Securing the Security System

Sabah Al-Fedaghi

Computer Engineering Department, Kuwait University, Kuwait
sabah@alfedaghi.com

Abstract

One of the main objectives of terrorist attacks on high-value structures (objects, or places selected as the aim of an attack) is to create headline-grabbing news. The more important the installation to be attacked, the more dramatic and widespread the news generated by the attack. The new phenomenon in such context is that the security systems of these significant structures have themselves become attractive targets that fulfill the requirement of being highly valued and newsworthy. The reason is that entry control on the perimeter of a security system (e.g., security checkpoint at an entrance) has no security barriers against attackers since it is the first line of defense. Accordingly, this paper concerns itself with the problem of terrorist acts in which the goal is not forced entry, but to attack the perimeter security system of a facility for the sake of heightened dramatic effect. This paper proposes reducing such effect by locating perimeter security posts some distance from significant targeted facilities. The purpose of creating distance is to disassociate a perimeter security system from its facility, to reduce the dramatic effect of any attack and thus demotivate potential terrorists.

Keywords: *security system, terrorism, perimeter attack, distancing entry control, security as a machine*

1. Introduction

“The new security era could be characterized as one of risk, complexity and uncertainty in comparison with the relative certainty of the preceding four decades” [1]. *Security* is typically described as the protection of persons and critical infrastructures or organizations against such *risks* as terrorism and organized crime. From a tighter perspective, Merriam-Webster dictionary [2] provides a “simple” definition of security: “the area in a place (such as an airport) where people are checked to make sure they are not carrying weapons or other illegal materials.”

Current indicators note an increase in global *terrorism risk* ratings, with 18 countries seeing an increase in their risk rating (2014, 2015, and 2016 scores) [3]. Terrorist attacks on critical infrastructure can succeed in shutting down or sabotaging important services, accessing sensitive data, and facilitating espionage [4]. The terrorists’ war “is a cruel war without rules” [1].

A facet in the study of terrorism phenomena is development of models that might be helpful in counterterrorism activities. For example, Gould [5] proposes a three-phase terrorism risk-management program:

1. Threat identification and initial site assessment
2. Detailed risk analysis
3. Risk management

An interesting aspect of this risk analysis is that Gould [5] places the highest risk at a facility’s entrance. According to Gomez [6], “As a security strategist, I teach that real security begins at the perimeter of the target location.” This is significant to our study, as will be discussed next.

Figure 1. The Entrance of an Important Facility has the Highest Risk (partial, re-drawn from Gould [5])

A main objective in attacking *structures of high economic or symbolic value* is to create sensational news, for publicity and for terroristic effect. The more important the target, the more dramatic and widespread the news generated by an attack.

1.1. Problem

According to Gomez [6], “The [recent terrorist] attacks are evidence that terrorist groups are returning to tried-and-true methods – *micro*-attacks with *macro*-effect. And they highlight an immediate need to *rethink security strategies*. Each successful attack will be emboldened to try more.” A new development in this context is that the *security system* of a targeted facility *becomes itself an attractive target* that fulfills the requirement of being highly valued and newsworthy. Hence, the problem under study in this paper concerns terrorist acts (most likely carried out by suicidal persons) in which the goal is not forced entry; rather, the objective is to *reach* the *perimeter* of the security system to inflict damage that maximizes the effect of the attack through a media frenzy that will report that the *significant target itself* has been exposed to terrorist violence.

This strategy achieves the following:

- First, a propagandistic agenda of headline-grabbing news related to valuable infrastructure. For example, following an attack on the security checkpoint at the entrance to Istanbul airport, news headlines screamed, “Istanbul Airport Explosions: 36 Dead, 147 Injured,” “Istanbul Airport Attack: 30 Charged Including Foreigners,” and “Istanbul Airport Terror Attack.” Clearly, the headlines would have been less dramatic if they had read, “Explosions Somewhere in Turkey: 36 Dead, 147 Injured,” “Attack Somewhere in Turkey: 30 Charged Including Foreigners,” or “Terror Attack Somewhere in Turkey.” The dramatic effect is greatly amplified by association with the mere name of the *targeted infrastructure* and what it symbolizes for the status and economic well-being of the country. The communicated message is, *We can violate your most cherished symbols of status and life.*

When a terrorist exploits the weaknesses of an airport and kills dozens, it strikes at the confidence of federal and local governments to keep us safe, in the one place they make a big show of doing so. The goal of terrorism is psychological, and airports have become the symbolic front line. [7]

- A typical secondary purpose of terrorism is to massacre people, since security checkpoints are places where people assemble to access protected infrastructure. The importance of this objective is to communicate the message, *Since we have reached a maximally protected place, you people are not safe anywhere in this country.* According to Jenkins [8], “terrorists want a lot of people watching, not a lot of people dead.”
- Less important is damage to the targeted infrastructure, where the message is, *If we can do this, then we can destroy any other establishment in this State.*

Such a deceptive attack on a highly valued facility would

- Ensure the spread of rumor, fear, and societal dysfunction.

- Expand the terrorists' support base and sympathizers through glamorizing the attack and showing that the government is ineffective in fulfilling its security function.

1.2. What is Special about Entry Control?

In general, *entry control* screens personnel, vehicles, and materials to identify unauthorized personnel and vehicles, and to detect explosives, weapons, etc. Control is not limited to the site boundary, but extends to all controlled areas of an organization or enterprise. Here, we focus on controlling entry of people at the boundary of an airport. A Security Screening Checkpoint (SSCP) [9] is a critical element in any infrastructure security system and here is intended to prevent and deter the transport of dangerous weapons in the airport and aboard aircraft.

Proper SSCP *design* helps avoid a host of problems for the airport and airlines, including terminal and queuing congestion, delays, and unnecessary security risks... *The location of the SSCP* relative to concessionaires and other airport services should be resolved early in the process through conversations with appropriate airport representative, as this will affect airport operations and critical revenue streams. [9] (Italics added).

Design considerations include [9] cost-effectiveness, prevention of SSCP exit lane breaches for entry into sterile areas, and *deterrence of potential adversaries*.

However, in attacking entry control on the perimeter of a security system,

- Even though a perimeter SSCP by itself is not the target, it is perceived to be the significant target; e.g., an attack *on the security checkpoint* at the entrance of an airport is viewed as an attack *on the airport*.
- An SSCP on the perimeter of a significant target (e.g., a security checkpoint at the entrance) has *no security* against approaching attackers since it is the system of the first line of defense.

The first security screens occur well after people show up — there is the entire arrival and check-in process to do before a single bag is checked. There's little to stop someone from showing up with a bomb in a suitcase or a firearm outside at that first checkpoint. With such an open layout and concentrations of potential victims, airports are tantalizing targets. [7]

1.3. Partial Solution?

According to van der Putten [10],

Convincing terrorists that acts of terrorism do not contribute to the *objective* that they are trying to achieve has a certain deterrent effect... The assessment of potential gains can be directly influenced by *reducing opportunities* to carry out harmful acts or the probability of success of such acts, or at any rate by generating the impression that success is less likely. (Italics added)

The solution to the problem should be to reduce the opportunity to attack the *facilities that attract the most sensational news and are the most difficult to penetrate*. According to Gomez [6], "Never forget ... the first rule of preventive counterterrorism should be 'prevent the terrorist from reaching his target.'"

However, it is *easy* to reach a physically unprotected boundary point such as a perimeter SSCP where the security system meets the outside. Proposals to enhance security such as enhancing technological and physical security measures and providing

more screening for people do not make a great difference at these points because the attack takes place before involving the actual security processing. “The problem today is that prevention [of terrorism] is not a technology problem. It's a capability problem” [6].

This paper proposes reducing the dramatic effect of such attacks by locating perimeter security posts some distance from targeted significant facilities. Distancing a perimeter security system would *disassociate* the perimeter of the security system from that facility in the public perception and thus *reduce the dramatic effect* of any attack, thereby creating a demotivating effect on terrorists.

1.4. Concern about Priority Consideration in the Paper

The pessimistic tone of the materials in the paper might be disturbing with its assumption that such attacks are inevitable, along with the focus on *reducing psychological effects* rather than on saving lives. But note that such priority is dictated by terrorists. Their first goal is to generate sensational news, whereas killing the largest number of innocent people is important only insofar as it contributes to the first goal. A terrorist attack in which at least 215 people were killed in Bagdad (July 4, 2016) generated a small fraction of the media attention given to 36 dead in the *Istanbul airport*. Accordingly, an effective security system should reflect such priority while assuming the imminence of the event as a fact in the current world. The focus of this paper does not mean that other factors are less important than reducing the psychological effects of dramatic news; it is intended as a small contribution to a particular aspect of a larger problem.

1.5. The Approach of This Paper

This paper utilizes the notion of *security as a machine* as proposed in Al-Fedaghi [11]. Such a model views a security environment in terms of flows of things and uses this flow to establish a system-based representation. The machine is an abstract apparatus of five states (stages) arranged in synchronic order: creation, release, transfer, receipt, and *process*. This description is suitable for the present purposes because it divides a security area into stages, and the type of attack discussed in the paper occurs before the security *process* stage is reached.

In order to provide a self-contained paper, a brief review of this abstract security machine based on a conceptual model [12-16] is provided in the next section.

2. Flowthings in an Abstract Security Machine

A secondary objective of this paper is to demonstrate that the *representation of phenomena* such as a security process plays a key role in making *thinking* visible through modeling of security-related events. Diagrams are needed at the level between “natural communication” (e.g., spoken language) and semiformal specification to provide a notation for events in the theater of operations. This paper utilizes a diagrammatic language that depicts *security as a machine* with five basic “operations”: creating, releasing, transferring, receiving, and processing of *things*. Such a language can play a central role in facilitating understanding among all security participants and as a first step toward developing and implementing security policies and implementation plans.

The abstract security machine is a diagrammatic schema that uses *flowthings* to represent a range of items, for example, passengers, luggage, signals, food, aircraft, data, and so on. Flowthings *flow* in the machine among basic stages where a flowthing can be created, released, transferred, processed, and received (see Fig. 1). Hereafter, flowthings may be referred to as *things* and an abstract security machine as a *machine*.

Figure 1. Machine

The machine is the conceptual structure used to change or transmit things as they pass through stages, from their inception or arrival to their de-creation or transmission. Machines form the organizational structure (blueprint) of any security system. These machines can be embedded in a network of assemblies called *spheres* (e.g., airport, terminal, SSCP) in which the machines operate. The stages in Fig. 1 can be described as follows:

Arrive: A passenger thing reaches a new machine, e.g., the SSCP.

Accepted: A thing is permitted to enter, or not (e.g., wrong credentials lead to rejection). If arriving things are always accepted, *Arrive* and *Accept* can be combined as a **Received** stage.

Processed (changed): A thing goes through some kind of transformation that changes it without creating a new thing (e.g., a traveler is processed at a passport checkpoint).

Released: A thing is marked as ready to be transferred outside the machine (e.g., a passenger is cleared to enter the boarding area).

Transferred: A thing is transported somewhere from/to outside the machine (from an airport to another airport).

Created: A new thing appears in a machine (e.g., a search exposes a weapon among the things flowing in the SSCP machine. If there is a camera in the SSCP, only a passenger appears in the view before the search, but after the search a weapon *appears* on the SSCP screen and has been effectively “created” in this system).

The machine shown in Fig. 1 is a generalization of the typical *input-process-output* model used in many scientific fields. The stages in this machine are mutually exclusive. An additional stage of *Storage* can also be added to any machine to represent the storage of things; however, storage is not an exclusive stage because there can be *stored processed* flowthings, *stored created* flowthings, etc.

The notion of *spheres and subspheres* refers to network environments (e.g., the SSCP machine is within the *sphere of the arrival terminal*). Multiple machines can exist in a sphere if needed. The machine is a subsphere that embodies the flow; it itself has no subspheres.

Triggering is the activation of a flow, denoted by a *dashed arrow*. It is a dependency among flows and parts of flows. A flow is said to be triggered if it is created or activated by another flow (e.g., the exit-flow from the SSCP triggers an in-flow of passengers waiting in queue). Triggering can also be used to initiate events such as starting up a machine (e.g., a manager’s signal triggers the opening of an additional SSCP to alleviate a long queue).

3. Example of a Security Machine: SSCP

A report by the USA Transportation Security Administration [9] includes a list of typical components of a checkpoint, along with sizes and space requirements and other considerations, where components are described as follows (see Fig. 2):

- A = Pre-screening Preparation Instruction Zone
- B = Queuing Space
- C = Divest Tables
- D = Walk-Through Metal Detector

E = Carry-on Baggage X-ray (TRX) Machine
F = Back Table
G = Searching Table
H = Passenger Containment

This “*conceptual* drawing underscores the point that all elements of the system, no matter how seemingly insignificant require an allocation of dedicated space” [9*TRANS-SE-AD*] (Italic added).

Figure 2. Typical diagram of elements that may be part of screening process in which passenger moves from non-sterile to sterile areas (partial, redrawn and modified from [9])

Clearly, the diagram is based on physical spaces and the locations of components of the SSCP. It is not a complete “conceptual” model of SSCP since it does not reflect the *required flows*. For example, an obvious requirement of any SSCP model is that a passenger *should* not bypass D; however, there is no indication in the diagram that a passenger cannot go directly from queue B to the sterile area, bypassing all other components. The representation is partial because the design is not based on the concept of *flow*, thus it violates the basic objective of the system: *Filtering the flow of passengers in an attempt to prevent undesirable occurrences*.

The design of the SSCP machine based on flow of things is shown in the preliminary diagram of Fig. 3. The traveler flows from the public area to the pre-processing area (circle 1) where he/she is processed and sent back (2) if certain credentials or conditions are not satisfied. Otherwise, the traveler joins the queue (3) and then proceeds to the SSCP entrance area (4). This area is not recognized as a separate component in the “conceptual drawing” of the Transportation Security Administration (Fig. 2).

There, in the SSCP entrance area (4), two new flows are generated: (i) the traveler him/herself (5 - body) and (ii) his/her possessions (6). The person (body) flows to the *walk-through metal detector* (7) where there is a possibility that he/she will have to go through the detector more than once (8). After finishing the metal detector process, the person goes to the exit area (9) or he/she may be searched individually in the passenger containment area (10), then go to the exit area (11).

Figure 3. Identified Flows in the SSCP

On the other hand, the possessions (6) flow to the front table (12) then through the X-ray (TRX) machine (13). When the possessions reach the back table (14), they may flow back (15) to X-ray (16). After finishing the X-ray process, the possessions go to the exit area (16) or they might be searched individually in the back table searching area (17), then go to the exit area (18).

Finally, at the exit area (16) the person and his/her possessions come together as the Traveler that flows to the sterile area (19).

Accordingly, the SSCP machine is completed by adding different stages, as shown in Fig. 4. Note how the traveler (circle 1 in the figure) and its subspheres body (2) and possessions (3) play their roles as flowthings. For simplicity's sake, the stages of the *Traveler* are not enclosed in a box.

In the public area (4), pre-processing area (5), queue (6), and entrance (7), the flowthing is the *traveler*, conceptualized as one flow unit, with its subspheres assumed to be included in the flow. In the entrance (7), the traveler generates two separate flows, each with its own flowthings: the body (8) and possessions (9). (In the online version of the paper, each flow is shown in a different color.) These two flows then reach the exit area (10) “united” again as the traveler (11) that flows to the sterile area (12).

The spatial and logical structure of the SSCP machine reflects the purpose of the SSCP as a screening filter, analogous to a filter used to purify flowing water. Of course, the design can be modified to allow “special paths” for working staff to bypass processing; nevertheless, the extended design specifies precisely these routes. Each stage and sphere in Fig. 4 can be supplemented with other flowthings such as constraints, rules, sensors, and cameras (which are actually subspheres with their own flow systems, e.g., a photograph is created, processed, released, received, and processed).

The machine representation seems to provide a conceptual tool for describing sequential events in the security area, as opposed to physical spatial descriptions such as the one given by the Transportation Security Administration (Fig. 2).

Figure 4. SSCP Machine

4. Protecting Checkpoints in the Perimeter of a Security System

“An action of violence is labeled ‘terrorist’ when its *psychological effects* are out of proportion to its purely physical result ... [and it] helps to spread fear, for if no one in particular is a target, no one can be safe” (from DiPaolo [17], who attributed it to Raymond Aron) (*Italics added*). The magnitude of *psychological effects* can be related to the “significance” of the *physical target* of the terrorist act, as in the case of an airport (in contrast to a post office), a nuclear plant (in contrast to a car factory), etc. From the aggressor’s point of view, the perceived “degree of reward” resulting from a successful attack is highly related to the type of physical target. The goal is to create wide publicity that reaches and psychologically affects the greatest number of people. Since an effective security system can detect and eliminate attackers, terrorists’ strategic objective is not entry into the facility; rather, it is to *create the news that the targeted facility has been attacked*. The public would conclude that since this valuable asset is not safe, then *anywhere else* is also not safe.

A strong security system that protects from intrusion, means an attack-proof target. However, psychological terror effects can be achieved by creating the news that the *perimeter* of the security system has been attacked when the public is under the impression that the security system is an integral part of the target, as shown in Fig. 5. Crippling a key part of a machine is viewed as crippling the whole machine. The point here is that, since the entry point is designed to allow the flow of things into the targeted installation, there is no warning of approaching danger as in the case of other perimeter points (e.g., fences, walls). Additionally, there is virtually no security barrier to prevent terrorists from merely *reaching* the perimeter security post.

Figure 5. Attack on Perimeter Security Post = Attack on Target

Accordingly, a new defense strategy should be developed for this type of attack, as proposed in Fig. 6. It involves reducing the association between a target and its perimeter security post as much as possible. Here the security post plays the role of a proxy (agent) that engages the attackers and disengages the target from the fallouts of battle.

Thus, for example, a news headline that reads “Attack on the Checkpoint Outside X Airport” is far less dramatic than “Attack on X Airport.” The dramatic effect of an attack is further reduced if the perimeter security post is shared by several significant targets, as for example in the news headline, “Attack on the Security Checkpoint for X Airport, Military Airport, and Aviation Ministry.” There would be no pictures on the Internet of damaged buildings with a broken sign for *X Airport*. Additionally, in the case of an actual attack, the normal operations of the significant target are not disturbed, especially if more than one perimeter security post is in operation.

Figure 6. Perimeter Security Post Dissociated from Target

According to a report by the USA Transportation Security Administration [9],

Vulnerabilities specific to a particular airport may affect the decision for *the location of a particular SSCP*. Some airports might choose to install a permanent security screening zone at or *near the entrance of the terminal*, making all interior spaces beyond that point sterile. The more common choice is to allow unscreened access further into the terminal, but may require that space and utility connections be available for temporary installation of SSCPs at the entry of the terminal during periods of elevated threats. *If the SSCP is implemented close to an entrance wall, thoughtful consideration must be given to passenger queuing to avoid creating a target by massing people in public areas.* [Italics added]

Our previous observation suggests that the *location* of the perimeter security post should be at some physical *distance* from the significant target, e.g., similar to the locations of toll stations at some distance from highways. The greater the distance between the security post and the significant target, the greater the disassociation between the two entities in public perception. Note that reducing the public dramatic effect of an attack is the only feature taken into consideration in this discussion. If reducing *human casualties* is a factor, the same strategy can be used by distancing the queue from the processing area of a security post. In this case the attackers have two attack options, as shown in Fig. 7.

Figure 7. Distancing the Queue from Processing in a Security Post

5. Distancing Security System inside Premises

The strategy of separating the perimeter of a security system from the target it protects is essential for reducing the dramatic effect of an event. For example, aircraft are actually on *the perimeter of the destination airport* when they bring in travelers from other airports. Suppose passengers arrive from an *untrustworthy airport*, but they must pass through a security post before being processed for passports. Note that terrorists can be assumed in many cases to be suicidal persons. They do not want to have to bypass a security check; rather they want to create sensational news by attacking the airport. Hence, when they *arrive*, they *want to be inside* the target.

The results of such an attack (Fig. 8) would be very damaging in terms of materials and infrastructure lost (e.g., fire spreading to other parts) and the dramatic psychological effect generated by headline-grabbing news. The objective of a terrorist is to double the dramatic effect by attacking the *destination country's facilities* with two outcomes: (i) a successful attack on the airport as a *significant target*, and (ii) a painful message to *the targeted country*. The *central aim* is control of the *airport* and the *country*, not of the plane or passengers. Otherwise, terrorists would carry out attacks in planes while in the air or on the ground.

Figure 8. Attack on perimeter security post inside airport

To minimize damage we apply the strategy of distancing the perimeter security post from the *inner* airport facilities. Accordingly, the airport is divided into *inner* area and *outer* area, as shown in Fig. 9. It would seem even better to call the inner area the *airport*, and the outer area the *runway field* to decrease the association between the two.

Note that the defense objective here is to minimize any psychological effect such as that created by videos of terrorized passengers running in panic inside an airport terminal. These pictures may also appear in the media, but the event could occur inside *an isolated minor building at the security checkpoint* while the airport's normal operations remain unaffected, especially if more than one perimeter security post has been established.

Figure 9. Attack on Perimeter Security Post in Outer Area of Airport

6. General Defense Model

In military terms, “defensive operations defeat an enemy attack, buy time, economize forces, or develop conditions favorable for offensive operation” [18]. Clearly, such defense operations are not related to the type of attack discussed in this paper; however, “The main purpose of the defense is to force or deceive the enemy into attacking under unfavorable circumstances... The defending commander seeks to dictate where the fight will occur, preparing the terrain and other conditions to his advantage” [18]. This insight seems applicable to our case, where the main purpose is to deprive the attackers of most if not all the fruits of initiating the attack. According to Stevens et al. in a RAND Corporation Report [19],

In meeting the terrorist threat, we find that the problem is how to influence the behavior of an unpredictable enemy... The solution is to shape the situation so that in any scenario the outcomes from the terrorist’s point of view will be unsatisfactory. The primary goal of this strategy is deterrence. Terrorists will see the airport as an unsatisfactory target that is not worth their effort.

It seems that a conceptual model is lacking that would provide a representation of the concept of *defense* in the sense described in this paper. A defense model is “meant to provide multiple layers of redundant defenses in order to delay and defuse an attacker away from their intended target” [6]. In our terminology, this means keeping the attacker at a distance.

A general conceptualization of such notion should involve the attacker and the defense (target). We assume that the defense has built a security system according to the distancing principle using a proxy SSCP as described previously. A general model of this type of attack is shown in Fig. 10, as follows:

- Recognition of the importance of the facility (circle 1)
- Collection of information about it (2)
- The above two phases trigger:
 - Preparation of the attack plan (3)
 - Evaluation of success of the plan (4)
 - Prediction of the expected effect of the attack (5)
- Depending on the anticipated effect and an evaluation of the probability of success, a decision is made (6)
- The attack is executed (7)
- The proxy receives the attack and absorbs (processes) it (8)
- The events themselves (8) and the level of association (9) of the proxy, together with the target (10) trigger the creation of an attack effect (11)
- The difference (12) between the actual effect and the anticipated effect influences the expected effect of any planning for a similar attack

“It might be crass to think of a violent attack in terms of a ‘return on investment,’ but terror cells certainly do” [7].

Figure 10. General Model of Defense using Distancing Strategy

The model is a general conceptual model for uniform specification of attack progression in various phases and its effect and influence on the next attack (not necessarily on the same target). The model provides a more exact description in which attack and defense-related “things” (e.g., information, plans, decisions, actions) are separated into different streams of flow incorporating basic operations: create, release, transfer, receive, and process. Such a model can provide the base for more elaborate analysis in the field of security and threat risks.

7. Conclusion

This paper considers terrorist acts in which the goal is *not forced entry* but, rather, to reach the *perimeter of a security system* (the first line of defense) to generate the dramatic effect of an attack on important or even critical infrastructure. The paper proposes that such an effect can be reduced by *distancing perimeter security posts from targeted facilities*. The purpose of such a move is security-related as well as psychological: to disassociate the perimeter of the security system from its *protected object or place* in order to reduce the dramatic effect of attack and thus demotivate terrorists. Here the problem has been represented in terms of the paradigm of security as machine. Various attack situations are represented by a high-level schematic representation that depicts the main aspects of defense: *distancing the delimiter of the security system from its threatened target*. The discussion seems to advance understanding of responses to diverse types of terrorist acts by developing models for use in defense planning. The result appears promising as a vehicle for modeling attacks and planning security. Further research would consider more complicated defense design cases.

References

- [1] J. van Bladel, “Security as a Holistic Idea and the Consequences for Central Asian States”, in A. H. Ebnöther, E. M. Felberbauer, and M. Malek (eds.), *Facing the Terrorist Challenge: Central Asia’s Role in Regional and International Co-Operation*, Vienna and Geneva (2005).
- [2] Merriam-Webster dictionary, Simple Definition of security. <http://www.merriam-webster.com/dictionary/security>
- [3] R. Akkoc, “Mapped: 2015 Was Europe’s Most Dangerous Year in a Decade for Terrorism”, *The Telegraph*, 12 April 2016. <http://www.telegraph.co.uk/news/2016/04/12/mapped-2015-was-europes-most-dangerous-year-in-a-decade-for-terr/>

- [4] K. Gordon and M. Dion, "Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security", Report of the Organisation for Economic Co-operation and Development (OECD), May 2008.
- [5] N. C. Gould, "Security, Managing Terrorism Risk, Catastrophe Risk Management", July 2004. <http://www.irmi.com/articles/expert-commentary/managing-terrorism-risk>
- [6] D. Gomez, "Time to Rethink Airport Security", Commentary, CNBC News, 23 Mar 2016. <http://www.cnbc.com/2016/03/23/>
- [7] J. Pappalardo, "Why Terrorists Attack Airports", 22 March 2016. Dallas Observer. <http://www.dallasobserver.com/news/why-terrorists-attack-airports-8147814>
- [8] B. M. Jenkins, The Potential for Nuclear Terrorism. RAND Corporation, Santa Monica, CA (1977), p. 8.
- [9] Transportation Security Administration (USA), Aviation Security: Security Checkpoint Layout Design // Reconfiguration Guide, 7 November 2006. http://www.google.com.kw/url?sa=t&rct=j&q=&esrc=s&source=web&cd=27&cad=rja&uact=8&ved=0ahUKEwih9bjk-LNAhUKcRQKHcYMA-U4FBAWCD8wBg&url=http%3A%2F%2Ffacina.org%2Fstatic%2Ftransit%2FCheckpoint_Layout_Design_Guide_v1r0-0.pdf&usq=AFQjCNHZFMNjwj3v6iOmrGPsuhKr2C1Z5w
- [10] F.-P. van der Putten, M. Meijnders, and J. Rood, "Deterrence as a Security Concept against Non-traditional Threats: In-depth Study", Netherlands Institute of International Relations, June 2015.
- [11] S. Al-Fedaghi, "Flow-based Physical Security", International Journal of Security and Its Applications, in press (2016).
- [12] S. Al-Fedaghi and M. Almutairy, "Applying Thing-Oriented Modeling and Patterns", International Journal of Software Engineering and Its Applications, vol. 10, no. 4 (2016), pp. 143-160.
- [13] S. Al-Fedaghi, "Systems Design: SysML vs. Flowthing Modeling", International Journal of Software Engineering and Its Applications, vol. 8, no. 1 (2014).
- [14] S. Al-Fedaghi and N. Aljallal, "Conceptual Schematization of Microcontroller and Assembly Language", International Journal of Software Engineering and Its Applications, vol. 8, no. 10 (2014), pp. 179-190.
- [15] S. Al-Fedaghi, "Toward Flow-based Semantics of Activities", International Journal of Software Engineering and Its Applications, vol. 7, no. 2 (2013), pp. 171-182.
- [16] S. Al-Fedaghi, "Flow-based Enterprise Process Modeling", International Journal of Database Theory and Application Compendex, vol. 6, no. 3 (2013), pp. 59-70.
- [17] P. J. DiPaolo, Motivations for Nuclear Terrorism in the United States, Master's Thesis, Naval Postgraduate School, Monterey, CA, June 1995.
- [18] GlobalSecurity.org, Military, Defensive Operations, chapter 5. <http://www.globalsecurity.org/military/library/policy/army/fm/3-21-21/chap5.htm>
- [19] D. Stevens, T. Schell, T. Hamilton, R. Mesic, M. S. Brown, E. Wei-Min Chan, M. Eisman, E. V. Larson, M. Schaffer, B. Newsome, J. Gibson, and E. Harris, "Infrastructure, Safety and Environment", RAND Corporation Report, 2004. http://www.rand.org/content/dam/rand/pubs/documented_briefings/2004/RAND_DB468-1.pdf