Manuscript ID POM-Mar-17-OA-0137.R4

Prevention of Terrorism–An Assessment of Prior POM Work and Future Potentials

Sushil Gupta
College of Business Administration, Florida International University, RB 250, 11200 S.W. 8th St, Miami, Florida 33199, USA
guptask@fiu.edu

Martin K. Starr
Crummer GSB, Rollins College, GSB, Columbia University, 100 S. Interlachen Avenue #304, Winter Park, Florida 32789, USA
starr@columbia.edu

Reza Zanjirani Farahani ***(Corresponding author)***
Kingston Business School, Kingston University London, Kingston Hill, Kingston Upon Thames, Surrey, KT2 7LB, UK
r.zanjiranifarahani@kingston.ac.uk; ; zanjiranireza@gmail.com

Mahsa Mahboob Ghodsi
GERAD, HEC Montréal, Montréal, Canada
mahsa.mahboob-ghodsi@hec.ca

Abstract

In this paper, we review POM-based research related to prevention of terrorism. According to the Federal Emergency Management Agency (FEMA) terrorist attacks have the potential to be prevented. Consequently, the focus of this paper is on security enhancement and improving the resiliency of a nation to prevent terrorist attacks. Accordingly, we review articles from the 25 top journals, [following procedures developed by Gupta et al. (2016)], in the fields of Production and Operations Management, Operations Research, Management Science and Supply Chain Management. In addition, we searched some selected journals in the fields of Information Sciences, Political Science and Economics. This literature is organized and reviewed under the following seven core capabilities defined by the Department of Homeland Security (DHS): (1) Intelligence and Information Sharing, (2) Planning, (3) Interdiction and Disruption, (4) Screening, Search, and Detection, (5) Forensics and Attribution, (6) Public Information and Warning, and (7) Operational Coordination. We found that POM research on terrorism is primarily driven by the type of information that a defending country and a terrorist have about each other. Game theory is the main technique that is used in most research

papers. Possible directions for future research are discussed.

Keywords: prevention; terrorist attack; disaster management; humanitarian operations; weapons of mass destruction; disaster supply chains; and Federal Emergency Management Agency.

History: Received: March 2017; Accepted: April 2020 by Kalyan Singhal, after 4 revisions.

1. Introduction

Tuesday, September 11, 2001 witnessed a dastardly act in human history which epitomizes the extreme malevolence of terrorists and their incredible level of planning and coordination. An unusual weapon system, (viz., hijacked airplanes), was used to attack simultaneously the world trade center and the pentagon in the U.S.A. At least one additional target was not achieved. This attack is often referred to as "the 9/11 attacks." *The National Commission on Terrorist Attacks Upon the United States (The Commission henceforth)* was created to investigate the incidents leading to this attack and to develop recommendations to avoid such incidents in the future. According to The Commission's report (page 340), "*Measured on a governmental scale, the resources behind it were trivial."* However, it was an intelligent, malevolent enemy and the U.S.A. was caught by surprise. How do we secure the Nation from such enemies? Can such incidents be prevented in the future? This POM research is intended to support decision making to improve the fight against terrorism. POM research can zero-in on questions that include but are not limited to profiling terrorists, search and screen policies at airports and seaports, study of terrorists' supply chains, securing infrastructure, and improving warning signals.

In the U.S.A., the Department of Homeland Security (DHS) is responsible for managing disasters. DHS (2015) has defined the following five *mission areas* to combat and face challenges posed by catastrophic disasters: prevention, protection, mitigation, response, and recovery. Gupta et al. (2016) in their survey paper mentioned: "Sound prevention/mitigation strategies can possibly reduce efforts and resources spent on humanitarian logistics activities."

The current paper discusses research contributions in the following seven core capabilities defined by DHS (2015) for the mission area "prevention": 1. Intelligence and Information Sharing, 2. Planning, 3. Interdiction and Disruption, 4. Screening, Search and Detection, 5. Forensics and Attribution, 6. Public Information and Warning, and 7. Operational Coordination. These core capabilities are discussed in detail in Section A1 of the online appendix. The interactions between core capabilities are depicted in Figure 1.

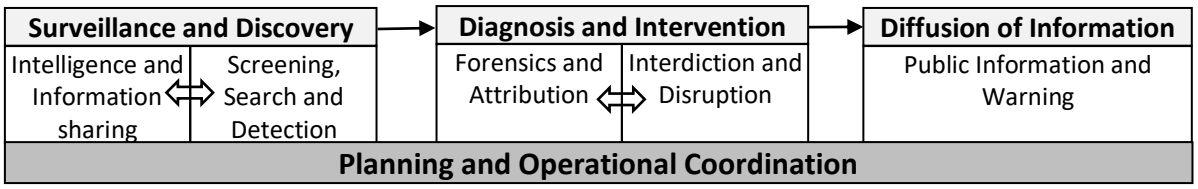

Figure 1: Core capabilities and their interactions.

These seven core capabilities fall within the research and practice domain of Production and Operations Management (POM). Therefore, it is necessary for POM researchers working in disaster management to understand and focus on these core capabilities. They must extend their vision to encompass new technological developments while enhancing their research agenda to meet the challenges of terrorism that are also evolving because of changing technological abilities.

The core capabilities numbers 1 through 5 are discussed in Sections 2 through 6 respectively. The core capabilities Public Information and Warning (number 6) and Operational Coordination (number 7) are discussed in sections A7 and A8 respectively in the online appendix since we did not find any papers that focus on these core capabilities. Section 7 includes conclusions and directions for future research.

1.1. Chronology of Growth in Prevention of Terrorism Research

We identified 91 papers published in top-ranking journals whose contributions are worthy of discussion in this paper. Section A2 “Search Methodology” in the online appendix explains the process for identifying these papers. Figure 2 is a graphical depiction of the three-year moving average of the published papers. Since the year 2001, interest in terrorism research gained momentum due to the 9/11 attacks in the U.S.A. and their global consequence. Considering the lead time of several years to write publishable papers since the 9/11 attacks, the years 2004-2010 witnessed a growth in terrorism research. The three-year moving average peaked in 2012-2014. We see a little decline over recent years. It seems the area, as it is, has reached maturity unless we introduce important future research directions. This survey paper might inspire some new work.

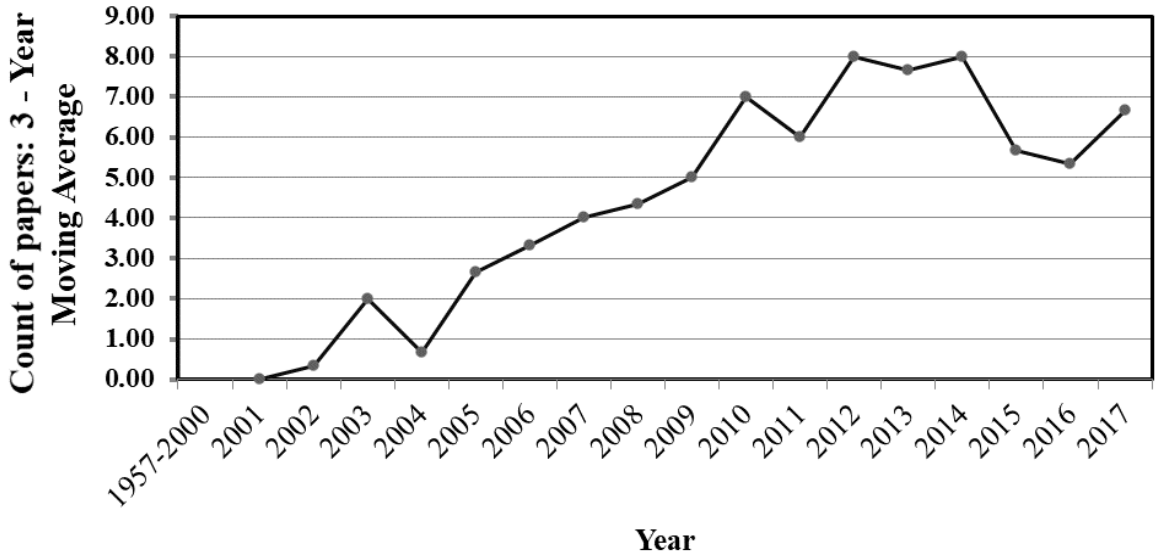

Figure 2: Three-year moving average of the count of 91 papers.

Table A1 in the online appendix gives the count of papers by year for each DHS core capability. Opportunities for research seem to exist for the categories with only a few papers. Three additional tables in the online appendix include cross-tabulation of core capabilities vs. data type (Table A2), cross-tabulation of core capabilities vs. analytical technique (Table A3), and cross-tabulations of data types vs. analytical techniques (Table A4).

2. Intelligence and Information Sharing

Acquisition, processing and dissemination of terrorism-related intelligence is the subject matter of this section. Figure 3 lists the research streams in this core capability.

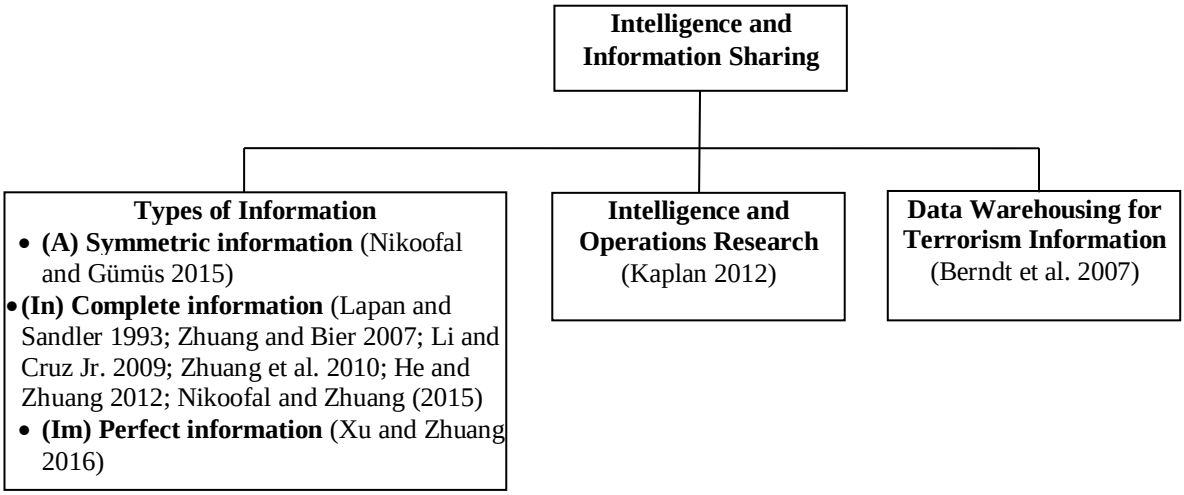

Figure 3: Categorization of the terrorism prevention research on Intelligence and Information Sharing.

2.1. Types of Information

In this section, we discuss research papers that focus on the following types of information: symmetric vs. asymmetric, complete vs. incomplete, and perfect vs. imperfect.

2.1.1. Symmetric vs. asymmetric information

Information symmetry means equality of knowledge among all players whereas a*symmetric information* refers to a situation where one player possesses better information than the opponent. This may occur if one of the players can perceive hidden actions of the opponent (e.g., information from spying). In a two-player game, we may have either defenders or attackers benefitting from asymmetric information.

Nikoofal and Gümüs (2015) study the impact of an unforeseeable terrorist's information about the government's spending priorities for the protection of targets. The authors show that (1) the value of information related to target preference is positive when the degree of information asymmetry is high enough; (2) the value of information enlarges the government's budget at the beginning of the process; and later, decreases; (3) the value of information is correlated (both positive and negative) with the degree of heterogeneity between targets; and, (4) the value of target information is not altered by the effectiveness ratio of attack, but the impact of that ratio on the value of rationality depends on the actual nature of the terrorist.

2.1.2. Complete vs. incomplete information

Complete information refers to the situation in which knowledge about all aspects of the game such as payoffs, strategies, utility functions and types of players is available to all players; otherwise, we will have a game with *incomplete information.*

Lapan and Sandler (1993) study a signaling game between an informed defender and an attacker. The attacker has complete information about the defender's strategy. However, the defender has incomplete information about the attacker's resources. The authors employ a two-period model.

Based on the attacker's behavior in the first period, the defender, in the second period, updates her[1] information about the attacker's resources using Bayesian methodology. The authors show that equilibrium occurs if each player makes its own optimal decision in every move. The main finding of the research is that the government should choose a partial-pooling signaling equilibrium (i.e., it is also called semi-separating where sometimes both players choose the same strategy and sometimes different ones) against a no-surrender attacker. We have not defined "equilibrium" in this paper because (Nash/Stackelberg) equilibriums are well-known concepts in game theory.

It is possible that inaccurate information may be signaled by one player to another that may lead to deception. We discuss below the papers that focus on deception, secrecy vs. deception, disclosure vs. secrecy, and agreement between two players.

Deception: Li and Cruz Jr. (2009) analyze the role of deception in a game-theoretic model. The authors classify deception in two categories: (i) "passive deception" that conceals reality with noise and (ii) "active deception" in which misleading signals are sent leading the opponent to make wrong decisions. The effectiveness of the deception is based on the measurement accuracy of the player receiving the information and the quality of the misleading signals sent by the deceiver. The authors derive conditions under which deception will be effective. They suggest extending the model to multi-player games and the impact of learning in repeated games. The authors show that, counter-intuitively, the introduction of deception can be harmful in certain applications. Active deception is more likely to be detected when repeated. They derive conditions under which deception will be effective.

Secrecy vs. deception: Zhuang and Bier (2007) study simultaneous and sequential games in a single-period between the attacker and the defender. The authors model secrecy in a simultaneous game in which none of the players are aware of the other players' moves. In the sequential game, the defender moves first, and the attacker chooses his level of effort after observing the defensive investments. The authors consider defensive investment as the only defender's decision variable. The authors suggest that by using Bayesian methods and signaling games it might be possible to relax the

[1] Following the convention in the literature, we use "she/her" for a defender (country) and "he/him" for a terrorist.

assumption of perfect information. The main finding of the research is that the defender should be involved in a sequential rather than a simultaneous game. Moreover, the defender should not try to deter an attack if it is of high cost. Zhuang et al. (2010) also model secrecy and deception using game theory in a multiple-period game with incomplete information about defense effectiveness, target valuations, and costs. They analyze a finite game between a single attacker and a single defender where the defender has private information. The defender's signals in each period include truthful disclosure, secrecy, and deception. These signals and the result of the game in each period are used by the attacker to update his information about the defender type. The authors study the tradeoff between capital investment and expenses and show that secrecy and deception lead to greater cost-effectiveness that lasts over multiple periods. This paper explains that deception may lead to the loss of defender's credibility in the long run, and the attacker may gain knowledge about the defender's private information through repeated attacks. The authors state that their model can address such scenarios.

Disclosure vs. secrecy: Nikoofal and Zhuang (2015) study the impact of defender's choices between *disclosure* and *secrecy* of her defensive information when facing a strategic terrorist. Disclosure is used in a sequential game whereas secrecy is used in a simultaneous game. These choices are affected by the asymmetry between the target valuations by the attacker and the defender. The analysis shows that the defender, as a first mover, has an advantage over the attacker but this advantage is significant only if both players have a similar valuation of targets. If the valuation of targets by the attacker is higher or lower than the valuation by the defender (i.e., the degree of information asymmetry between the players is high), then the government should not waste its resources by investing more on the high-value targets. The authors also conclude that in a simultaneous game the optimal defence allocation is more robust against uncertainty in the attacker's valuation of targets.

Agreement: He and Zhuang (2012) show that in some situations, either with complete or incomplete information, there is always a possibility that both players accept mutually beneficial arrangements or even contracts. They consider a sequential game in which the government provides positive rent to achieve the terrorist's (partial) attack deterrence. Stopping the attack may result in

lower cost for the defender.

2.1.3. Perfect vs. imperfect information

Perfect information deals with situations in which each player is perfectly aware of all events and their consequences when making a decision. Perfect information has been widely used in decision tree analysis focusing on the value of information. For example, a government may pay a reliable spy to purchase information with the intent of achieving perfect information before making any decision to improve its payoff.

Xu and Zhuang (2016) study a sequential game of imperfect information where vulnerability learning is costly for the attacker, therefore, the attacker could choose to launch an attack or not after the costly learning. The authors investigate the value of perfect and imperfect information for the attacker and show that the attacker's optimal learning and attack strategies and the defender's deception or defense equilibrium are impacted by the attackers learning cost. A counter intitutive finding is that as a result of deception, the attaker may attack when the target is erroneously thought to be vulnerable. The reverse (may not attack) applies when the target is erroneously thought to be invulnerable.

2.2. Intelligence and Operations Research

In the context of terrorism, strategic adversaries can use intelligence to learn the defender's private information by monitoring and testing the government's defensive strategies over time. On the other hand, the defender faces a tradeoff between investing in counter-learning to deceive the attacker and defense to strengthen the target.

Kaplan (2012) provides a comprehensive review of the application of operations research (OR) models to intelligence problems. The author defines intelligence, explains the intelligence production cycle, and discusses different organizations involved in this process. The author provides a survey of various efforts to apply OR techniques to intelligence in the US Intelligence Community and summarizes possible contributions to intelligence by OR which he names intelligence OR. Such OR techniques can be used to investigate how to maximize the quality of intelligence produced. Finding

the optimal intelligence collection portfolio and evaluating the effectiveness of different intelligence activities are other interesting problems amenable to OR modeling. Kaplan (2012) also recommends developing intelligence priorities via the national intelligence priorities framework (NIPF) as a potentially high-impact research area for OR study. Moreover, the author suggests that developing methods for evaluating the effectiveness of different intelligence activities represents a promising future research direction.

2.3. Data Warehousing for Terrorism Information

Data warehousing is important for the use of intelligence in terrorism prevention. Berndt et al. (2007) study the role of data warehousing to improve bioterrorism surveillance systems. Disastrous consequences of biological attacks make them one of the biggest threats to national security. Prevention of such security threats demand intelligent and effective techniques to identify them early enough to respond effectively, viz., to prevent their epidemiological impact. The Florida healthcare data warehouse provides historical context for six years of wildfires that occurred naturally in Florida. The wildfire phenomenon bears a resemblance to bio-attacks. Thus, these authors use this data for suspect health data pattern-recognition. They show that employing online analytic processing (OLAP) techniques and other data analytic techniques (such as statistical models, machine learning techniques, and pattern recognition) together can provide a framework that accelerates discovery and exploration of unusual situations.

2.4. Summary and Future Research

Papers in this section center around the types of information that include: symmetric vs. asymmetric information, complete vs. incomplete information and perfect vs. imperfect information. Some papers focused on the outcomes of deception, secrecy, disclosure and agreement. The role of Intelligence and Operations Research, and data warehousing were also discussed.

Researchers should consider relaxing the assumption of perfect information. This promotes building models under imperfect information and studying games with asymmetric information. While a problem that incorporates asymmetric, incomplete and imperfect information is technically

difficult, researchers should consider the potential rewards of studying such problems. Relaxing the complete information assumption between attacker and defender may provide a more realistic problem. The context of learning and repeated games is another possible direction for future research since the deception signal is likely to be effective only once. Secrecy vs. exposure of information to the opponent is also a fertile research area. Future research can focus on improving the quality of intelligence, finding the optimal intelligence portfolio, and evaluating the effectiveness of different intelligence activities. Large databases (e.g., health data in the case of a bio-terrorism attack) should be developed and be made available to researchers. Data mining, social media, text mining, and tracking social movements can provide intelligence in the early stages of a terrorist attack. Technical knowledge transfer about the growth of extremist groups is another example of the use of information analysis. Finally, buying information before making decisions (e.g., through a reliable spy system) can be an interesting research subject.

3. Planning

Planning is defined by DHS as carrying out a step-by-step process to make decisions on strategic, operational and tactical levels to prevent terrorist attacks (DHS, 2015). Keeney (2007) is one of the few papers that introduces a general step-by-step procedure focusing on actions and interactions between the DHS and a terrorist: (1) the DHS considers its possible alternatives and makes her first decision; (2) the terrorist takes an action; (3) the DHS responds by making her second decisions; (4) the terrorist takes his second action and (5) finally, the public responds to these interactions. Keeney (2007) also identifies appropriate objectives to be used in value models to be utilized in anti-terrorism. These objectives include: minimizing loss of health, safety and life and also the number of deaths, injuries, disabled, economic damage (personal, business, government) and future terrorism. Figure 4 illustrates research streams in the core capability of "Planning".

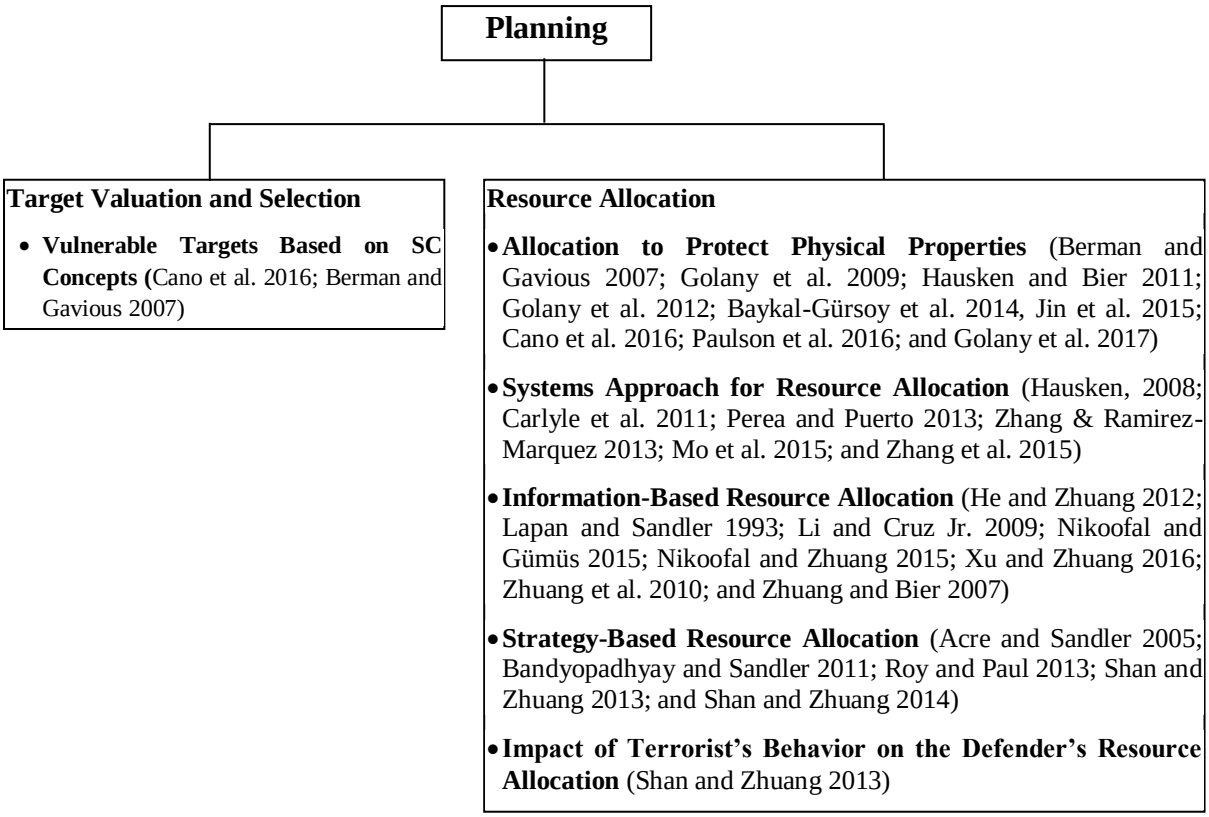

Figure 4: Categorization of published papers on terrorism prevention that are based on Planning research.

3.1. Target Valuation and Selection

Defender's vulnerable assets include the following among others: public places, train stations, airports, transportation systems, government buildings, roads, bridges, embassies and schools. These targets may have different importance, also called valuation in this paper, for the attacker and for the defender. The selection of target (s) depends on the terrorist's goals and may include one or more of the following: publicity for the terrorist organization, hatred towards the victim nation, political power, financial gains, killing people with different values and religious beliefs, etc.

Terrorist groups hold varying beliefs and values about human life, religion, politics, money, etc. which motivate them to commit disastrous acts. For example, in the case of the 9/11 bombings, The Commission describes the attacker's motive as, "*Its purpose is to rid the world of religious and political pluralism, the plebiscite, and equal rights for women. It makes no distinction between military and civilian targets. Collateral damage is not in its lexicon."*

Target selection is a strategic decision made by high-ranking leaders of the terrorist organization. For example, in the 9/11 bombings, *"Bin Ladin, Atef, and KSM developed an initial list of targets.*

These included the White House, the U.S. Capitol, the Pentagon, and the World Trade Center. According to KSM, Bin Ladin wanted to destroy the White House and the Pentagon, KSM wanted to strike the World Trade Center, and all of them wanted to hit the Capitol. No one else was involved in the initial selection of targets," (The Commission, page 155). The full names of the people in quotes are: Bin Ladin (Usama Bin Ladin), head of Al Qaeda; Atef (Mohammed Atef), al Qaeda military commander, and KSM (Khalid Sheikh Mohammed), mastermind of the 9/11 attacks.

Strategies for preventing terrorist attacks include budget allocation, intelligence, detection, deterrence, negotiations, defensive policies and proactive actions. Papers related to these strategies are not discussed here since planning cuts across all core capabilities and these strategies are discussed in other relevant sections.

3.1.1. Vulnerable Targets Based on SC Concepts

Borrowing the terminology from SC concepts, we identify downstream and upstream targets. An attack could be planned downstream or upstream with different objectives as discussed below.

Airports, train stations, schools, universities, shopping centers, cinemas, sports stadiums, hotels, tourist attractions, museums, leisure centers, etc. are downstream targets. At these locations, people socialize, relax, live and visit. Among these facilities, transportation systems comprising infrastructures (airport, train station, and seaport) and moving entities (vehicles, passengers and airplanes) are of great importance. For example, Cano et al. (2016) study the case of an airport with a special focus on terrorist attacks against the Air Traffic Control Tower. They aim to reduce the probability of attack through resource allocation. Terrorists may attack all these components in all transportation modes namely land, sea, and air. These threats are not limited to passenger transportation networks and may be extended to cargo transportation. Berman and Gavious (2007) study a Stackelberg game played by a terrorist (attacker) and a state; the attacker is the leader. The terrorist attacks one or more metropolitan areas. The follower (defender) intends to identify the appropriate location of facilities in a metropolitan area to minimize loss. Both players are aware of each other's behavior. Berman and Gavious mathematically formulate the problem and test it on the 20 largest metropolitan areas in the U.S. They show that there is a unique, optimal number of facilities

to defend. Increasing the number of facilities beyond this number does not make any further improvement.

Terrorists also aim on sabotaging power grids, energy systems, cyber networks, oil pipelines, and water systems, etc. These targets can be considered as the upstream part of SCs. In such cases, the attack may or may not leave casualties, but its social costs and media impacts are high. A series of bombs that targeted British Columbia gas pipelines during 2008–09, and the Dalles, Oregon water supply tank contamination in 1984 are instances of such terrorist attacks. Electric power, telecommunications, banking and finance, petroleum and natural gas, food infrastructure and space systems fall within this category. Similarly, falling within this category are dams and locks, factories, power plants and refineries are examples of such targets in the U.S.A.

In general, we observe that regardless of the reasons for terrorist acts (patriotism, racism, religion, etc.), they mainly attack non-military, non-hardened or weakly defended targets rather than military bases. These are soft targets which are low cost, high impact. Hardening is toughening sensitive targets by putting up barriers or reinforcing vulnerable building.

3.2. Resource Allocation

Appropriate resource allocation, as discussed below, is important to prevent, delay, or reduce damage in terror activities.

3.2.1. Allocation to Protect Physical Properties

The research studies in this sub-section focus on either general resource allocation problems or transportation networks. Among them, Golany et al. (2009) is the only research that considers terrorist attacks and natural disasters together. They conduct a comparative study about mitigating consequences of unexpected disruptive events with probabilistic uncertainty (for natural disasters) and strategic uncertainty (for terrorist attacks). The research shows that when facing probabilistic uncertainty, the government should allocate its resources based on priority for those locations with the highest impact. In the case of strategic uncertainty, the government should spread its resources among the most vulnerable sites. Natural disasters are excluded in Golany et al. (2012) and Golany et al.

(2017). These two papers consider allocation of substitutable resources to protect multiple targets. The effectiveness of various resources to protect each target will differ. In both papers, Nash equilibrium and properties of allocations are determined. Golany et al. (2012) study the case of multiple resources whereas Golany et al. (2017) focus on two resources and suggest an efficient algorithm to calculate the equilibria.

Hausken and Bier (2011) have introduced the concept of multiple attackers in both simultaneous and sequential games under the assumption that attackers are heterogeneous having different strengths and different valuations of the asset. The authors investigate three scenarios: (1) the defender moves first by allocating resources, but the attackers do not have information about the defender's move; (2) the defender and the attackers move simultaneously; and (3) the attackers move first and then the defender decides about resource allocation. The defender wants to know whether to protect her assets against the stronger or the weaker attacker or consider the total strength of the attackers. An application of this problem is in computer security problems. The research shows that players' defense/attack costs, their valuations of targets and the number of attacks affect their decisions. In a simultaneous single-period game withdrawal is not an option; but it can be a potential decision in a two-period game. In the presence of a stronger attacker, the weaker attacker might withdraw if the weaker attacker's valuation of the asset is not high enough. In such a situation, the defender need to consider only the stronger attacker. Additionally, the defender may decide to deter the attack by moving first; otherwise, she may suffer from being attacked.

Paulson et al. (2016) have extended the resource allocation problem to multiple criteria. Paulson et al. (2016) combine game-theoretic concepts with multi-attribute utility functions for the resource allocation problem. The defender has a set of countermeasures and a set of possible targets to protect. She allocates resources to each pair of countermeasures and targets. The attacker then selects a target and the type of attack. After an attack is launched, depending on whether the attack is successful or not, the payoff is calculated.

In addition to the papers discussed above for general resource allocation problems, there are some papers that focus on different modes of transportation networks such as road, rail and air. Berman and Gavious (2007) study a set of cities connected by road networks. A rational terrorist is

likely to attack cities based on different probability assessments regarding maximizing damage. The authors assume that terrorists might know the location of resources and attack a city accordingly. In addition to the location of resources, the authors assume that the defender could invest a part of the resources on prevention. In case of an attack on a city, resources from all over the network will be shipped to that city through the shortest path. The problem is formulated as a leader-follower game between a defender and an attacker where the defender moves first to locate resources. The authors define a damage cost measure for the nation as a function of delay time experienced by the victim city in receiving resources.

Berman and Gavious (2007) have assumed unlimited resources. This assumption has been relaxed by Baykal-Gürsoy et al. (2014) to study a transportation network. The authors argue that transportation infrastructure is susceptible to terrorist attacks because of mass transit systems characterized by continuous service hours. The attacker plans to damage the nodes of the transportation network to maximize damage while the defender plans to allocate limited resources like emergency personnel to find the attacker for the security of the infrastructures. Using static and dynamic versions of the problem, the authors study the security of transportation infrastructures via hide-and-seek games. In this modeling approach, a defender allocates resources such as emergency personnel to various sites to find the adversary's hidden bomb or a person with evil intention. The researchers show that for the static game, there is a unique equilibrium under certain conditions. For the dynamic game, the best strategy is identified based on Markov decision processes.

Jin et al. (2015) also study a game between an attacker and a defender in the context of an urban rail transit network. The authors have included the user of the system as one of the decision makers. This study involves decisions at three levels: defender, attacker and user. The defender allocates resources among vulnerable stations. Based on this information, the attacker selects rail stations to attack. The attacker can consider multiple coordinated attacks applied to various locations with different intensities. In the end, according to the previously made decisions, the user decides what path to choose to travel. To include users, a network flow model is utilized to embed their travel patterns.

Air transport systems have always been attractive targets for terrorists. The only research study

related to air transportation that we found, is Cano et al. (2016). Unlike the previous research, Cano et al. (2016) does not study the resource allocation problem at transportation network level. This study is concerned with the safety of Air Traffic Control (ATC). The authors focus on allocating resources among portfolios composed of protective investments in cameras, metal detectors, X-ray devices, police, and private security forces, etc. all aimed at minimizing the likelihood of attack. The attacker calculates his damage (preparation costs, lives lost, or the possibility of being imprisoned), for the deployed preventive measures and then decides whether to attack the ATC tower or not. The authors develop a sequential defend-attack model and suggest an adversarial risk analysis (ARA) to devise the best deployment strategy.

3.2.2. Systems Approach for Resource Allocation

In this subsection, resource allocation problems are discussed in which a system constituting of several components are involved. Hardening components, and series and parallel systems are the most popular approaches studied in the literature. Hausken (2008) studies both series and parallel systems in which components may have different probabilities of failure or being damaged. After any adverse event, if there exists at least one connected path from the start to the end, the system is considered as not having failed. The defender wants to maximize the system's reliability within a limited budget and identifies the components that need to be strengthened by investing resources in hardening those components. The findings show that the defender benefits from the substitution of components in parallel systems. Therefore, series systems are the attacker's favorite target while defenders benefit from parallel system designs.

Compared to Hausken (2008), Mo et al. (2015) study only parallel systems to provide protection and redundancy. Mo et al. (2015) analyze protection and redundancy as two alternatives in parallel systems exposed to attack. An attack is successful when all system components are destroyed by the attacker. The authors study the following two strategies: (1) increase protection of all existing components, and (2) create new identical redundant components in the network. They consider the defense cost associated with each strategy as a criterion for comparison. To create redundant components, the authors have compared the impact of the construction pace of creating these

components. The two construction pace strategies include geometric (aka rapid) and constant. The system destruction probability is minimized by the geometric pace. They analyze system vulnerability as a function of time. They show that a larger investment in protection (1) leads to decreased system vulnerability; (2) and that deploying more resources in building redundant components causes a system's vulnerability to decrease over time.

Unlike the previous studies which are based on series or parallel systems, Carlyle et al. (2011) study whether a large system that enjoys economies of scale is better than several smaller systems. An example will be the design of a hospital system – one large hospital or several smaller hospitals. Both types of systems are likely to face disruptions due to intentional attackers. The authors consider two types of attacks: (1) deterministic incremental and (2) zero-one random-outcome (ZORO). In the case of deterministic incremental attacks, the capacity of an attacked system is partially decreased while in ZORO, after a successful attack, either all capacity is knocked out or there is no damage. ZORO attacks result when the attackers are strong whereas incremental attacks occur when the attackers do not possess extensive damaging capacity. The results suggest that large systems are preferred while facing incremental attacks whereas several smaller systems are desirable in case of ZORO attacks.

Perea and Puerto (2013), Zhang and Ramirez-Marquez (2013) and Zhang et al. (2015) also study protecting critical infrastructures that can be represented through a flow network. Maximization of network flow between two nodes is the measure of an appropriate fortification for the defender, and a decrease in the network flow represents damage to the network for the attacker. Among these three papers, Perea and Puerto (2013) focuses on a practical problem with application to rail transportation but the other two are more generic. All three papers use game theory as an analytical tool.

Perea and Puerto (2013) study an attacker-defender dynamic game which means the terrorist can attack several times to maximize the expected damage. The authors formulate the worst-case scenario of the problem mathematically as a mixed integer linear model to design the railway network. They also allocate security resources to minimize the effects of the attack by maintaining the efficiency of the network.

Zhang and Ramirez-Marquez (2013) and Zhang et al. (2015) focus on strategies including protection, secrecy and truthful disclosure rather than a specific application. Zhang and Ramirez-

Marquez (2013) model the problem as a two-stage sequential game with incomplete information. The defender moves first and protects a subset of links followed by the attacker who destroys a subset of links. The two subsets are not necessarily the same. It is assumed that the attacker has complete information about the defender's activities, but the defender is not aware of the attacker's resources. The attacker can adaptively react to the defender's protection strategy and change his strategy. Solutions to the game can help the defender understand trade-offs between costs and total flows. The defender can study possible attack scenarios and choose an appropriate strategy. Zhang et al. (2015) study secrecy in a simultaneous game and prove that secrecy is a better alternative than truthful disclosure for the defender.

3.2.3. Information-Based Resource Allocation

Information-based resource allocation research has focused on the following issues: information asymmetry, completeness of information, private information of the terrorist, secrecy and deception. There is a conceptual overlap between the current section and Section 2 on Intelligence and Information Sharing. These overlaps between sections are related to perspectives that are essential properties of each section and its subsections. The relevant papers are discussed in Section 2. They include the following: He and Zhuang (2012), Lapan and Sandler (1993), Li and Cruz Jr. (2009), Nikoofal and Gümüs (2015), Nikoofal and Zhuang (2015), Xu and Zhuang (2016), Zhuang et al. (2010), and Zhuang and Bier (2007).

3.2.4. Strategy-Based Resource Allocation

Acre and Sandler (2005) examine the problem where the defenders can choose either deterrence (defensive) or pre-emption (proactive) activities or both. Proactive strategies can benefit all potential targets but may incur high costs and be undersupplied if there are free-ride nations. Free-ride nations emerge when terrorist groups target some countries more than others. On the other hand, the defensive strategy can be oversupplied and useless if the terrorists launch the attacks disproportionately. The authors show that in the case of asymmetric targeting, proactive strategies are preferred to defensive ones. Moreover, when asymmetries are sufficiently great, a country may utilize both proactive and

defensive strategies.

Bandyopadhyay and Sandler (2011) also study pre-emption vs. defensive activities, but unlike Arce and Sandler (2005), they investigate interaction between policies via including cost parameters in each policy. Bandyopadhyay and Sandler (2011) consider two commonly targeted nations, which can allocate their resources to pre-emptive and defensive strategies. Unlike defensive strategies, pre-emption comes at a high cost and its foreign involvements are high. On the other hand, a defensive strategy will not completely remove the need for pre-emption particularly when the attacker is determined to attack. Obviously, pre-emption is proactive and attractive because it damages the attacker's resources to stop or reduce future attacks. This strategy can be followed by countries like the U.S.A. and the UK. The authors indicate that pre-emption strategies often have high costs as a result of free riders who do not share the costs of pre-emption.

Compared to the previous studies, Roy and Paul (2013) only study deterrence and exclude pre-emption; but they divide it into different measures. Roy and Paul (2013) study the following strategic interactions of two nations: interdependence between the two countries on the choice of the deterrence measures; interaction between the three deterrence measures (defense, research and development (R&D) and pre-emption); and interaction between the terrorist and the defender. The authors suggest future research on a multi-disaster scenario such as a terrorist attack immediately after a natural disaster. This chain of events raises many new questions for disaster management researchers.

Unlike Shan and Zhuang (2013) who investigate a defensive strategy, Shan and Zhuang (2014) study a proactive strategy with a focus on the destruction of terrorist's SCs. They study two subgames. The first subgame has two governments. One is a potential Weapons of Mass Destruction (WMD) victim who prepares for the attack while paying a subsidy to the other government to intervene and prevent terrorist activities. The other subgame has two terrorist groups. One group manages the black-market operations for profits (upstream operations of terrorist SC) and the other group manages the attack (downstream operations of terrorist SC).

3.2.5. Impact of Terrorist's Behavior in the Defender's Resource Allocation

A potential terrorist could be either strategic or non-strategic. The main difference is that

strategic terrorists adapt to the observed defense strategy. Therefore, strategic and non-strategic terrorists respond differently to the defender's resource allocation decisions. Shan and Zhuang (2013) have proposed a hybrid model that integrates game-theoretic and non-game-theoretic approaches to the resource allocation problem by a country (government, defender) to defend her from an attacker. The authors compare the expected losses under the following scenarios: (a) there is a known probability that the terrorist is strategic; (b) the terrorist could be non-strategic, but the government erroneously assumes him to be fully strategic; and (c) the government erroneously assumes a non-strategic terrorist whereas he could be strategic. In the game-theoretic model proposed by the authors, the response of a strategic terrorist is determined based on the defender's allocation decisions. Whereas, in the non-game-theoretic model, used for non-strategic terrorists, the terrorist's decision does not depend on resource allocation decisions by the defender and is exogenously determined. The authors show the superiority of game-theoretic models over non-game-theoretic models in minimizing expected losses for various scenarios.

3.3. Summary and Future Research

In this section, we review and discuss the papers related to Planning Core Capability. Target valuation and selection, and resource allocation are the two major themes of these papers. SC concepts can be used to make decisions in these two areas.

"National Preparedness Goals" defined by Homeland Security, DHS (2015), highlights two directions for purposes of planning: (1) planning measures including strategic, tactical and operational that must be integrated and (2) improved coordination between local, state, tribal, territorial, federal, and private sector entities. The existing body of the literature is mainly focused on resource allocation and hardly studies these two aspects of planning. Therefore, studies on integrating and coordinating decision-making processes across various entities in different geographical areas (nationwide or global). Also time frames (long term, midterm and short term) are possible directions for future research.

Terrorism prevention problems have been studied as a system of interconnected links (of assets) in series or in parallel. Which system is preferred by the defender and by the attacker can be further

explored in future research. More research is needed to study domino effects. For example, a single attack can result in a cascade of damaging effects on the system over time, such as the spread of disease. Static resource allocation problems can be extended to study dynamic re-allocation problems. The consequences of terror attacks (e.g., human losses or infrastructure damage) are generally modeled as linear functions of the number of successful terror attacks. Adding a non-linear term may capture economic side effects caused by people's reaction to more frequent terror threats. Exploring the impact of attacker's or defender's risk preferences (e.g., risk neutral, risk averse or risk seeking) is a potentially valuable research area. Different terrorist groups may have different risk attitudes which provides another example of the role of behavioral OM in the prevention area. The bounded rationality of a non-strategic attacker in modeling is a relatively unexplored research area.

4. Interdiction and Disruption

Interdiction and disruption include any proactive or reactive action taken by a defender to intercept, stop, postpone or avert a terrorist attack. The objectives of the defender, as well as those of the attacker; and the type of attacks are important in developing and understanding interdictions and disruption strategies. Knowledge about the type of threat is necessary to meet the challenge. Type of threat includes bomb blasts, kidnapping and hostage taking, assassinations, suicide bombing, and using weapons of mass destruction (WMD). The majority of papers that we found in the literature on terror prevention consider general forms of terrorist attacks rather than a specific attack mode. Interdiction and disruption strategies to deal with general attacks can be grouped into the following three categories: Operational Intervention, Deception and Information, and Financial. However, some research papers study specific attacks like WMD, suicide bombing, and kidnapping or hostage taking. Figure 5 illustrates research streams in the core capability of "Interdiction and Disruption".

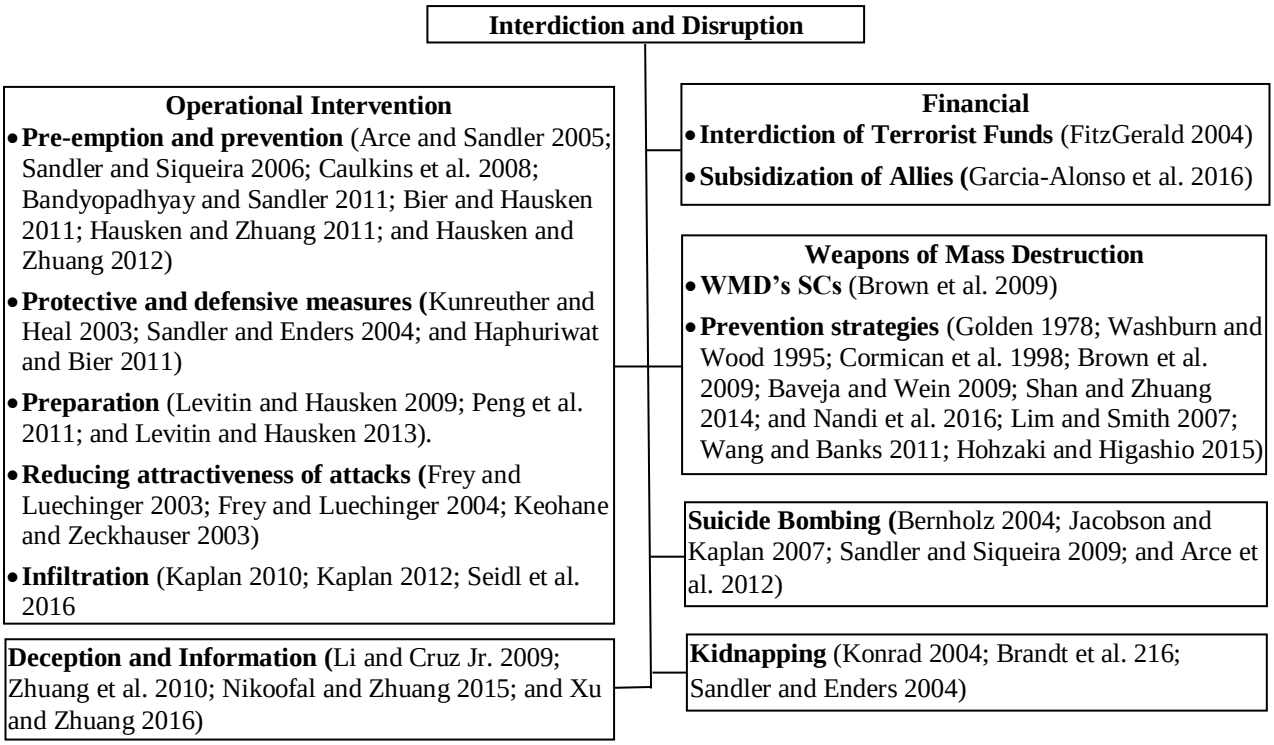

Figure 5: Categorization of published papers on terrorism prevention that are based on Interdiction and Disruption Research.

4.1. Operational Intervention

We discuss Pre-emption and Prevention, Protective and Defensive Measures, Preparation, Reducing Attractiveness of Attacks, and Infiltration in the sub-sections below.

4.1.1. Pre-emption and prevention

Pre-emption and prevention involve capturing (even killing) terrorist leaders, sponsors and other operatives, freezing assets, destroying terrorists' breeding grounds, safe havens, training camps, and infrastructures. Arce and Sandler (2005) employ game theory to investigate both deterrence and pre-emption strategies for at-risk nations' optimal counterterrorism efforts. They study trade-offs between the public costs of defensive measures and the public benefits of proactive policies. Their main research finding is that when the degree of asymmetry in the number of attacks over the set of nations under attack is high, such nations will engage in both proactive and defensive actions.

The work of Arce and Sandler (2005) consider a single decision maker (that can be a set of nations); therefore, they do not include any interaction between at-risk countries. This work is extended by Sandler and Siqueira (2006) who assume that any nation is a decision maker and at-risk

countries interact. Sandler and Siqueira (2006) focus on the difference between pre-emptive and defensive policies to counter terrorism across more than one nation. The authors discuss how all nations at risk can benefit from other nation's pre-emptive actions against terrorism owing to the presence of externalities due to the public acceptance of these actions. On the contrary, defensive actions may transfer threats to less secure targets (abroad) and create additional external costs. The authors propose a game theory framework under leader-follower behavior to investigate how such positioning could impose externalities across countries. When a simultaneous game is played between the government and a terrorist, decision making for counter terrorism leads to underspending and overspending on proactive and defensive measures respectively.

Interactions between pre-emptive and defensive strategies have been studied by Bandyopadhyay and Sandler (2011) and Hausken and Zhuang (2011). For example, less pre-emption may result in increased defense expenditure. Similar to Sandler and Siqueira (2006), Bandyopadhyay and Sandler (2011) study the interplay between pre-emptive (i.e., destroying the attacker's resources) and defensive (i.e., hardening of targets) strategies to benefit only two targeted nations. Pre-emption is a high-cost strategy that strong nations like the U.S.A. and the U.K. may take proactively. The situation in the case is that the other nations may not contribute and all costs will be incurred by the proactive countries. This research also relates to resource allocation that has been discussed in section 3 on Planning.

While there are many commonalities between Hausken and Zhuang (2011) and Bandyopadhyay and Sandler (2011), there are some differences also. Bandyopadhyay and Sandler (2011) assume that the terrorists are non-strategic, two nations are involved, and the government does not defend. But Hausken and Zhuang (2011) consider one unitary government that is fully strategic and can also defend. Hausken and Zhuang (2011) study a two-stage game between a government and an attacker where both players can simultaneously choose between pre-emptive and defensive strategies. The authors consider that the terrorist can choose to allocate resources to defend its own resources. They argue that governments should choose proactive attacks when the terrorists' resources are low. It is desirable to both attack and defend when encountering a resourceful terrorist. In a follow-up paper, Hausken and Zhuang (2012) analyze a two-stage game, repeated T times, between a defender and an

attacker. In the game, the assets (infrastructure) of the defender, which she has built over time, are attacked repeatedly by the attacker. The defender wants to protect her asset(s). The elapsed time between each two-stage game is much longer than the time between the two stages; each player is assumed to solve only one two-stage game at a time. The defender is assumed to make the first move in stage 1 followed by the attacker in stage 2. Both attacker and defender have common knowledge about the game structure and all parameters. The terrorist is knowledgeable about defense information and uses it to plan an attack strategy. The authors determine the optimal timing for deterrence of terrorist attacks related to exogenous dynamics.

Caulkins et al. (2008) study two new types of counter terrorism strategies: (1) "fire" (2) "water". The fire strategy includes aerial bombing of residential neighborhoods to weed out terrorists and also capturing them through road blocks and check points. Bombings could cause deaths and injuries to civilians. Such strategies cause disasters as well as inconvenience to the general public and may raise sympathy towards terrorists. This also angers potential recruits and will facilitate more recruitment. The "water" strategy includes intelligence-driven arrests or "surgical" operations. These are costly and choices are limited. The authors have analyzed several scenarios based on these strategies and have proposed that the water strategy is usually recommended. The fire strategy is prescribed only if the number of terrorists in the area is higher than a specified limit.

Unlike the previous studies, Bier and Hausken (2011) consider financial and non-financial incentives against terrorists. They study the impacts of positive and negative incentives to influence the attacker's behavior. Financial incentives (e.g., tax removal), provisions of goods/services and possible economic development are examples of positive strategies. Imposing trade restrictions, disrupting money transfers, freezing assets and military retaliation are examples of negative strategies. The authors argue that negative incentives can be both useful and harmful; the same applies to positive incentives. The negative incentives may alter the terrorist's motivation and generate even higher levels of hatred and eventually can result in multiplying their attack efforts. Similarly, positive incentives may also encourage terrorists to continue attacks. The authors model the problem as a single-stage game between an attacker and a defender. They derive conditions under which positive incentives are recommended conditionally to encourage the attacker to accept it provided that the

terrorist does not to launch an attack. Cost-based utilities are defined for both players depending on positive or negative incentives imposed. It is also shown that the defender should offer the smallest possible amount of positive incentives. When the attacker is advantaged (e.g., with a low attack cost), positive incentives are not recommended.

4.1.2. Protective and defensive measures

These measures include installing sensors at strategic locations, fortifying buildings and structures (e.g., embassies prone to attack) and safeguarding power plants with protective equipment. Kunreuther and Heal (2003) study an airline security system in which several airlines can independently decide whether or not to invest in protection and security systems. They study how externalities could influence defensive policy-making among multiple interdependent defenders facing terrorism risk. The authors consider international airline security systems and investigate how the security level for an airline is affected by other airline's security technology adoption decisions. Their research shows that cost and risk parameters and incentives suggest two Nash equilibriums (i.e., either everyone invests or no one does). However, in reality, some invest and some do not. Perhaps, intervention by local authorities to change the amount of incentives can persuade all airlines to make the same decision.

Similar to Kunreuther and Heal (2003), Haphuriwat and Bier (2011) study a single period game where a defender chooses to allocate defensive resources on target hardening (protect them individually) and on overarching protection (protect them collectively). The main difference between these two papers is that in Haphuriwat and Bier (2011) there is no decision made by an individual for target hardening. Haphuriwat and Bier (2011) implement the research on data related to the state of Wisconsin and show that overarching protection is preferred to hardening.

Sandler and Enders (2004) study the substitution effect in counter terrorism policies, especially in hijackings and hostage events. According to the authors, proactive operations such as technological barriers could be useful to deter the risk of a specific type of attack in the short term, but terrorists eventually will find a way to substitute this type of attack with another life-threatening one.

4.1.3. Preparation

Preparation is another defensive measure to counter attacks and may include: adding redundancy

to a system, increased protection of the system's elements, and diverting attacks by creating false targets.

Levitin and Hausken (2009) propose the following three defense strategies to maintain a system composed of identical elements and fulfilling a demand, against an external attack: system redundancy, deploying false elements, and protecting the system elements. The authors analyze system reliability and the optimal resource allocation problem among three different attack strategies to minimize the expected damage and the system's vulnerability. The authors model the problem as a two-period, nonzero, non-cooperative game and develop an algorithm to find the optimal strategy. They show that when chance plays a greater role than the efforts made by the players, protection investments result in an intermediate vulnerability regardless of the amount of resource allocated to this strategy. Therefore, redundancy is more effective than protection. Deploying false elements also decreases risk if the number of elements is large.

The following two papers are different from Levitin and Hausken (2009) because they consider false targets or decoys. Peng et al. (2011) study the problem of how to deploy decoy(s) for protecting a single target. Decoys are characterized by their costs and detection probabilities. The defender must choose the number of decoys and types of decoys to locate to minimize the chance of the real target being destroyed. The authors use reliability theory to solve two versions of the problem: single and multiple decoys. The results show that when the defender and attacker do not have significant superiority over each other in terms of available resources, flexibility in choosing the type of decoys is more beneficial to the defender particularly when the intensity of the attack is uncertain. When the attacker has more resources, he will attack more targets with less intensity. Moreover, with an increase in decoy detection probability and also with an increase in the unit cost of decoys, the optimal number of decoys decreases.

Levitin and Hausken (2013) investigate resource allocation policies among genuine targets and false targets (decoys) similar to Peng et al. (2011) but in series and parallel systems. A series system is considered destroyed when at least one of its genuine elements fails whereas a parallel system is presumed destroyed when all of its genuine elements fail. The attacker is unable to distinguish between genuine and false targets, and randomly attacks a subset of the targets. The authors study a

two-period game. In the first period, the defenders allocate resources between false and genuine targets. In the second period, a single attack occurs. The defender wants to minimize her system vulnerability by minimizing the maximum system damage (worst-case scenario).

4.1.4. Reducing attractiveness of attacks

The defender can potentially prevent an attack by making it less attractive. Defender's strategy can increase the cost of an attack (Frey and Luechinger 2003), the potential target could be made less attractive (Frey and Luechinger 2004), and by decreasing the capacity of the attacker (Keohane and Zeckhauser 2003). This strategy converts a large target into several smaller dispersed targets making a single attack to cause less damage. In other words, if the attacker would like to cause the same level of damage in a decentralization set up as in the centralized version, he needs to spend more on resources.

Frey and Luechinger (2003) discuss alternative strategies for deterrence, such as raising the attack opportunity cost to influence the price of terrorism. The authors distinguish between benefits from "benevolence" and "deterrence" strategies to reduce terrorism. Deterrence strategies increase the opportunity cost of terrorism whereas benevolence strategies aim at reducing the cost of all other activities and decreasing incentives to attack. The research suggests that depending on the type of terrorist organizations, a mixture of different strategies should be adopted.

Keohane and Zeckhauser (2003) argue that asset destruction is not an effective deterrent strategy. Instead, they propose influencing the stock of terror capacity and propose controlling the capacity of terrorist organizations by reducing the flow of resources to them or by directly destroying the existing stock of terror capacity. They introduce two types of measures for governments: averting actions and amelioration to counter terrorism. The former aims at decreasing the probability of a successful terrorist attack while the latter reduces damages from an attack. These two strategies focus on disrupting terrorist plans without influencing terrorist's underlying capacity.

According to Frey and Luechinger (2004), the terrorist's intentions need to be known. Terrorists seek (i) attention of the media, (ii) to destabilize the polity, and/ or (iii) to damage the economy. The authors calculate marginal costs and marginal benefits of terrorist acts. Governments are interested in deterrence strategies because, in this way, they show people their determination to fight terrorism. Such deterrence strategies increase marginal costs. On the other hand, utilizing a decentralization

strategy is not directly attributed to the government while its marginal cost is lower than deterrence because of its easier maintenance. The authors suggest decentralization because it disincentivizes attackers.

4.1.5. Infiltration

Kaplan (2010) studies infiltration by undercover intelligence agents to interdict terrorist schemes using queueing theory and Markov processes. This model is static and provides cost-benefit analysis and estimates the number of undetected terror plots as well as the rate at which new threats could be detected and interdicted. Kaplan (2010) looks at terror plots as customers entering a queue and intelligence agents as servers to investigate trade-offs between terror damages and prevention costs and decide the optimal assignment of agents. The idea is illustrated with some suicide bombing data.

In a follow up paper, Kaplan (2012) proposes the use of network theory and project networks to fight terrorism. In terrorist networks, nodes and links represent individual operatives and transactions, respectively. In addition, the author surveys network models for the development of adversarial projects such as a nuclear weapons development project. Next, he considers contributions of operations research to the models which are intended to search and find embedded terror networks. Kaplan (2012) also proposes queuing models as a beneficial method to provide guidance for detecting and interdicting terror plots. He creates the concept of "terror queues." These newly hatched terror plots correspond to arriving customers - where the queue of customers represents the number of undetected terror plots. The terror queue framework enables estimation of the number of undetected terror threats.

Seidl et al. (2016) extend Kaplan (2010) and apply optimal control theory to terror queues and formulate a dynamic model to evaluate the government's prevention costs for staffing policies. They assume a constant arrival rate for the new terror plots and define the number of known and unknown terror plots as two state variables that change dynamically over time. The authors control the number of covert intelligent agents to be hired to detect and infiltrate terror plots. They consider various scenarios with different initial states and show that the optimal strategy for the government utilizes both detected and undetected terror plots. Allowing for new terror threats, the government's strategy evolves over time. The authors assume that the interdiction rate is fixed because it is not controllable

by the government; it is related to technology. Based on this assumption, they assess the impact of the interdiction rate on the optimal policy and find that if the agents are not efficient, it is optimal for the government to reduce the number of agents.

4.2. Deception and Information

In games involving deception and secrecy, the majority of studies are based on a two-player game between a defender and an attacker. Information secrecy and deception are mostly about the preference and valuation of potential targets; and the amount of resources the defender allocates to the targets. Depending on the amount of this information and its accuracy, the attacker (and also, the defender) develop and alter their strategies. The findings of the four papers discussed in Section 2, Intelligence and Information Sharing, can be used for effective interdiction. These papers include Li and Cruz Jr. (2009), Zhuang et al. (2010), Nikoofal and Zhuang (2015) and Xu and Zhuang (2016).

4.3. Financial

Counter-terrorism strategies also include systematic efforts to track financing of terrorists' activities. Tracking the flow of finances to support terrorism unfolds the terrorists' networks, helps to identify them and to disrupt their operations. Capturing or even killing people that facilitate money transfers decreases the money available to terrorist organizations and makes the flow of money difficult. The Commission report (2011) page (382) states that *"Vigorous efforts to track terrorist financing must remain front and center in U.S. counter terrorism efforts …. Captures have additionally provided a windfall of intelligence that can be used to continue the cycle of disruption."*

Financial strategies include interdiction of terrorist funds, and subsidization of allies. Papers within each category are discussed below.

4.3.1. Interdiction of Terrorist Funds

According to FitzGerald (2004), international cooperation helps to focus on interdicting the financial flow of terrorist funds. The involved countries cooperate in terms of tracking transactions and exchanging information to deny terrorists access to international financial systems. In fact, denial

of access to the financial systems is based on disclosure in level of identity, transaction purpose, informal money transfer, etc. The author suggests that instead of a disincentive-based strategy (that is normally being followed) the countries can take a positive incentive-based strategy for disclosure of the abovementioned information. Positive incentives can be based on reducing transfer taxes for immigrants.

4.3.2. Subsidization of Allies

Garcia-Alonso et al. (2016) consider two countries (home and foreign). The terrorist is likely to attack both countries to cause damage. Both countries can take a defensive strategy to minimize damage. The foreign country is damaged by the terrorist attack in its own territory but the home country cares about both countries in accord with its national strategy. Consequently, the foreign country tries to limit resources available to the terrorist while the home country tries to encourage the foreign country to attack terrorist assets through subsidization. Subsidizing and direct intervention are two strategies that can be taken by the foreign country. The authors formulate a multi-stage game in which the home country, the foreign country, and the terrorist make their decisions respectively. Their research shows that only when the efforts made by both countries on defensive strategy are not sufficient to limit the terrorist's resources, direct intervention is recommended. Moreover, only if the home country has an effective and efficient military power, should it proactively choose intervention.

4.4. Weapons of Mass Destruction

According to 18 U.S. Code § 2332a, Weapon of Mass Destruction (WMD) means (i) any destructive device such as bomb, grenade, rocket, missile and mine, (ii) any weapon that may cause death or serious injury, (iii) any weapon involving a biological agent, toxin, or vector, and (iv) any weapon that is designed to release radiation or radioactivity at a dangerous level. (https://www.law.cornell.edu/uscode/text/18/2332a).

Deployment of WMDs for terrorism generally involves several terrorist groups. Similarly, multiple governments are involved in counter-terrorism efforts. Similar to any business SC, from the terrorist group's perspective, WMDs have their own SCs (Shan and Zhuang 2014) and their

procedural phases include (1) purchasing or acquisition of raw materials, (2) production and distribution and (3) attacking targets.

WMD's SCs : One of the differences between many business SCs and WMD's SCs is that the terrorists' SC is designed similar to a project network rather than a routine product to be produced repetitively. The terrorist or proliferator plans to minimize the completion time of the SC project (Brown et al. 2009). The interdictor attempts to stop the development of terrorist's SC. The interdictor can use either a reactive or a proactive strategy to delay or stop the final attack on targets (Brown et al. 2009). This raises the issue of how extensive is the damage. If the cost or loss caused by a possible attack is high, then it must be stopped by an effective defense shield or a pre-emptive strike which are both proactive strategies. Brown et al. (2009) analyze a case study of uranium-enrichment technologies and suggest some diplomatic, economic or military solutions to policy makers to achieve interdiction for various levels of proliferation.

Prevention strategies: Prevention strategies (proactive) have been studied by Golden (1978), Washburn and Wood (1995), Cormican et al. (1998), Brown et al. (2009), Baveja and Wein (2009), Shan and Zhuang (2014), and Nandi et al. (2016).

Golden (1978) and Washburn and Wood (1995) focus on network interdiction problems. Golden (1978) formulates this problem as maximizing the length of an adversary's shortest path in a supply network. Washburn and Wood (1995) focus on network interdictions of drugs' SCs but the research achievements can also apply to WMD's SC. Washburn and Wood (1995) assume that a single evader (intruder) has already entered the defender's network (e.g., transportation network of roads in the target nation) and attempts to travel from an origin to a destination. On the other hand, the government (i.e., the interdictor) attempts to detect the evader by inspecting the network links through which the evader may select to pass. Given that budget limits will not allow the interdictor to inspect all network links, the researchers suggest a path-selection strategy to maximize the detection chance. Cormican et al. (1998) study the stochastic version of this network interdiction problem using two-stage, stochastic integer programming to minimize the expected maximum flow through the network. They test their developed methods on a large network.

Nandi et al. (2016) also study a network interdiction problem. In this case, one or more links are

removed from a network to make it disconnected. Such a problem has an application in the prevention of infection spread (in epidemiology). In epidemiology, they consider a part of the network that has already been infected and the idea is to remove some links to disconnect the infected and susceptible nodes. The authors define four types of problems which are different in term of their objective functions as follows: (1) the number of connections between infected and susceptible nodes; (2) the number of susceptible nodes having one or more connections with infected nodes; (3) the total number of paths between infected and susceptible nodes; (4) the total weight of the paths between infected and susceptible nodes. The problem is formulated as a mixed integer linear programming problem. They design and propose heuristic algorithms with findings as follows: (1) To reduce the average number of new infections, isolation of susceptible nodes from infected nodes is usually the most effective way; (2) To increase the average time to infect half of the susceptible nodes, remove the highest probability transmission paths. This is usually the most effective way.

In addition to the above-mentioned literature, some scholars apply game theoretic techniques to these problems. Lim and Smith (2007) investigate an interdiction problem on a network with a leader and a follower. The follower intends to transport multiple commodities in a network from multiple origins to multiple destinations while the leader plans to damage some arcs of the network to minimize the maximum profit made by the follower in the shipping process. Each arc has a finite capacity and there is a cost for damaging an arc. The authors study (1) discrete interdiction in which each arc is either completely disabled, or is safe; (2) continuous interdiction in which partial damage is allowed, which means an attack may not completely disable an arc but can reduce its capacity. The authors show that the continuous interdiction problem is more difficult to solve particularly for large-size problems.

While Lim and Smith (2007) apply a leader-follower game to an interdiction problem, Wang and Banks (2011) study a simultaneous single-period game played between a convoy commander (defender) and ambushing insurgents (attacker). The defender selects a route across a road network while insurgents can ambush on vertices to attack the convoy with improvised explosive devices (IEDs). A vertex in a road shows a candidate location chosen by an attacker to place IEDs. An undirected edge links two adjacent vertices in which traffic can move in both directions. The IEDs

cause random levels of damage to the convoy. The attacker locates a fixed number of IEDs to cause damage. It is assumed that the use of IEDs cannot necessarily block all routes. The attacker intends to maximize their expected utility which is based on random payoffs of damages cumulatively on vertices. Similarly, after the defender chooses the route, the damages along the way are cumulatively collected by passing through vertices depending on damages caused by the attacker. The defender chooses a route to minimize the expected cumulative damage.

In addition to the previous studies, Hohzaki and Higashio (2016) introduce attrition games to such problems. They investigate an attacker-defender, zero-sum game in a network. The attacker's members intend to march from an origin node and reach a destination node in the network. The defender intercepts the attacker and the attacker may lose some of his members during the attack. The attacker wants to find the best path through the network with maximum survival while the defender wants to deploy her forces on the arcs of the network and to increase causalities as much as possible. This problem is called an attrition game with applications in network security, anti-terror operations and logistics networks.

Another issue under consideration is that in the downstream part of WMD's SC, terrorists may enter the target country. Baveja and Wein (2009) focus on the use of biometric systems at the border of the U.S. to quickly and precisely maximize the detection probability of terrorists. This paper is discussed in Section 7 (ahead) on Screening, Search and Detection. Shan and Zhuang (2014), discussed in Section 3.2.4 (Strategy-Based Resource Allocation), focus on the destruction of terrorist SCs.

In 2006, the FBI created the WMD Directorate (WMDD) "to build a cohesive and coordinated approach to incidents involving nuclear, radiological, biological, or chemical weapons–with an overriding focus on prevention." (https://www.fbi.gov/investigate/wmd). WMDD focuses on (i) Preparedness, (ii) Countermeasures, (iii) Investigations & Operations, and (iv) Intelligence against WMD. As mentioned by Brown et al. (2009), proactive or reactive strategies (or both) can be taken against the SC of WMD. This is also applicable to these four areas which are less explored in the POM field. WMD preparedness ensures that the FBI and the U.S. Government are always ready to react against attacks or threats. Training, enhancing understanding of WMD threats, and simulating

scenario-based exercises are examples of WMD preparedness activities. According to the FBI, the WMD countermeasures are "actions taken to counter, eliminate, or offset the WMD threat." Particularly, proactive strategies called "tripwires" are at the heart of these activities which are proactive early warning systems. Investigations & operations attempt to explore potential or actual transfer of knowledge, materials and technology to form the SC of WMD. For example, collecting evidence from radioactively-contaminated areas falls within this category. Intelligence collection is a proactive strategy to provide information for stakeholders (e.g., U.S. and foreign partners). Such information is utilized in the countermeasures, investigations, and operations to make appropriate decisions.

In summary, it seems that the nature of WMD persuades researchers to use game-theoretic approaches and also graph and network theory concepts. If we focus on WMD's SC before attack, we will see that the evader attempts to create a resilient SC against the interdictor. On the other hand, the interdictor attempts to disrupt this SC. Consequently, the value of perfect information, the existence of complete/incomplete information, and symmetric/ asymmetric information, all play an important role in this game.

4.5. Suicide Bombing

Suicide bombers are those people who are willing to give up their own lives to take other people's lives. They are not responsive to deterrent actions taken by the target government. Suicide bombers constitute a resource for the attacker that must be replenished by training new people.

Bernholz (2004) studies supreme-value terrorists who are true believers willing to take other people's lives by giving up their own lives. The author utilizes utility functions of a representative believer to parametrically model this type of terrorist act linking the number of attacks to terrorist resources. Three types of defensive measures are considered: (1) reduce the level of physical and psychological vulnerability; (2) reducing availability of tools and sources for terrorists and (3) converting the ideology of the believers. Possible strategies recommended by the authors are decentralization (technological, economic and political), military pre-emption, prevention by intelligence and police actions, and education (of children about values of tolerance and self-

improvement). The research concludes that the main threats to Western societies can come from immigrants or social media. Therefore, the defender tries to minimize the impact of this way of thinking and living on society. Strategies such as decentralization and isolation of terrorists (e.g., selective immigration) in a free society can be helpful.

A comprehensive survey of research that focuses on developing strategies by a government for counter-terrorism measures using game theory has been presented by Sandler and Siqueira (2009). The authors mention that in recent studies suicide terrorists are considered rational players who sacrifice their lives for organizational goals. Later, the survey analyses various agent combinations in suicide terrorism. It also reports on findings of the recent literature of game theory applied to suicide terrorism. One of the results of this survey is that the dissolution and schism of terrorist groups over time is an important issue that needs more investigation by developing a game-theoretic model to better understand the important factors at work to hasten their demise. According to Sandler and Siqueira (2009), terrorist success and failure could affect terrorist resource accumulation.

One of the key papers in the area introduced by Sandler and Siqueira (2009) is Jacobson and Kaplan (2007). They focus on the attacker's suicide bombings and the defender's target killings strategy to formulate a sequential game to learn how often a terrorist will attack and how often the government should kill suspected killers. They find that if the suicide bomber is patient in undertaking the future attacks the levels of violence will converge to stationary equilibrium. On the other hand, when the government is patient and delays the killing of suspected killers over time it may face chaotic fluctuations in attacks rates.

In contrast to Jacobson and Kaplan (2007) which focuses on examining the "targeted killing", as a proactive/pre-emptive measure, Arce et al. (2012) assume a one-shot, simultaneous game between a terrorist and a defender based on complete information. The attacker considers two types of attacks: (i) more damage at a low cost (e.g., suicide attack) and (ii) a non-suicide traditional mode (e.g., WMD). The attacker's objective is to have at least one successful attack. The defender uses a constant level of hardening and is defined as successful if she defends and protects all targets from such attacks. The research assumes that the players have asymmetric payoff functions. When the players exert the same level of force to a target, the defender will win. The problem is solved by using a

mixed strategy Nash equilibrium. The results indicate that if the terrorist organization utilizes either or both attack modes, he faces a non-trivial trade-off. The authors show that (i) the attacker may choose not to attack; (ii) the suicide attack is more cost-efficient than the traditional mode, and that the probability of launching the suicide attack is not certain (i.e., 100%).

4.6. Kidnapping

Konrad (2004) points out that terrorism is an ancient phenomenon. The author posits a structural "equivalence" between extortion and terrorism that extends over thousands of years. There is ample history (which the author calls upon) to show that enduring terrorist groups use violence, kidnapping, and blackmail to pursue political, religious and monetary goals. The "equivalence" permits deductions from the "theory of extortion" that can be applied to the study of the terrorism process which might lead to a "theory of terrorism". The author looks at the interactions between the extortionist and the government from an information perspective. As both sides repeatedly interact, they gain information from each other. This process may or may not converge to an equilibrium state. Using the concept of game-play (well-represented by a decision tree) the author examines the effect of repeated extortions wherein a committed government can deteriorate the attacker's capabilities over time. This analysis shows that organizational design matters regarding immunity to threats of extortion which provides important opportunities for future research.

Brandt et al. (2016) also investigate kidnapping as a terrorist attack method. The Bayesian Poisson change point model of Park (2010) is employed. This model fits a Poisson regression that identifies the number of change points in the time series and estimates different regression parameters via the filtering method. This model and historical data are used to analyze whether the defender should make concessions to kidnappers. The authors do not recommend concession as a strategy because their analysis of real-life data over the U.S.A. and U.K. cases shows that success by terrorist kidnappers in negotiations will encourage more kidnapping. Sandler and Enders (2004) also talk about hostage taking which amounts to kidnapping. The skyjackings (by mentally disturbed and psychologically distressed individuals) in Turkey and Cuba (during March 2003) demonstrate that not all skyjackings include terrorists bent on mass destruction. Nevertheless, suicide skyjackings and the

reactions of desperate passengers to fight back must be analyzed in the future along with a government's decision to destroy a hijacked plane.

4.7. Summary and Future Research

In this section, we discuss papers under operational intervention, deception and information, financial, WMD, suicide bombing, and kidnapping or hostage taking.

Disruption of a terrorist's financial SC is an important topic for future research. This is further discussed in Section 9. In addition, information and people-based strategies such as media control and education (of potential victims) need to be studied. When it comes to modeling and measuring the performance of interdiction strategies, a vast majority of the research is cost-based and/or probability-based. It is noteworthy that while there are many uncertainties involved in outcomes of interdiction strategies, the lack of sufficient historical data does not facilitate calculating probability density functions. In the future, using utility-based and time-based measures are suggested because not all interdiction strategies can be evaluated in terms of cost and probability. When disrupting a terrorist network, we should note that their SC networks are usually global. Therefore, alliance between several nations is needed to develop a collaborative network disruption strategy (financial, physical and information networks). Finally, future research can be more useful if interdiction strategies are developed for specific attack modes. For example, interdiction strategies taken against WMD may not be effective for suicide bombing.

5. Screening, Search and Detection

A screening system specifies the checkpoints through which passengers and baggage have to go through at an airport; and containers pass through at a seaport. Passengers can be divided into "threat" and "no-threat" groups. TSA might use "unknown risk" as a third category. Passengers in the "unknown risk" group are subjected to more screening. What are the characteristics of the travelers belonging to each group (aka profiling)? How much money should be spent in gathering intelligence? How much screening is necessary? These are important questions for airport security that POM researchers have attempted and are discussed in this section. The indicators for profiling people may

include race, religion, gender, education, economic status, political beliefs and perspectives on the value of human lives. Figure 6 illustrates research streams on this topic.

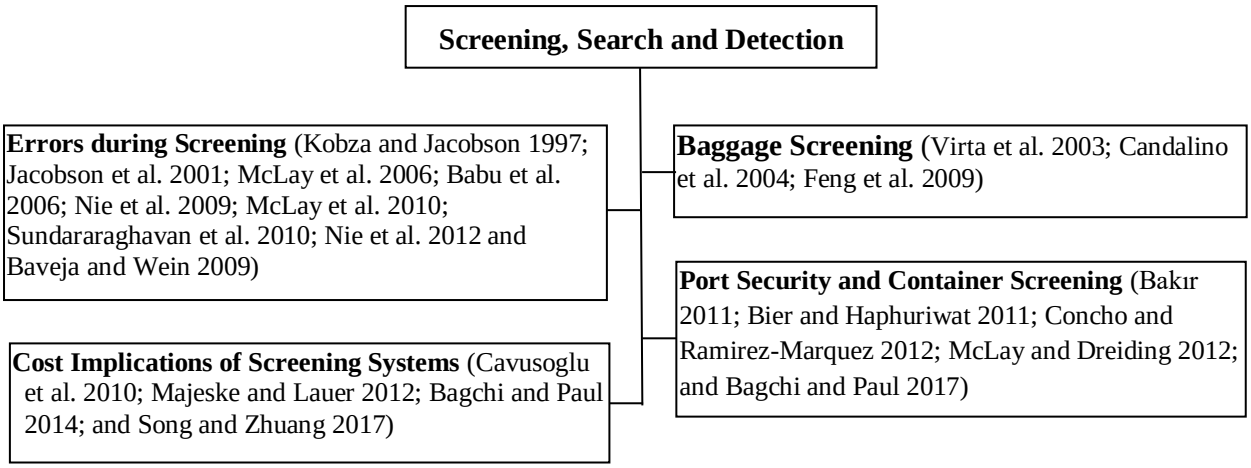

Figure 6: Categorization of published papers on terrorism prevention that are based on Screening, Search and Detection Research

5.1. Errors During Screening

A screening process results in the following four outcomes. The traditional matrix, given below in Figure 7, provides a visual of these four system results.

1. *True Alarm (correct):* A real threat is detected, and the system raises an alarm.
2. *False Clear* (*false negative results/ type II error*)*:* A real threat exists but is not detected by the system. This is an error.
3. *False Alarm (false positive results/ type I error):* There is no real threat, but the system raises an alarm. This is an error.
4. *True Clear (correct):* There is no real threat and the system identifies that fact.

		Actual Condition	
		No Problem Exists	A Real Problem Exists
Test Results	Test Indicates No Problem	***Correct***	***False Negative Results*** (Type II Error)
	Test Indicates a Real Problem Exists	***False Positive Results*** (Type I Error)	**Correct**

Figure 7: Four Outcomes That Can Result from Any Screening (Detection) Process.

A higher percentage of false-clear errors indicates that more terrorists pass through the system undetected; thus, increasing the probability of a sabotage. The false-alarm, on the other hand, is a source of inconvenience (lost time, missed flights) to passengers, particularly for those who are incorrectly singled out. Missed flights add to the passengers' cost. False-alarms also increase

screening costs due to additional screening. The Federal Aviation Administration (FAA) imposes upper limits on the probability of false-clear errors.

Controlled sampling, in which passengers may take different paths through multiple device screening system, was proposed by Kobza and Jacobson (1997). The authors developed probability models for security system based on Type I and Type II errors. The system comprises of two components: the devices and policies/procedures to utilize these devices. The authors designed cascaded (series) and parallel device systems and compared them with a single device system. It was found that the appropriate system depends on the specific threat levels. However, multiple-device systems are usually preferred to single-device systems in terms of both errors and costs. Later, Jacobson et al. (2001) introduced an upper bound on pre-specified false-clear probability; and used Greedy heuristic and Dynamic Programming knapsack heuristic to solve the problem. The authors used simulated security data for a two-device system to report the computational results. They show that the methodology provides insights into determining how much to invest in new security information devices.

In addition to series and parallel architectures introduced by Kobza and Jacobson (1997), Babu et al. (2006) and McLay et al. (2006, 2010) suggest grouping and multilevel passenger screening. Babu et al. (2006) assume that the threat probability is known and equally risky for all passengers. This assumption was relaxed by Nie et al. (2009) as discussed later. Babu et al. (2006) model the number of groups, the percentage of passengers assigned to each group and the check points assigned to each group. Their objective is to minimize the occurrence of false alarms. They show that the optimal grouping is a function of threat probability, and even when all passengers pose an equal threat, passengers-grouping is beneficial.

McLay et al. (2006, 2010) also study a multilevel passenger screening problem. In McLay et al. (2006), each passenger is described by an "assessed threat value" which captures the relevant "perceived risk" characteristics of the person. Passengers are then divided into threat-level groups with corresponding security screening methods. The objective is to maximize the true alarm rate within the given budgetary constraints. The authors found that more efficient passenger screening strategies could be obtained with two classes of security risks. Similarly, in the model proposed by

McLay et al. (2010), passengers sequentially enter a security checkpoint and a pre-screening system quantifies their stochastic risk levels. Based on their perceived risk levels, passengers are divided into selectees and non-selectees. The selectees are further screened. Their research intends to find the optimal policy to maximize expected security, subject to capacity and assignment constraints. The sequential stochastic multilevel passenger screening problem (SSMPSP) is formulated by using a Markov decision process and then the optimal policy is determined by using dynamic programming. It is shown that dynamic programming is computationally intractable for large problems. The authors provide a heuristic to obtain approximate optimal solutions to screening passengers in real-time. The model is tested on real-life data in the UK.

Nie et al. (2009) relax the assumption in Babu et al. (2006) that all passengers pose the same threat level; and have used mixed-integer linear programming to solve the problem. They also include the constraint that screening must be completed within an allotted time. The authors have compared their results with the model proposed by Babu et al. (2006) based on two performance criteria: false-alarm probability and staffing needs. The authors conclude that their model gives the same level of false-clear risk with a decreased false-alarm probability; using a fewer number of screeners.

Similar to Nie et al. (2009), Nie et al. (2012) consider different passenger risk levels but they divide passengers into selectee and non-selectee. Nie et al. (2012) propose a simulation-based queuing model to determine the assignment of passengers with different risk levels to the selected screening lanes to maximize the passenger checkpoint system's security effectiveness. Specifically, they focus on the system's probability of a true alarm. They find that more effective checkpoint screening can be made with their proposed model, since the probability of a true alarm increases while maintaining a reasonable screening time of passengers.

The above papers assume that the threat probability for passengers is known in advance; whereas Baveja and Wein (2009) and Sundararaghavan et al. (2010) suggest different approaches to identify threat levels. Baveja and Wein (2009) consider a Stackelberg game to compare alternative methods to maximize the detection probability of terrorists. The authors focus on the use of biometric systems and compare the following strategies: single-stage, two-finger multistage, face recognition, minutiae-based fingerprint analyses, texture-based fingerprint matcher and ten-finger analyses. The authors find

that to improve the US-VISIT biometric program, it is not necessary to shift from two-finger to ten-finger analyses. Instead by implementing the texture matching system, which is much less costly, the two-finger strategy may achieve better performance.

Sundararaghavan et al. (2010) suggest asking airport passengers a series of questions. Based on their responses passengers are cleared to board or denied boarding. The answer to each question is binary (yes/no), and the answers are mapped against the predefined responses that support or deny clearance. The authors investigate the best sequence of questions to minimize the number of questions asked to reach a decision. Three heuristic approaches determine the most efficient sequence of questions. The performance of the algorithms is measured in terms of correctness of the results and also the time required to solve large problems by testing on randomly generated sample problems. The results indicate that efficient question sequencing can significantly save time in the screening process for a large number of passengers.

5.2. Cost Implications of Screening Systems

Increased staffing levels are likely to increase the detection probability and decrease congestion at airports. The reverse is true if staffing is decreased. A cost-benefit analysis is needed to find the appropriate level of resources to be deployed.

Cavusoglu et al. (2010) investigate the impact of screening policies on the following four performance measures: (i) detection of attackers, (ii) inconvenience to passengers, (iii) reliability of screening system alarms, and (iv) security-related costs. The scenarios studied by the authors are a combination of (1) the deployed Computer Assisted Passenger Prescreening System (CAPPS), (2) the capability of the profiler, (3) the quality of the screening device, and (4) the number of deployed screening devices. Depending on the quality and number of devices, the four performance measures change. The authors find that if the profiler is less vulnerable to attacker gaming and the screening devices are of low-quality, then profiling is more beneficial. It should be noted that none of the profiling setups are superior under these performance measures.

Bagchi and Paul (2014), in line with, Cavusoglu et al. (2010), also study the optimal allocation of limited resources between profiling and screening. Increased intelligence leads to less screening. A

highly motivated attacker, if his payoff is high, is more likely to attempt to carry out the attack when the investment in intelligence is increased. If technological innovation reduces the cost of screening, then social welfare improves. Investment in intelligence increases if the cost of having the resources (the opportunity cost of resources) is high and vice versa. The authors also observe that expenditure on intelligence becomes more beneficial from a cost/benefit perspective with an increase in the time value of the passengers. Bagchi and Paul (2014) also review the role of TSA's PreCheck program that allows some selected passengers expedited screening in exchange for voluntarily revealing information about themselves. They show the cushioning effect of this program on budget shortfalls (i.e., it can save money). Further, these authors examine the role of enhanced punishment if the terrorist is caught during inspection. Knowledge on the part of the terrorist of enhanced punishment, if caught, will reduce the optimal effort level for intelligence gathering, whereas the reverse is true for a low level of punishment. The authors suggest extending this research to cargo and port security.

Majeske and Lauer (2012) use Bayesian modeling to form three passenger groups, like the three groups in TSA's "Secure Flight", that is, high risk (no fly), low risk (fly), and unknown risk. The passengers in the "unknown risk" group need more screening. Based on the outcome of the additional screening, these passengers may be denied boarding. These three categories are akin to three states of nature. The probability of occurrence of each state is dependent on the personal characteristics of an individual. The authors develop a decision tree that uses probabilities for various events (e.g., the probability that a passenger belongs to the no-fly category) and the corresponding payoffs. The payoffs include the following cost categories in the model: the expected cost if an undesirable (no-fly) passenger is allowed to fly, the cost of inconvenience to the low-risk passengers if they are subjected to additional screening and the enhanced cost of screening of passengers with unknown risk. The authors discuss components of these costs in detail. They point out that the government and passengers may have different perspectives on the magnitude of these costs. For example, an individual passenger will put a higher value on his/her own life as compared to the valuation by the government. It is, therefore, possible that from an individual's perspective some passengers should not be allowed to fly that the government deems worthy of flying; or alternatively, a passenger's perspective could be more permissive.

Song and Zhuang (2017) study a two-stage screening system with potential errors in each stage. In each stage, a passenger is screened and labeled as clear or not-clear. The authors combine queuing theory and game theory concepts to design and numerically solve an analytical model. Findings of the research show that the two-stage system is always superior to the one-stage system for reducing congestion and improving the security level.

5.3. Baggage Screening

Virta et al. (2003) compare two baggage-screening scenarios in airports. The checked baggage is divided into two types: selectee and non-selectee. The authors compare the system in which only selectee baggage is screened with the system in which, if there is excess capacity of the screening device, some of the non-selectee baggage is also screened. The cost structure includes the cost of deploying, maintaining, and operating the screening device for one year. The cost structure along with the volume of checked baggage screened and the resulting outcomes define the trade-offs between the two systems. The authors conclude that using excess capacity to screen non-selectee checked bags increases the expected annual cost, decreases the cost per checked bag screened, and increases the expected cost per detected threat. The most important finding of the research is that screening non-selectee checked bags results in a significantly lower increment of benefit in security per dollar spent.

Whereas Virta et al. (2003) focus on the system's total direct cost as the main objective, subject to the capacity limit of screening devices, ignoring the cost of errors, Candalino et al. (2004) identify the most effective configuration of baggage screening security devices to achieve the minimum expected total cost including the direct costs and the indirect costs associated with false alarms due to screening errors. The authors employ artificial intelligence techniques to obtain the optimal solution and find that under high probability of threat the best screening strategy is using fewer but more precise devices. Later, Feng et al. (2009) study the problem of designing sequential screening procedures using a Bayesian analysis. They develop metrics to assess the trade-off between system risk of Type I and Type II errors and costs associated with specific detection device configurations.

5.4. Port-Security and Container Screening

Containers move via highways, railroads and ships at sea; and there are transfer points on the way. Terrorists attempt to find the most vulnerable spot(s) to insert and hide weapons in the containers. The country of destination faces the problem of inspecting containers to avoid smuggling of weapons. The objectives of screening policies are to improve detection probability and minimize the cost and time required for inspection.

Bakır (2011) studies the container inspection problem as a Stackelberg game between a port authority (defender) as the leader and an attacker as the follower. The defender can either allocate resources to non-intrusive inspections en route or increase the physical security of facilities on the route (e.g., transfer facilities, container yards, warehouses and truck stops). The author models two problems: (1) a single container-route and (2) multiple container-routes. The results of the single container-route show that equal levels of security must be exerted at each site en route whereas in the case of multiple container-routes, there is a trade-off between the security of foreign seaports and the physical security of sites en route. Additionally, the resource allocations are influenced by the attacker's capability to detonate weapons remotely in transit or at a seaport.

Bakır (2011) exploits a leader-follower game, whereas, Bier and Haphuriwat (2011) study the same problem using a simultaneous game. The authors identify the right proportion of containers to be screened to minimize the defender's loss. The authors model a simultaneous zero-sum game played between the defender and the attacker. Initially, the research assumes that while a single inspection is applied, it can find multiple attack types. Then, the authors extend the model to the case of multiple attackers. The results suggest that threatening to retaliate against attacks may also be beneficial to defenders if the threat is credible. Moreover, high-consequence attacks (e.g., a nuclear weapon) are more likely to be deterred than low-consequence attacks (e.g., rifles). The authors assume all containers are homogenous (i.e., all have the same risk); and suggest that this research can be extended to the case of nonhomogeneous containers.

While Bakır (2011), and Bier and Haphuriwat (2011) study minimizing (maximizing) expected loss (gain) between a defender and attacker, and Concho and Ramirez-Marquez (2012) use the decision-tree approach to study vulnerability, cost, and tardiness. The scanning devices represent decision tree nodes and the outcomes are suspicious or unsuspicious containers. The defender has

three options after the inspection: continue screening, release containers or check them manually. The defender has three criteria to minimize: vulnerability, cost, and tardiness. Inspection strategies can be developed by investigating trade-offs among the objective functions. The authors also suggest an evolutionary algorithm to solve the problem. Through exemplary tests, the research results suggest that the best strategy is testing a small number of different configurations. Using some test examples, the authors suggest a threshold for sensors. A container is considered "suspicious" if the sensor reading is greater or equal to the threshold value.

McLay and Dreiding (2012) use a two-stage process for screening of containers searching nuclear materials smuggled to the US via container cargoes. Initially, a pre-screening process on all containers classifies containers into several given risk groups (high risk and low risk). Then the suspicious containers must be unpacked through a secondary inspection method. The secondary inspection is labor-intensive, costly and time-consuming. Therefore, in the secondary inspection, only a small proportion of containers are inspected. Given a set of independent devices, the research aims at defining a primary screening alarm. The authors formulate two linear programming models based on the knapsack model to maximize the detection probability subject to a budget limit constraint. They also suggest another model based on enforcing a threshold policy to find the optimal policy (instead of grouping) which is easier to implement. Computational results show that enforcing a threshold policy does not necessarily decrease the detection probability.

Bagchi and Paul (2017) study a three-player game. The players include the government, an importer and a terrorist group. They study the impact of Customs Trade Partnership Against Terrorism (C-TPAT), a voluntary program developed by the U.S. Customs and Border Protection Agency. An importer (a private firm) may sign up for the program provided it agrees to incur costs to secure its supply chain. In return, there is reduced scrutiny of the cargo of this firm which decreases the security clearance time at the port. The authors study the interactions between the following three security measures to minimize congestion at a port and improve security: (1) the degree of security required from the private importer (ii) resources spent by the government in gathering intelligence about the terrorist, and (iii) inspection of cargo. The results show that if the government has superior information, the terrorist group will not engage in smuggling activities.

5.5. Summary and Future Research

All research studies in this section are related to screening of either human beings (e.g., passengers) or objects (e.g., baggage and containers). Passenger screening research is primarily focused on studying the impact of classifying passengers into several groups and suggesting different degrees of inspection for different groups to minimize the false alarm rate. A potential future research direction is a joint determination of the number of groups and the number of security check-in servers assigned to each group.

A screening, search and detection system can be installed on specific gateways for a point search (such as seaports, airports and land borders) or installed as fixed-location monitors (sensors) or moving monitors (sensors) to search non-point regions like coastal waters, lakes and illegal border entries. Regardless of the type of application of a screening and search problem, almost all research studies investigate trade-offs between accuracy, cost, and time of detection. Accuracy of detection is critical because the system is dealing with terrorist attacks which are considered to be low-probability-high-consequence acts. Cost is important because all fixed and moving devices and sensors are very costly, high-tech equipment. Time is also vital as long waiting times of people (e.g., passengers or museum visitors) or objects (e.g., delay in sending parcels carried by a mailing company) are significant societal costs. The current body of research follows two streams: (1) traditional quality control approaches in inspection and sampling and (2) reliability approaches in the design of systems that combine parallel and series inspections and screening devices. We foresee that future research problems will follow the same pattern as in the past. Consequently, we recommend that new research efforts should mainly focus on specific applications as extensions of threads of prior research work. The constant possibility of new technologies being developed expands these horizons. For example, a system designed and used in container screening for radioactive materials is different from systems used for passenger screening in airports searching for explosives. The difference is not only regarding the type of devices but also in terms of how many of them are used and how they are linked (series and parallel). While a government may highly weigh the accuracy of detection, commercial organizations (e.g., airlines) also care about their business costs and competitive factors.

Keeping a balance between the interests of government and commercial organizations can be a valuable potential direction for future research. This last possibility raises interesting questions about combining commercial objectives with societal goals. Models to find optimal allocation of resources between profiling and screening to meet a given level of societal security can be extended to cargo security as well as port security.

6. Forensics and Attribution

Forensics and Attribution is the category that deals with learning about terrorist groups, their attack modes, sources, timing and locations so that attacks might be prevented. While DHS does not limit this core capability to any specific attack mode, they focus on chemical, biological, radiological, nuclear, and explosive (CBRNE) materials. Obviously, data collection and finding strong evidence is critical for analysis in this core capability. We found the following eight papers focusing on different issues that are relevant for this section: Sullivan and Perry (2004), Schumaker and Chen (2007). Atkinson and Wein (2008), Szechtman et al. (2008), Hochbaum and Fishbain (2011), Dimitrov et al. (2015), Fu et al. (2015), and Yan and Nie (2016).

Intelligence and (CBRNE) weapons: Sullivan and Perry (2004) propose investigating the behavior of terrorist groups to trace the development of chemical, biological, radiological or nuclear (CBRNE) weapons. Observations of a terrorist group during various stages of the development of CBRNE include technical capacity, organizational capacity, opportunity, leadership mind-set and ideology, isolation from outside, internal restraint, external restraint, defensive aggression, and available alternatives. Such data allow intelligence agencies to conduct statistical analysis to learn about the level of development of CBRNE weapons.

Dialog-based ALICEbots: Schumaker and Chen (2007) investigate how dialog-based ALICEbots (a class of Question-Answer programs designed by Richard Wallace in 1995), (Wallace 2009), can distribute information about terrorism to the public. To better serve the terrorism scenario, the authors modified the ALICEbots and have proposed the Terrorism Activity Resource Application (TARA) system. The results show that a system that utilizes knowledge of both general conversation and terrorism, performs better than the two forms of knowledge separately.

Sensors and Surveillance of Terrorist: Atkinson and Wein (2008), Szechtman et al. (2008), Hochbaum and Fishbain (2011), and Yan and Nie (2016) have studied surveillance of terrorist activities using fixed and mobile sensors for intelligence gathering in different settings. Atkinson and Wein (2008) study the problem of detecting a radiological weapon (a dirty bomb) mounted on a vehicle that is moving in a city to reach its target destination. The sensor mounted vehicles (interdiction vehicles) are used to locate the vehicle carrying the bomb. The interdiction vehicles form a circular wall and chase any vehicle that sets off the alarm. The authors use a spatial queueing model that incorporates scarce interdiction resources and implicitly accounts for false positives. Hochbaum and Fishbain (2011) also study the detection of radioactive sources in densely populated areas through the creation of mobile Distributed Sensor Networks (DSN). The sensors in the DSN are installed on public service vehicles (e.g., taxicabs, police cars, fire trucks, trains or buses) moving around urban areas. GPS tracks the location of each vehicle in real-time. Based on the information collected from these vehicles, the system discovers the existence of any nuclear source and identifies its approximate location. The objective is to reduce the likelihood of false-positive and false-negative errors. Yan and Nie (2016) study the problem of placing detectors (fixed-position sensors) in a port to track small vessels that carry water-borne explosive devices to attack maritime targets. The detectors can identify radiological, chemical, and biological materials. There are multiple types of detectors with different costs, detection rates, and effective detection radii. The objective is to find the mix of detectors to be placed to minimize expected damage subject to a budget limit for detectors.

Border Surveillance and Illegal Immigrants: Szechtman et al. (2008) study a border surveillance problem in which illegal immigrants, including terrorists, attempt to enter the U.S.A. Infiltrators arrive randomly in a Poisson process at random locations on the border, and after a random duration, if undetected, infiltrate. Two types of sensors are studied: (i) the sensor scans from the start point to the end point of the border and then jumps back to the start point again; (ii) a UAV-mounted sensor that moves continuously back and forth between the start and end points. The decision variables include starting and end points, and the velocity of the sensor.

Collecting Intelligence via Social Media: Dimitrov et al. (2015) focus on collecting intelligence from communications in social media. Such communications can be divided into (1) by terrorists and

(2) by harmless people. Intelligence thus collected can be analyzed for identification of adversaries. The model developed by these authors has two main elements: (i) nodes of the network which are people participating in communications and (ii) edges which are the content communicated between the nodes. The authors propose an algorithm to prioritize the accumulated intelligence for actions to identify terrorist activities.

Characteristics of Terrorist Activities: Fu et al. (2015) introduce the following six elements to learn about terrorist activities: people, organization, time, location, manner and event. They use empirical data related to regions around Xinjiang Uyghur (China) with special focus on East Turkistan terrorist groups. They employ network modeling and correlation analysis as their analytical tools. These methods can help in clustering groups engaged in various terrorist activities. While the results are validated, such problems are complicated because many factors in the fields of politics, economy, culture, history, society and education, affect such analyses.

Screening in Public Areas: Lin et al. (2009) study a surveillance system to screen people in a large public area (e.g., an airport lobby or a tourist attraction). People arriving at the public area are first visually examined and are placed into two groups: non-suspects and suspects. Suspects are subjected to further screening. The surveillance system has a capacity limit of screening one person at a time. The authors model the problem as an M/G/1 queue, and prescribe a heuristic dynamic policy to maximize the probability of detecting a terrorist. They use numerical examples in which arrival rates follow a Poisson process. The following service rules are used: First-Come-First-Serve, Last-Come-First-Serve, Random-Selection, or heuristic. A ratio of expected reward to required serving time can be maximized by the heuristic which chooses customers that have the highest expected reward rate.

Terrorist Communication in Social Network: Lindelauf et al. (2013) view a terrorist organization as a social network. They use terrorists' personal information and their interrelationships to identify key players in a terrorist network to prevent attacks. A terrorist organization tries to keep minimum interaction (in terms of duration and frequency) with outsiders. However, they need to maintain communications with members within their network for coordinating attacks. The authors use Shapely values in a cooperative game to rank the key players. Therefore, the authors' suggested

approach is based on constructing the network, defining the game and rankings of players. This approach can help a government to damage a terrorist organization by removing their high-ranked members. The approach is tested on two terrorist attacks namely the Bali bombing and the 9/11 attacks.

6.1. Summary and Future Research

Almost all building blocks of forensics and attribution have been well covered. The majority of research topics in the area have been dedicated to collecting and analyzing intelligence from people participating in social media. Detection of terrorists and their tools (e.g., vehicles) has also been well explored. When it comes to means and methods of terrorism, chemical, biological, radiological or nuclear (CBRN) weapons have drawn more attention than the others. Bombings, suicide attacks, vehicle-based attacks, aircraft attacks, and hijackings also need more attention. Further, it is important to analyze the sources of support for terrorism including financial, information and human ~~resources~~ beliefs and ideology.

We recognize that this area is understudied. Machine learning techniques, time series, regression, clustering, data mining, explosives sensing devices, and social media can play an important role in the collection and analysis of terrorism-related intelligence. Possible explanations about why this area is underexplored could be either the lack of empirical data or the need for gathering large amounts of data. Empirical data play an important role in this core capability. Some of these data are easily accessible and some are highly confidential that can only be acquired through intelligence (refer to Section 2 on Intelligence and Information Sharing for some relevant research papers).

7. Conclusions and Directions for Future Research

In this paper, we review POM research to fight terrorism. The research findings are grouped in the core capabilities of the FEMA's prevention mission, FEMA (2015). The review shows significant opportunities for future research in combatting terrorism. Future research directions are included in each section. In this section, we discuss additional recommendations that cut across various core capabilities. Table 1 summarizes these research directions; and are further discussed in Section A9 in

the online appendix.

Table 1: Future Research Direction

Topics	Research Issues
Modelling and solution techniques	- Multi-players - Multi-criteria decision making for each player (including multiple objectives and multiple attributes) - Infinite horizon - Non-zero sum games - Dynamic aspects • Multi-period problems • Dynamic games (e.g., dynamic re-allocation problems) - Repeated game with learning - Uncertainty aspects • Fuzzy theory • Simulation • Stochastic dynamic programming • Bayesian inference • Robust optimization - Data driven optimization
Learning from commercial SCM concepts	**Financial flow:** (1) Disrupting and destroying terrorists' financial SCs is essential; (2) Tracking unusual financial transactions may provide vital intelligence; (3) Governments can also find other avenues to curb the flow of money that support terrorism. **Physical flow:** (1) Mapping the attackers' SC in terms of acquisition, purchasing, distributing and assembling of materials and spare parts; (2) monitoring physical movements across all transportation modes; (3) identifying weak and vulnerable points in the attacker's SC for disrupting and destroying them and strengthening defender's vulnerable points; (4) Learning from the past considering prior and posterior functions, forming strategic alliances between multiple attackers or multiple defenders. **Information flow:** Refer to Section "2. Intelligence and Information Sharing"
Empirical research	- Collaboration between POM researchers and FEMA administrators could provide avenues for data collection. - Researchers should collect and analyze data available through social media.
New concepts and techniques	Including behavioral aspects (e.g., prospect theory, regret theory, bounded rationality) related to the attacker, defender and people

ACKNOWLEDGMENT

The authors would like to thank the review team for their valuable comments that helped them improve the paper significantly. We are especially grateful to the referee who suggested Figures 1 and 4 and permitting their inclusion in the paper.

References

We have included references in Section A10 in the online appendix.

ONLINE APPENDIX

A1. The Department of Homeland Security

DHS (2015) has defined the following five *mission areas* to combat and face challenges posed by catastrophic disasters: prevention, protection, mitigation, response, and recovery. Gupta et al. (2016), in their survey paper mentioned: "Sound prevention/mitigation strategies can possibly reduce efforts and resources spent on humanitarian logistics activities." DHS uses the word "terrorism" in defining its prevention mission which is stated as, *"Preventing, avoiding, or stopping a threatened or an actual act of terrorism."* We review POM research in support of this theme and provide directions for future research.

DHS (2015) has identified a set of *core capabilities* for each mission area. DHS (2015) states that *"Further, there is an expectation that each of the core capabilities will leverage advances in science and technology and be improved through post-event evaluation and assessment."* This is where developments and advances in POM's disaster research can contribute to the successful management of disasters.

Brief explanations of the seven core capabilities for the mission area "prevention" are provided below with more elaborate descriptions in the respective sections.

1. *Intelligence and Information Sharing:* This core capability requires collection, analysis, evaluation and dissemination of information. Information sharing deals with the capability to exchange intelligence among government or private sector entities.

2. *Planning:* Engage everyone who can play a role in the development of operational strategies and successful tactics aimed at achieving well-defined objectives.

3. *Interdiction and Disruption:* Stop, prevent, divert, intercept, halt and apprehend the agents of terror and/or hazards caused by nature or human-error.

4. *Screening, Search, and Detection:* Discover threats (hazards of any kind) through both proactive means and passive surveillance. Search processes should include systematic procedures for locating sources of damage or danger using bio-assessments, sensor technologies to provide maximal

investigative power and intelligence.

5. *Forensics and Attribution:* Use forensic methods to uncover terrorist intentions leading to acts that include the means and methods of terrorism. Tracing causal possibilities to their source is necessary to prepare for an attack of any kind. This is a procedure used to prevent initial or follow-on acts of terror. It is needed to develop counter-options.

6. *Public Information and Warning:* Communicate promptly the reliable and implementable information that is vital to protect against threats and hazards.

7. *Operational Coordination:* Coordinate all critical stakeholders into a unified operational structure which supports the core process capabilities of prevention.

A2. Search Methodology

Initially, we used the same 25 journals to identify papers of interest that were used by Gupta et al. (2016). These journals were searched in the full-text context using the keywords "terrorism", "terrorist", "attacker", "disaster", "disasters", "apocalypse", "calamity", "cataclysm", "catastrophe", "debacle", "tragedy", "crisis" and "crises". We employed Google Scholar as the search engine. We found a total of 75 publications in thirteen of the 25 journals. The remaining 12 journals had no relevant papers. Our search extended from the year 1957 to the year 2017.

In addition to the 25 journals, we decided to search some more reputable journals in the non-POM fields that are likely to publish papers on the prevention of terrorism. To select these journals, we examined the bibliographies of the 75 papers and identified those journals in which terrorism-related articles had been published. This new set of journals, based on the bibliographic review, was rather large, and included journals that do not command the same respect as the 25 journals used by Gupta et al. (2016). Therefore, a subset of these newly identified journals was selected based on their meeting at least one of the following four criteria: (1) they appear in the Financial Times list, (2) they appear in the University of Texas, Dallas (UTD) list that is used to rank top 100 Business Schools, (3) their rank is 3* or above in the Academic Journal Guide (AJG) 2018 - Chartered Association of Business Schools, and (4) their rank is "A" or above in the Australian Business Deans Council (ABDC) Journal Quality List of 2016. Based on these four criteria, the following seven journals

(listed in alphabetical order) were identified for inclusion in the search process. These journals span the fields of information sciences (IS), political science, and economics.

1. Canadian Journal of Economics
2. Economica
3. European Journal of Political Economy
4. Journal of Conflict Resolution
5. Journal of Management Information Systems
6. Journal of Political Economy
7. Risk Analysis

These seven journals were searched and any paper that had at least one of the following words, *terrorism*, *terrorist*, or *attacker* in the journal title or abstract, was included. The search engine used was SCOPUS.

In addition, we have included the following twelve studies to enhance and enrich our discussion of terrorism prevention research: Frey and Luechinger (2003), Gupta et al. (2016), Hausken and Zhuang (2011), Kaplan (2010), Keohane and Zeckhauser (2003), Kunreuther and Heal (2003), Levitin and Hausken (2009), Loch and Wu (2007), Nandi et al. (2016), Sandler and Acre (2003), Sandler and Siqueira (2005), and Starr and Wassenhove (2014).

Figure A1 lists the count of papers by the contributing journals. Five journals published 7 or more papers for a total of 56 papers out of 91 (61.5%). These journals include the European Journal of Operational Research (20 papers), Annals of Operations Research (11 papers), Operations Research (9 papers), Journal of the Operational Research Society (9 papers), and Naval Research Logistics (7 papers). These journals primarily publish modeling-based methodology papers. This observation points to the opportunity for more empirical and practice-oriented research.

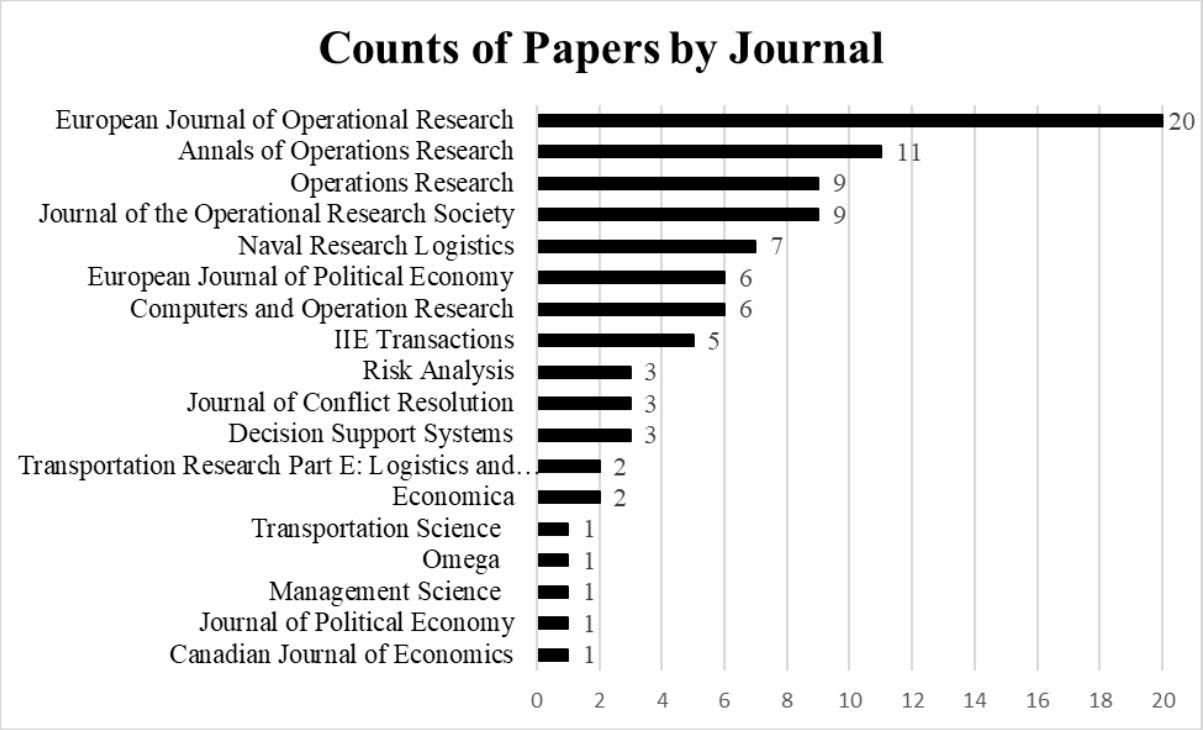

Figure A1: Count of 91 papers by contributing journals.

A3. Count of Papers by DHS Core Capability

Table A1 gives the count of papers by year for each DHS core capability. Opportunities for research seem to exist for the categories with only a few papers.

Table A1: Count of papers by DHS core capabilities by year

Core Capability/Year	1957 to 2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	Total
Intelligence and Information Sharing	1	0	0	0	0	0	0	1	0	0	2	0	0	0	1	2	2	0	9
Planning	1	0	0	0	2	2	1	4	1	3	1	4	2	4	2	5	5	1	38
Interdiction and Disruption	3	0	0	0	3	1	0	2	1	1	1	4	2	2	1	0	3	0	24
Screening, Search, and Detection	1	0	0	1	1	0	2	0	0	4	3	2	4	0	1	0	1	1	21
Forensics and Attribution	0	0	0	0	1	0	0	1	2	1	0	1	0	1	0	2	1	0	10
Operational Coordination	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Public Information and Warning	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	2
Total	6	1	0	1	7	3	3	9	4	9	7	11	9	8	6	9	13	2	105

Note: The total count (105) is more than 91 because some papers belong to more than one category, and are counted more than once.

A4. Cross-tabulation of core capabilities vs. data type

We have divided the type of data used in disaster research into the following four categories: Field and Archival (F&A), Hypothetical, Real and No Data. F&A refer to empirical data, which

include primary, secondary and tertiary data widely used in empirical research. The cross-tabulations between core capability and data type are provided in Table A2. Some papers belong to more than one cell and, therefore, the total is more than 91.

Table A2: Core Capability vs. Data Type.

Core Capability vs. Data Type	F&A	Hypothetical	Real	Case Study	No Data	Total
Intelligence and Information Sharing	4	1	0	0	4	9
Planning	8	9	3	1	17	38
Interdiction and Disruption	3	5	1	0	15	24
Screening, Search, and Detection	7	5	4	0	5	21
Forensics and Attribution	2	2	1	3	2	10
Operational Coordination	0	0	0	0	1	1
Public Information and Warning	0	2	0	0	0	2
Total	24	24	9	4	44	105

Note: The total count (105) is more than 91 because some papers belong to more than one category, and are counted more than once.

A5. Cross-tabulation of core capabilities vs. analytical technique

Tables A3 cross tabulates each core capability against analytical techniques. We identified the following nine analytical techniques that have been used in terrorism research: adversarial risk analysis, decision analysis, game theory, mathematical programming, queueing theory, social network analysis, statistical analysis, qualitative analysis, and heuristics/meta-heuristics.

Table A3: Core Capability vs. Data Analysis Technique.

Core Capabilités vs. Data Analysis Technique	Adversarial Risk Analysis	Decision Analysis	Game Theory	Mathematical Programming	Queueing Theory	Social Network Analysis	Statistical Analysis	Qualitative	Heuristics/ Meta-heuristics	Total
Intelligence and Information Sharing	0	0	6	2	0	0	1	0	0	9
Planning	1	0	33	3	0	0	1	0	0	38
Interdiction and Disruption	0	0	13	7	0	0	2	2	0	24
Screening, Search, and Detection	0	1	6	11	1	0	1	0	1	21
Forensics and Attribution	0	0	1	6	0	1	2	0	0	10
Public Information and Warning	0	0	0	2	0	0	0	0	0	2
Operational Coordination	0	0	1	0	0	0	0	0	0	1
Total	1	1	60	31	1	1	7	2	1	105

Note: The total count (105) is more than 91 because some papers belong to more than one category, and are counted more than once.

A6. Cross-tabulations of data types vs. analytical techniques

Table A4 gives Data Types vs. Analysis Technique. Data type and analytical techniques are described in Tables A2 and A3 respectively.

Table A4: Data Type vs. Data Analysis Technique.

Data Types vs. Analytical Technique	Adversarial Risk Analysis	Decision Analysis	Game Theory	Mathematical Programming	Queuing Theory	Social Network Analysis	Statistical Analysis	Qualitative Analysis	Heuristics/ Meta-heuristics	Total
F&A	1	0	8	6	1	1	3	0	1	21
Hypothetical	0	1	12	8	0	0	1	0	0	22
Real	0	0	2	3	0	0	3	0	0	8
Case Study	0	0	2	2	0	0	0	0	0	4
No Data	0	0	24	10	0	0	0	2	0	36
Total	1	1	30	13	1	1	5	2	1	91

A7. Public Information and Warning

Public Information and Warning is of great potential value but it is not well studied. There is only one paper that deals with this topic. We have included it in the appendix since we believe that it is a subject of potential benefit for future research.

Public information can be useful for the whole community before a terrorist attack and also after an attack to help people with evacuation, locating shelter, routing, etc. There are two types of warnings: public and private. Public warnings are issued to the general public whereas the private warnings are issued to the security forces. Warnings are less expensive but also less effective as compared to physical deployment of security forces. We found only one paper relevant to this section. Pinker (2007) studies trade-offs between warnings and deployment of security forces under uncertainty in the timing and location of attacks. The author shows how the probability of attack, the vulnerability of the target and the value of target (economically and politically) determine terrorism costs. The results also suggest that governments should avoid public warning and rely more on private warnings.

Future Research

Awareness of people, stakeholders, and also law enforcement is the key to having a successful public information system for terrorist prevention and/or mitigation of impact severity. Social media and big data analytics can be useful tools in gathering information and issuing warnings to the public about terrorist attacks. Data need to be collected about suspicious behaviors of people and other anomalies. The application of public information and detection is not limited to critical data about transportation systems associated with airports, bus stops or train stations. Targets such as hospitals, tourist attractions and malls that can be appealing to terrorist groups are also relevant to this core capability.

Research in the area should include possible errors (i.e., false clear and false alarm). Practically, a well-designed system should carefully consider removing false alarm signals to reduce the "crying wolf" effect. Obviously, using information technology is an inseparable component of research within this core capability. For example, developing optimal mobile systems for public warnings throughout a region might become a significant research stream in this domain. Finally, the reaction of people to warnings in various geographical regions may differ depending on culture and behavioral characteristics. This can also be a possible fruitful future research direction.

A8. Operational Coordination

Operational Coordination is of great potential value but it is not well studied at the micro-level of coordination. We have included it in the appendix because we only found papers at the macro-level of coordination. We believe that micro-coordination is a subject of potential benefit for future research.

Operational Coordination organizes all critical stakeholders into a unified operational structure which supports the core process capabilities of prevention. Coordination can be viewed at two levels: (1) coordination at the micro-level in which various state agencies and the public are involved in orchestrating a plan to fight terrorism, and (2) coordination at the macro level in which various governments are involved. We did not find any relevant paper at the micro-level of coordination. However, macro-level coordination can be studied by using the SCM point of view. Some of the pertinent papers for coordination include Golden (1978), Washburn and Wood (1995), Cormican et al. (1998), Brown et al. (2009), Baveja and Wein (2009), and Shan and Zhuang (2014). These papers

have been discussed earlier in subsection 4.4, Weapons of Mass Destruction. Coordination is a prime example of a core capability that cuts across many domains and requires consideration at various levels with different perspectives.

Future Research

Coordination requires efficient processes which provides an opportunity for important POM research. Development of such processes is important at the country level, state level, and local level, and among various government and non-government agencies. This subject is also discussed in subsection 3.3.

A9. Conclusions and Directions for Future Research

Future research directions are included in each section. In this section, we discuss additional recommendations that cut across various core capabilities. Table 1 in Section 9 summarizes these research directions.

A9.1. Modeling and solution technique

Most of the models presented in the literature have used only a single objective – primarily the optimization of defensive investments. However, the models can be extended by using multi-criteria decision making (MCDM) wherein both the attacker and the defender may be able to include multiple objectives and multiple attributes. Future models could include deception, pre-emptive action and multi-targets. Extension of research to non-zero-sum games is also a potential research area. Studying multi-period problems is another important research direction. In a multi-period game, or in an infinite horizon dynamic game, the defender-attacker strategies are likely to change from period to period. Stochastic dynamic programming may be an efficient tool to show the optimal policy based on prior and posterior distributions with learning over time in attacker-defender games. Extending models to multi-players (population games) is another interesting research direction. For multi-players, levels of proliferation, attack, defense, and subsidy could be continuous variables. This would make the model more realistic and provide interesting scenarios.

We also make recommendations about modeling techniques. Uncertainty about parameters in

game-theoretic models has made researchers use certain techniques extensively such as stochastic optimization, robust optimization, and simulation. These techniques will remain important as long as the probabilities of various scenarios are known. However, building scenarios of events that have not happened in the past (often called black swan events, Taleb (2007)) requires more creativity. In other words, historical data can help us build models that may tell us what happens in the future (if the future looks like the past). In reality, terrorists may take actions in the future which do not have any prior precedents. Fuzzy theory can help model disaster management problems which lack sufficient historical and reliable data. As the problem complexity increases simulation will be an appealing technique to use. Data-driven optimization can also be an excellent research direction because a lack of data and intelligence will make us think more of data-driven modeling than problem-driven modeling. Data-driven optimization methods enable us to make informed decisions based on using the limited available data.

We observed that the majority of game theory models are leader-follower models in which either the defender or the attacker is the leader depending on who makes the first move. Research on simultaneous games needs to be further explored. In addition to game theory, terrorism research is amenable to alternative methodologies like predictive analytics (including data mining), preventive maintenance, statistical quality control, search theory, specialized statistical techniques, utility functions, utility maximization models, time series analytics, spectral analysis and pattern recognition, whenever historical data are available.

A9.2. Learning from commercial SCM concepts

There are two competing groups that influence the development of terrorism SCs. Terrorists want to develop their SCs whereas the defenders what to destroy these SCs. Defenders have to identify targets (events and partners) that are susceptible to be destruction. Should the developer of the arms be targeted or the transporter or the final terrorist? Financial SCs supporting terrorists' activities have also to be targeted and destroyed. This is an interesting and important area for research. Development of SCs for disaster management mainly for the prevention of terrorism can benefit from developments in SCs for business and industry. This requires broad-based research, specifically for terrorism, in

financial, material, and information flows.

Terrorist groups need substantial financial resources to implement their plans. Tracking unusual financial transactions may provide vital intelligence. Governments can also find other avenues to curb the flow of money that supports terrorism. One interesting example is the Draconian step taken by the Indian government in 2016 as described below. *"On 8 November 2016, Prime Minister of India Narendra Modi announced the demonetisation in an unscheduled live televised address to the nation at 20:15 IST. In the announcement, Modi declared circulation of all ₹500 and ₹1,000 banknotes of the Mahatma Gandhi Series as invalid effective from the midnight of the same day."* See https://en.wikipedia.org/wiki/2016_Indian_banknote_demonetisation.

"After Modi's announcement, the Governor of the Reserve Bank of India, Urjit Patel, and Economic Affairs secretary, Shaktikanta Das explained in a press conference that one purpose of the action was to fight terrorism funded by counterfeit notes. ……. They said that forged cash was used to fund terrorist activities against India and that the demonetisation had a counter-terrorism purpose." See http://www.news18.com/news/india/why-were-the-notes-scrapped-rbi-chief-and-economic-affairs-secretary-explain-1309756.html. We hasten to add that we have not seen any formal follow up report about the impact of this decision. This is a potential topic for significant research.

Readers are encouraged to read more about financing of terrorism at the website of The Financial Action Task Force (FATF) using the following: http://www.fatf-gafi.org/home/. FATF was established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF, an inter-governmental body, "*are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.*"

For high-intensity attacks, the attacker needs acquisition, purchasing, distributing and assembling of materials and spare parts. Monitoring physical movements across all transportation modes can also help the defender learn about potential attacks. Future research can focus on identifying weak and vulnerable points in the attacker's SC for disrupting and destroying them and strengthening defender's vulnerable points. Global SCs to fight terrorism are influenced by local laws and regulations, e.g., right to bear arms in the US can help attackers to have access to weapons easily.

Future research can focus on developing SCs that are more resilient to possible terrorist attacks with uncertain locations. Learning from the past considering prior and posterior functions, forming strategic alliances between multiple attackers or multiple defenders are other possible research areas.

A10. References

Arce, D. G., D. Kovenock, B. Roberson. 2012. Weakest-link attacker-defender games with multiple attack technologies. *Naval Research Logistics (NRL)* **59**(6) 457–469.

Arce, D. G., T. Sandler. 2005. Counterterrorism: A game-theoretic analysis. *Journal of Conflict Resolution* **49**(2) 183–200.

Atkinson, M. P., L. M. Wein. 2008. Spatial queueing analysis of an interdiction system to protect cities from a nuclear terrorist attack. *Operations Research* **56**(1) 247–254.

Babu, V. L. L., R. Batta, L. Lin. 2006. Passenger grouping under constant threat probability in an airport security system. *European Journal of Operational Research* **168**(2) 633–44.

Bagchi, A., J. A. Paul. 2014. Optimal allocation of resources in airport security: Profiling vs. Screening. *Operations Research* **62**(2) 219–233.

Bagchi, A., J. A. Paul. 2017. Espionage and the optimal standard of the Customs-Trade Partnership against Terrorism (C-TPAT) program in maritime security. *European journal of operational research* **262**(1) 89–107.

Bakır, N. O. 2011. A Stackelberg game model for resource allocation in cargo container security. *Annals of Operations Research* **187**(1) 5–22.

Bandyopadhyay, S., T. Sandler. 2011. The interplay between preemptive and defensive counterterrorism measures: A two-stage game. *Economica* **78**(311) 546–564.

Baveja, M., L. M. Wein. 2009. An effective two-finger, two-stage biometric strategy for the US-VISIT program. *Operations Research* **57**(5) 1068–1081.

Baykal-Gürsoy, M., Z. Duan, H. V. Poor, A. Garnaev. 2014. Infrastructure security games. *European Journal of Operational Research* **239**(2) 469–478.

Berman, O., A. Gavious. 2007. Location of terror response facilities: A game between state and terrorist. *European Journal of Operational Research* **177**(2) 1113–1133.

Berndt, D. J., J. W. Fisher, J. G. Craighead, A. R. Hevner, S. Luther, J. Studnicki. 2007. The role of data warehousing in bioterrorism surveillance. *Decision Support Systems* **43**(4) 1383–1403.

Bier, V. M., N. Haphuriwat. 2011. Analytical method to identify the number of containers to inspect at US ports to deter terrorist attacks. *Annals of Operations Research* **187**(1) 137–158.

Bier, V. M., K. Hausken. 2011. Endogenizing the sticks and carrots: modeling possible perverse effects of counterterrorism measures. *Annals of Operations Research* **186**(1) 39–59.

Brown, G. G., W. M. Carlyle, R. C. Harney, E. M. Skroch, R. K. Wood. 2009. Interdicting a nuclear-weapons project. *Operations Research* **57**(4) 866–877.

Candalino Jr, T. J., J. E. Kobza, S. H. Jacobson. 2004. Designing optimal aviation baggage screening strategies using simulated annealing. *Computers & Operations Research* **31**(10) 1753–1767.

Cano, J., D. R. Insua, A. Tedeschi, U. Turhan. 2016. Security economics: an adversarial risk analysis approach to airport protection. *Annals of Operations Research* **245**(1–2) 359–378.

Carlyle, W. M., S. G. Henderson, R. Szechtman. 2011. Allocating capacity in parallel queues to improve their resilience to deliberate attack. *Naval Research Logistics (NRL)* **58**(8) 731–742.

Caulkins, J. P., D. Grass, G. Feichtinger, G. Tragler. 2008. Optimizing counter-terror operations: Should one fight fire with "fire" or "water"? *Computers & Operations Research* **35**(6)1874–1885.

Cavusoglu, H., B. Koh, S. Raghunathan. 2010. An analysis of the impact of passenger profiling for transportation security. *Operations Research* **58**(5) 1287–1302.

Concho, A. L., J. E. Ramirez-Marquez. 2012. Optimal design of container inspection strategies

considering multiple objectives via an evolutionary approach. *Annals of Operations Research* **196**(1) 167–187.

Cormican, K. J., D.P. Morton, R. K. Wood. 1998. Stochastic network interdiction. *Operations Research* **46**(2) 184–197.

DHS (Department of Homeland Security), 2015. *National Preparedness Goal*. Washington, D.C.: U.S. Retrieved from https://www.fema.gov/media-library-data/1443799615171-2aae90be55041740f97e8532fc680d40/National_Preparedness_Goal_2nd_Edition.pdf (last visited on 31 January 2020)

Dimitrov, N. B., M. Kress, Y. Nevo. 2016. Finding the needles in the haystack: efficient intelligence processing. *Journal of the Operational Research Society* **67**(6) 801–812.

FATF (The Financial Action Task Force). 2019. http://www.fatf-gafi.org/home/, (last visited on 17 July 2019)

Feng, Q., H. Sahin, M. J. Karson. 2009. Bayesian analysis models for aviation baggage screening. *IIE Transactions* **41**(11) 995–1006.

FitzGerald, V. 2004. Global financial information, compliance incentives and terrorist funding. *European Journal of Political Economy* **20**(2) 387–401.

Frey, B. S., S. Luechinger. 2003. How to fight terrorism: alternatives to deterrence. *Defence and Peace Economics* **14**(4) 237–249.

Frey, B. S., S. Luechinger. 2004. Decentralization as a Disincentive for Terror. *European Journal of Political Economy* **20**(2) 509–515.

Fu, J., D. Sun, J. Chai, J. Xiao, S. Wang. 2015. The "six-element" analysis method for the research on the characteristics of terrorist activities. *Annals of Operations Research* **234**(1) 17–35.

Garcia-Alonso, M. D. C., P. Levine, R. Smith. 2016. Military aid, direct intervention and counterterrorism. *European Journal of Political Economy* **44**(1) 112–135.

Golany, B., N. Goldberg, U. G. Rothblum. 2015. Allocating multiple defensive resources in a zero-sum game setting. *Annals of Operations Research* **225**(1) 91–109.

Golany, B., N. Goldberg, U. G. Rothblum. 2017. A two-resource allocation algorithm with an application to large-scale zero-sum defensive games. *Computers & Operations Research* **78** 218–229.

Golany, B., E. H. Kaplan, A. Marmur, U. G. Rothblum. 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.

Golden, B. 1978. A problem in network interdiction. *Naval Research Logistics Quarterly* **25**(4) 711–713.

Gupta, S., M. K. Starr, R. Z. Farahani, N. Matinrad. 2016. Disaster management from a POM perspective: mapping a new domain. *Production and Operations Management* **25**(10) 1611–1637.

Haphuriwat, N., V. M. Bier. 2011. Trade-offs between target hardening and overarching protection. *European Journal of Operational Research* **213**(1) 320–328.

Hausken, K. 2008. Strategic defense and attack for series and parallel reliability systems. *European Journal of Operational Research* **186**(2) 856–881.

Hausken, K., V. M. Bier. 2011. Defending against multiple different attackers. *European Journal of Operational Research* **211**(2) 370–384.

Hausken, K., J. Zhuang. 2011. Governments' and terrorists' defense and attack in a T-period game. *Decision Analysis* **8**(1) 46–70.

Hausken, K., J. Zhuang. 2012. The timing and deterrence of terrorist attacks due to exogenous dynamics. *Journal of the Operational Research Society* **63**(6) 726–735.

He, F., J. Zhuang. 2012. Modelling 'contracts' between a terrorist group and a government in a sequential game. *Journal of the Operational Research Society* **63**(6) 790–809.

Hochbaum, D. S., B. Fishbain. 2011. Nuclear threat detection with mobile distributed sensor networks. *Annals of Operations Research* **187**(1) 45–63.

Hohzaki, R., T. Higashio. 2016. An attrition game on a network ruled by Lanchester's square

law. *Journal of the Operational Research Society* **67**(5) 691–707.

Indian banknote demonetisation, 2016. Available online on https://en.wikipedia.org/wiki/2016_Indian_banknote_demonetisation (last visited on 18 September 2018)

Jacobson, D., E. H. Kaplan. 2007. Suicide bombings and targeted killings in (counter-) terror games. Journal of Conflict Resolution **51**(5) 772–792.

Jacobson, S. H., J. E. Kobza, A. S. Easterling. 2001. A detection theoretic approach to modeling aviation security problems using the knapsack problem. *IIE Transactions* **33**(9) 747–759.

Jin, J. G., L. Lu, L. Sun, J. Yin. 2015. Optimal allocation of protective resources in urban rail transit networks against intentional attacks. *Transportation Research Part E: Logistics and Transportation Review* **84** 73–87.

Kaplan, E. H. 2010. Terror queues. *Operations Research* **58**(4–part-1) 773–784.

Kaplan, E. H. 2012. OR forum-intelligence operations research: The 2010 Philip McCord Morse lecture. *Operations Research* **60**(6) 1297–1309.

Keeney, R. L. 2007. Modeling values for anti-terrorism analysis. *Risk Analysis* **27**(3) 585–596.

Keohane, N. O., R. J. Zeckhauser. 2003. The ecology of terror defense. In: *The Risks of Terrorism* (103–131). Springer US.

Kobza, J. E., S. H. Jacobson. 1997. Probability models for access security system architectures. *Journal of the Operational Research Society* **48**(3) 255–263.

Konrad, K. A. 2004. The investment problem in terrorism. *Economica* **71**(283) 449–459.

Kunreuther, H., G. Heal. 2003. Interdependent security. *Journal of Risk and Uncertainty* **26**(2–3) 231–249.

Lapan, H. E., T. Sandler. 1993. Terrorism and signaling. *European Journal of Political Economy* **9**(3) 383–397.

Levitin, G., K. Hausken. 2009. Redundancy vs. protection vs. false targets for systems under attack. *IEEE Transactions on Reliability* **58**(1) 58–68.

Levitin, G., K. Hausken. 2013. Defence resource distribution between protection and decoys for constant resource stockpiling pace. *Journal of the Operational Research Society* **64**(9) 1409-1417.

Li, D., J. B. Cruz Jr. 2009. Information, decision-making and deception in games. *Decision Support Systems* **47**(4) 518–527.

Lim, C., J. C. Smith. 2007. Algorithms for discrete and continuous multicommodity flow network interdiction problems. *IIE Transactions* **39**(1)15–26.

Lin, K. Y., M. Kress, R. Szechtman. 2009. Scheduling policies for an antiterrorist surveillance system. *Naval Research Logistics (NRL)* **56**(2) 113–126.

Lindelauf, R. H. A., H. J. M. Hamers, B.G.M. Husslage. 2013. Cooperative game theoretic centrality analysis of terrorist networks: The cases of Jemaah Islamiyah and Al Qaeda. *European Journal of Operational Research* **229**(1) 230–238.

Loch, C. H., Y. Wu. 2007. Behavioral operations management. *Foundations and Trends in Technology, Information and Operations Management* **1**(3) 121–232.

Majeske, K. D., T. W. Lauer. 2012. Optimizing airline passenger prescreening systems with Bayesian decision models. *Computers & Operations Research* **39**(8) 1827–1836.

McLay, L. A., R. Dreiding. 2012. Multilevel, threshold-based policies for cargo container security screening systems. *European Journal of Operational Research* **220**(2) 522–529.

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

McLay, L. A., S. H. Jacobson, J. E. Kobza. 2006. A multilevel passenger screening problem for aviation security. *Naval Research Logistics* **53**(3) 183–197.

Mo, H., M. Xie, G. Levitin. 2015. Optimal resource distribution between protection and redundancy considering the time and uncertainties of attacks. *European Journal of Operational Research* **243**(1) 200–210.

Nandi, A. K., H. R. Medal. 2016. Methods for removing links in a network to minimize the spread of

infections. *Computers & Operations Research* **69**(1) 10–24.

Nie, X., G. Parab, R. Batta, L. Lin. 2012. Simulation-based Selectee Lane queueing design for passenger checkpoint screening. *European Journal of Operational Research* **219**(1) 146–155.

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

Nikoofal, M. E., M. Gümüs. 2015. On the value of terrorist's private information in a government's defensive resource allocation problem. *IIE Transactions* **47**(6) 533–555.

Nikoofal, M. E., J. Zhuang. 2015. On the value of exposure and secrecy of defense system: First-mover advantage vs. robustness. *European Journal of Operational Research* **246**(1) 320–330.

Park, J.H., 2010. Structural change in US presidents' use of force. *American Journal of Political Science* **54**(3) 766–782

Paulson, E. C., I. Linkov, J. M. Keisler. 2016. A game theoretic model for resource allocation among countermeasures with multiple attributes. *European Journal of Operational Research* **252**(2) 610–622.

Peng, R., G. Levitin, M. Xie, S. H. Ng. 2011. Optimal defence of single object with imperfect false targets. *Journal of the Operational Research Society* **62**(1) 134–141.

Perea, F., J. Puerto. 2013. Revisiting a game theoretic framework for the robust railway network design against intentional attacks. *European Journal of Operational Research* **226**(2) 286–292.

Pinker, E. J., 2007. An analysis of short-term responses to threats of terrorism. *Management Science* **53**(6) 865–880.

Roy, A., J. A. Paul. 2013. Terrorism deterrence in a two country framework: strategic interactions between R&D, defense and pre-emption. *Annals of Operations Research* **211**(1) 399–432.

Sandler, T., Arce D.G. 2003. Terrorism & game theory. *Simulation & Gaming* **34**(3) 319–337.

Sandler, T., W. Enders. 2004. An economic perspective on transnational terrorism. *European Journal of Political Economy* **20**(2) 301–316.

Sandler, T., K. Siqueira. 2006. Global terrorism: deterrence versus pre-emption. *Canadian Journal of Economics* **39**(4) 1370–1387.

Sandler, T., K. Siqueira. 2009. Games and terrorism recent developments. *Simulation & Gaming* **40**(2) 164–192.

Schumaker, R. P., H. Chen. 2007. Leveraging Question Answer technology to address terrorism inquiry. *Decision Support Systems* **43**(4) 1419–1430.

Seidl, A., E. H. Kaplan, J. P. Caulkins, S. Wrzaczek, G. Feichtinger. 2016. Optimal control of a terror queue. *European Journal of Operational Research* **248**(1) 246–256.

Shan, X., J. Zhuang. 2013. Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender–attacker game. *European Journal of Operational Research* **228**(1) 262–272.

Shan, X., J. Zhuang. 2014. Subsidizing to disrupt a terrorism supply chain—a four-player game. *Journal of the Operational Research Society* **65**(7) 1108–1119.

Simchi-Levi, D. 2014. OM forum—OM research: From problem-driven to data-driven research. *Manufacturing & Service Operations Management* **16**(1) 2–10

Song, C., J. Zhuang. 2017. Two-stage security screening strategies in the face of strategic applicants, congestions and screening errors. *Annals of Operations Research* **258**(2), 237–262.

Starr, M. K., L. N. Van Wassenhove. 2014. Introduction to the Special Issue on Humanitarian Operations and Crisis Management. *Production and Operations Management* **23**(6) 925–937.

Sullivan, T. J., W. L. Perry. 2004. Identifying indicators of chemical, biological, radiological, and nuclear (CBRN) weapons development activity in sub-national terrorist groups. *Journal of the Operational Research Society* **55**(4) 361–374.

Sundararaghavan, P. S., A. Kunnathur, X. Fang. 2010. Sequencing questions to ferret out terrorists: Models and heuristics. *Omega* **38**(1-2) 12–19.

Szechtman, R., M. Kress, K. Lin, D. Cfir. 2008. Models of sensor operations for border surveillance. *Naval Research Logistics (NRL)* **55**(1) 27–41.

Taleb, N.N., 2007. The black swan: The impact of the highly improbable (Vol. 2). Random house.

The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States. 2011. Government Printing Office. Available online on https://9-11commission.gov/report/911Report.pdf (last visited on 9 January 2017)

Virta, J. L., S. H. Jacobson, J. E. Kobza. 2003. Analyzing the cost of screening selectee and non-selectee baggage. *Risk Analysis* **23**(5) 897–908.

Wallace, R. S. 2009. The Anatomy of A.L.I.C.E., Chapter 13 IN: Parsing the Turing Test pp. 181-210, Springer Science + Business Media B.V. 2009.

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

Wang, S., D. Banks. 2011. Network routing for insurgency: An adversarial risk analysis framework. *Naval Research Logistics (NRL)* **58**(6) 595–607.

Washburn, A., K. Wood. 1995. Two-person zero-sum games for network interdiction. *Operations Research* **43**(2) 243–251.

Weapons of Mass Destruction, Federal Bureau of Investigation (FBI), Available online on https://www.fbi.gov/investigate/wmd (last visited on 3 November 2016)

Xu, J., J. Zhuang. 2016. Modeling costly learning and counter-learning in a defender-attacker game with private defender information. *Annals of Operations Research* **236**(1) 271–289.

Yan, X., X. Nie. 2016. Optimal placement of multiple types of detectors under a small vessel attack threat to port security. *Transportation research part E: logistics and transportation review* **93** 71–94.

Zhang, C., J. E. Ramirez-Marquez. 2013. Protecting critical infrastructures against intentional attacks: a two-stage game with incomplete information. *IIE Transactions* **45**(3) 244–258.

Zhang, C., J. E. Ramirez-Marquez, J. Wang. 2015. Critical infrastructure protection using secrecy–A discrete simultaneous game. *European Journal of Operational Research* **242**(1) 212–221.

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

Zhuang, J., V. M. Bier, O. Alagoz. 2010. Modeling secrecy and deception in a multiple-period attacker–defender signaling game. *European Journal of Operational Research* **203**(2) 409–418.