.

Funding

The first author was in part supported by the National Science Foundation Awards 1935550 and 2000986. The third author's research has been supported in part by the Air Force Office of Scientific Research, United States (FA9550-19-1-0106). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Government, the National Science Foundation, or the Air Force Office of Scientific Research.

Notes on contributors

Laura Albert, PhD, is a Professor and the David Gustafson Department Chair of Industrial & Systems Engineering at the University of Wisconsin-Madison. Her research interests are in the field of operations research, with a particular focus on applications in the public sector. She has been awarded many honors for her research, including the American Association for the Advancement of Science (AAAS) Fellow Award, Institute of Industrial and Systems Engineers (IISE) Fellow Award, the INFORMS Impact Prize, a National Science Foundation CAREER award, and a Department of the Army Young Investigator Award, and a Fulbright Award. She is the author of the blogs "Punk Rock Operations Research" and "Badger Bracketology."

Alexander Nikolaev, PhD, is an associate professor in the Department of Industrial and Systems Engineering at the University at Buffalo. He has a BSc from Moscow Institute of Physics and Technology, and MS from the Ohio State University and PhD from University of Illinois at Urbana-Champaign (both in industrial engineering). Dr. Nikolaev's interests and expertise are in resource allocation under uncertainty, social network analysis, causal inference, and decision-making that supports pro-health, pro-environmental and educational programs. He has (co)authored 65 publications in archival journals and refereed proceedings and was a (co)recipient of INFORMS Impact Prize and University at Buffalo Teaching Innovation Award.

Sheldon H. Jacobson, PhD, is a Founder Professor in the Department of Computer Science at the University of Illinois at Urbana-Champaign. He has a BSc and MSc (both in mathematics) from McGill University, and a PhD (in operations research) from Cornell University. Jacobson's research focuses on data-driven risk-based decision-making applied to problems in public health and public policy. He has been working on the design and analysis of aviation security systems using operations research and artificial intelligence models since 1995. He has received numerous awards for this research, including a John Simon Guggenheim Memorial Foundation Fellowship, the IISE David F. Baker Distinguished Research Award, the INFORMS Impact Prize. He is an elected Fellow of INFORMS, IISE, and the American Association for the Advancement of Science (AAAS).

ORCID

Laura A. Albert http://orcid.org/0000-0001-7079-4473
Alexander Nikolaev http://orcid.org/0000-0002-5364-0672
Sheldon H. Jacobson http://orcid.org/0000-0002-9042-8750

References

Albert, L.A., Nikolaev, A., Lee, A.J., Fletcher, K. and Jacobson, S.H. (2020) A review of risk-based security and its impact on TSA precheck. *IISE Transactions*, **53**(6), 657–670.

Alderson, D.L., Brown, G.G. and Carlyle, W.M. (2015) Operational models of infrastructure resilience. *Risk Analysis*, **35**(4), 562–586.

Bakshi, N., Flynn, S.E. and Gans, N. (2011) Estimating the operational impact of container inspections at international ports. *Management Science*, **57**(1), 1–20.

Barnett, A. (2004) CAPPS II: The foundation of aviation security? *Risk Analysis*, **24**(4), 909–916.

Baroud, H. (2021) Risk analysis methods in resilience modeling: An overview of critical infrastructure applications. *Applied Risk Analysis for Guiding Homeland Security Policy*, **24**, 357–379.

Biden, J. (2021) Executive Order on Improving the Nation's Cybersecurity. 5(22). https://www.whitehouse.gov/briefing-room/presidential-actions/2021

/05/12/executive-order-on-improving-the-nations-cybersecurity/. (accessed 22 May 2021).
Bier, V., Oliveros, S. and Samuelson, L. (2007) Choosing what to protect: Strategic defensive allocation against an unknown attacker. *Journal of Public Economic Theory*, **9**(4), 563–587.
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*, **28**(3), 763–770.
Boros, E., Fedzhora, L., Kantor, P., Saeger, K. and Stroud, P. (2009) A large-scale linear programming model for finding optimal container inspection strategies. *Naval Research Logistics*, **56**(5), 404–420.
Boros, E., Goldberg, N., Kantor, P.B. and Word, J. (2011) Optimal sequential inspection policies. *Annals of Operations Research*, **187**(1), 89–119.
Brown, G., Carlyle, M., Salmerón, J. and Wood, K. (2006) Defending critical infrastructure. *Interfaces*, **36**(6), 530–544.
Brown, G.G., Carlyle, W.M., Harney, R.C., Skroch, E.M. and Wood, R.K. (2009) Interdicting a nuclear-weapons project. *Operations Research*, **57**(4), 866–877.
Brown, G.G. and Cox, L.A. Jr. (2011) How probabilistic risk assessment can mislead terrorism risk analysts. *Risk Analysis*, **31**(2), 196–204.
Casorrán, C., Fortz, B., Labbé, M. and Ordóñez, F. (2019) A study of general and security Stackelberg game formulations. *European Journal of Operational Research*, **278**(3), 855–868.
Caunhye, A.M., Nie, X. and Pokharel, S. (2012) Optimization models in emergency logistics: A literature review. *Socio-economic Planning Sciences*, **46**(1), 4–13.
Church, R.L. and Scaparra, M.P. (2007) Protecting critical assets: The r-interdiction median problem with fortification. *Geographical Analysis*, **39**(2), 129–146.
Cox, L.A. Jr. (2008) Some limitations of "risk = threat x vulnerability x consequence" for risk analysis of terrorist attacks. *Risk Analysis*, **28**(6), 1749–1761.
Des Mesnards, N.G., Hunter, D.S., El Hjouji, Z. and Zaman, T. (2021) Detecting bots and assessing their impact in social networks. *Operations Research*, **70**(1), 1–22.
Dimitrov, N.B., Michalopoulos, D.P., Morton, D.P., Nehme, M.V., Pan, F., Popova, E., Schneider, E.A. and Thoreson, G.G. (2011) Network deployment of radiation detectors with physics-based detection probability calculations. *Annals of Operations Research*, **187**(1), 207–228.
Enayaty-Ahangar, F., Albert, L.A. and DuBois, E. (2020) A survey of optimization models and methods for cyberinfrastructure security. *IISE Transactions*, **53**(2), 182–198.
Ezell, B.C., Bennett, S.P., Von Winterfeldt, D., Sokolowski, J. and Collins, A.J. (2010) Probabilistic risk analysis and terrorism risk. *Risk Analysis*, **30**(4), 575–589.
Farasat, A., Gross, G., Nagi, R. and Nikolaev, A.G. (2016) Social network analysis with data fusion. *IEEE Transactions on Computational Social Systems*, **3**(2), 88–99.
Galindo, G. and Batta, R. (2013) Review of recent developments in OR/MS research in disaster operations management. *European Journal of Operational Research*, **230**(2), 201–211.
Gaukler, G.M., Li, C., Cannaday, R., Chirayath, S.S. and Ding, Y. (2011) Detecting nuclear materials smuggling: Using radiography to improve container inspection policies. *Annals of Operations Research*, **187**(1), 65–87.
Gaukler, G.M., Li, C., Ding, Y. and Chirayath, S.S. (2012) Detecting nuclear materials smuggling: Performance evaluation of container inspection policies. *Risk Analysis*, **32**(3), 531–554.
Golany, B., Kaplan, E.H., Marmur, A. and Rothblum, U.G. (2009) Nature plays with dice–terrorists do not: Allocating resources to counter strategic versus probabilistic risks. *European Journal of Operational Research*, **192**(1), 198–208.
Greenberg, M., Cox, A., Bier, V., Lambert, J., Lowrie, K., North, W., Siegrist, M. and Wu, F. (2020) Risk analysis: Celebrating the accomplishments and embracing ongoing challenges. *Risk Analysis*, **40**(S1), 2113–2127.
Greenberg, M., Haas, C., Cox, Jr., A., Lowrie, K., McComas, K. and North, W. (2012) Ten most important accomplishments in risk analysis, 1980–2010. *Risk Analysis*, **32**(5), 771.
Haphuriwat, N. and Bier, V.M. (2011) Trade-offs between target hardening and overarching protection. *European Journal of Operational Research*, **213**(1), 320–328.
Hunt, K., Agarwal, P., Al Aziz, R. and Zhuang, J. (2020) Fighting fake news during disasters. *OR/MS Today*, **47**(1), 34–39.
Israeli, E. and Wood, R.K. (2002) Shortest-path network interdiction. *Networks*, **40**, 97–111.
Jacobson, S.H., Virta, J.L., Bowman, J.M., Kobza, J.E. and Nestor, J.J. (2003) Modeling aviation baggage screening security systems: A case study. *IIE Transactions*, **35**(3), 259–269.
Jain, M., Kardes, E., Kiekintveld, C., Ordónez, F. and Tambe, M. (2010) Security games with arbitrary schedules: A branch and price approach, in *Proceedings of the AAAI Conference on Artificial Intelligence*, Atlanta, GA, USA, July 11–15, Association for the Advancement of Artificial Intelligence, volume **24**, pp. 792–797.
Jain, M., Tsai, J., Pita, J., Kiekintveld, C., Rathi, S., Tambe, M. and Ordónez, F. (2010) Software assistants for randomized patrol planning for the LAX airport police and the Federal Air Marshal Service. *Interfaces*, **40**(4), 267–290.
Jenkins, M.P., Gross, G.A., Bisantz, A.M. and Nagi, R. (2015) Towards context aware data fusion: Modeling and integration of situationally qualified human observations to manage uncertainty in a hard + soft fusion process. *Information Fusion*, **21**, 130–144.
Jia, H., Ordonez, F. and Dessouky, M.M. (2007) Solution approaches for facility location of medical supplies for large-scale emergencies. *Computers & Industrial Engineering*, **52**(2), 257–276.
Kaplan, E.H. (2010) Terror queues. *Operations Research*, **58**(4), 773–784.
Kaplan, E.H., Craft, D.L. and Wein, L.M. (2002) Emergency response to a smallpox attack: The case for mass vaccination. *Proceedings of the National Academy of Sciences*, **99**(16), 10935–10940.
Kaplan, E.H. and Kress, M. (2005) Operational effectiveness of suicide-bomber-detector schemes: A best-case analysis. *Proceedings of the National Academy of Sciences*, **102**(29), 10399–10404.
Khouzani, M., Liu, Z. and Malacaria, P. (2019) Scalable min-max multi-objective cyber-security optimisation over probabilistic attack graphs. *European Journal of Operational Research*, **278**(3), 894–903.
Klausen, J., Marks, C.E. and Zaman, T. (2018) Finding extremists in online social networks. *Operations Research*, **66**(4), 957–976.
Konrad, R.A., Trapp, A.C., Palmbach, T.M. and Blom, J.S. (2017) Overcoming human trafficking via operations research and analytics: Opportunities for methods, models, and applications. *European Journal of Operational Research*, **259**(2), 733–745.
Larson, R.C. (2004) OR models for homeland security. *OR/MS Today*, **31**(5), 22–29.
Lawson, C.H. (2021) What covid teaches us about homeland security: How not to be the mouse. *Journal of Homeland Security and Emergency Management*, **18**(3), 335–346.
Lee, A.J. and Jacobson, S.H. (2011) The impact of aviation checkpoint queues on optimizing security screening effectiveness. *Reliability Engineering & System Safety*, **96**(8), 900–911.
Lee, A.J., McLay, L.A. and Jacobson, S.H. (2009) Designing aviation security passenger screening systems using nonlinear control. *SIAM Journal on Control and Optimization*, **48**(4), 2085–2105.
Lim, G.J., Cho, J., Bora, S., Biobaku, T. and Parsaei, H. (2018) Models and computational algorithms for maritime risk analysis: A review. *Annals of Operations Research*, **271**(2), 765–786.
Martonosi, S.E. and Barnett, A. (2006) How effective is security screening of airline passengers? *Interfaces*, **36**(6), 545–552.
McLay, L.A. and Dreiding, R. (2012) Multilevel, threshold-based policies for cargo container security screening systems. *European Journal of Operational Research*, **220**(2), 522–529.
McLay, L.A., Jacobson, S.H. and Kobza, J.E. (2006) A multilevel passenger screening problem for aviation security. *Naval Research Logistics*, **53**(3), 183–197.

McLay, L.A., Jacobson, S.H. and Kobza, J.E. (2007) Integer programming models and analysis for a multilevel passenger screening problem. *IIE Transactions*, **39**(1), 73–81.

McLay, L.A., Jacobson, S.H. and Nikolaev, A.G. (2009) A sequential stochastic passenger screening problem for aviation security. *IIE Transactions*, **41**(6), 575–591.

McLay, L.A., Lee, A.J. and Jacobson, S.H. (2010) Risk-based policies for airport security checkpoint screening. *Transportation Science*, **44**(3), 333–349.

Mete, H.O. and Zabinsky, Z.B. (2010) Stochastic optimization of medical supply location and distribution in disaster management. *International Journal of Production Economics*, **126**(1), 76–84.

Morse, P.M., Kimball, G.E. (1946). Methods of operations research. Center for Naval Analyses Alexandria va Operations Evaluation Group.

Morton, D.P., Pan, F. and Saeger, K.J. (2007) Models for nuclear smuggling interdiction. *IIE Transactions*, **39**(1), 3–14.

Nie, X., Batta, R., Drury, C.G. and Lin, L. (2009) Passenger grouping with risk levels in an airport security system. *European Journal of Operational Research*, **194**(2), 574–584.

Nikolaev, A.G., Jacobson, S.H. and McLay, L.A. (2007) A sequential stochastic security system design problem for aviation security. *Transportation Science*, **41**(2), 182–194.

Pan, F. and Morton, D.P. (2008) Minimizing a stochastic maximum-reliability path. *Networks*, **52**(3), 111–119.

Paul, H. and Nikolaev, A. (2021) Fake review detection on online e-commerce platforms: A systematic literature review. *Data Mining and Knowledge Discovery*, **35**, 1830–1881.

Pay, B.S., Merrick, J.R. and Song, Y. (2019) Stochastic network interdiction with incomplete preference. *Networks*, **73**(1), 3–22.

Popp, R.L. and Yen, J. (2006) *Emergent Information Technologies and Enabling Policies for Counter-terrorism*, John Wiley & Sons.

Sefair, J.A. and Smith, J.C. (2016) Dynamic shortest-path interdiction. *Networks*, **68**(4), 315–330.

Simon, J. and Omar, A. (2020) Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research*, **282**(1), 161–171.

Smith, J.C., Lim, C. and Sudargho, F. (2007) Survivable network design under optimal and heuristic interdiction scenarios. *Journal of Global Optimization*, **38**(2), 181–199.

Smith, J.C. and Song, Y. (2020) A survey of network interdiction models and algorithms. *European Journal of Operational Research*, **283**(3), 797–811.

Stone, L.D. (1976) *Theory of Optimal Search*, Elsevier, Mathematics in Science and Engineering, Volume 118, Academic Press Inc.

Su, S. and Nwafor, E. (2021) Detecting network traffic intrusions on memory constrained embedded systems, in *Proceedings of the 2021 IEEE International Symposium on Technologies for Homeland Security (HST)*, IEEE Press, Piscataway, NJ, pp. 1–5.

Von Winterfeldt, D. and O'Sullivan, T.M. (2006) Should we protect commercial airplanes against surface-to-air missile attacks by terrorists? *Decision Analysis*, **3**(2), 63–75.

Wang, C. and Bier, V.M. (2011) Target-hardening decisions based on uncertain multiattribute terrorist utility. *Decision Analysis*, **8**(4), 286–302.

Wein, L.M., Craft, D.L. and Kaplan, E.H. (2003) Emergency response to an anthrax attack. *Proceedings of the National Academy of Sciences*, **100**(7), 4346–4351.

Wein, L.M. and Liu, Y. (2005) Analyzing a bioterror attack on the food supply: The case of botulinum toxin in milk. *Proceedings of the National Academy of Sciences*, **102**(28), 9984–9989.

Willis, H.H. (2007) Guiding resource allocations based on terrorism risk. *Risk Analysis*, **27**(3), 597–606.

Wood, R.K. (1993) Deterministic network interdiction. *Mathematical and Computer Modeling*, **17**(2), 1–18.

Wright, P.D., Liberatore, M.J. and Nydick, R.L. (2006) A survey of operations research models and applications in homeland security. *Interfaces*, **36**(6), 514–529.

Zheng, K. and Albert, L.A. (2019) Interdiction models for delaying adversarial attacks against critical information technology infrastructure. *Naval Research Logistics (NRL)*, **66**(5), 411–429.

Zheng, K., Albert, L.A., Luedtke, J.R. and Towle, E. (2019) A budgeted maximum multiple coverage model for cybersecurity planning and management. *IISE Transactions*, **51**(12), 1303–1317.

Zhuang, J. and Bier, V.M. (2007) Balancing terrorism and natural disasters—defensive strategy with endogenous attacker effort. *Operations Research*, **55**(5), 976–991.