HAL
open science

A vulnerability assessment approach for hospital protection against terrorism attacks

Alain Guinet, Julien Fondrevelle, Daniele Baranzini, Susan Cook, Ahmad R Djalali, Roberto Faccincani

To cite this version:

Alain Guinet, Julien Fondrevelle, Daniele Baranzini, Susan Cook, Ahmad R Djalali, et al.. A vulnerability assessment approach for hospital protection against terrorism attacks. [Research Report] INSA Lyon. 2016. hal-02001875

HAL Id: hal-02001875

https://hal.science/hal-02001875v1

Submitted on 31 Jan 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A vulnerability assessment approach for hospital protection against terrorism attacks

Alain Guinet [a], Julien Fondrevelle [a], Daniele Baranzini [b], Susan Cook [c], Ahmad R. Djalali [d], Roberto Faccincani [b]
[a] INSA Lyon (Université de Lyon), DISP laboratory, 21 av. Jean Capelle, 69621 Villeurbanne, France, +33 472 437 994, alain.guinet@insa-lyon.fr, corresponding author.
[b] IRCCS San Raffaele, Via Olgettina, 60, Milano 20132, Italy.
[c] Hanover Associates, 44 Church Rd, Teddington TW11, United Kingdom.
[d] CRIMEDIM, Università del Piemonte Orientale, Via Solaroli, 17, Novara 28100, Italy.

Acknowledgement
This work has been done in the framework of the European project "THREATS" (Terrorist attacks on Hospital: Risk and Emergency Assessment, Tools and Systems) which is sponsored by the CIPS program of the European Community (http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/terrorism-and-other-risks/index_en.htm).

Abstract: Terrorism is a very sad reality for countries all over the world. Our society and its infrastructures are not prepared to face such threat. Most of buildings receiving people, are open spaces and can be easily attacked by terrorists, like in Paris on November 13, 2015. One of the vulnerable places is the hospital which is easily accessible by any people, in order to facilitate the health care. We propose a vulnerability assessment approach to increase the resilience of hospitals. Our quantitative approach first evaluates the likelihood of the threats taking into account on one hand the motivation and capabilities of terrorists, and on the other hand the accessibility of potential targets that the critical assets define. These latter are identified by building an IDEFØ model of the hospital patient flows. Second, the impacts of terrorist scenarios on the critical assets, are evaluated by a linear program which is a direct translation of the IDEFØ model to a flow model. The impacts of the worst scenarios are reduced, by proposing effective counter-measures which are evaluated by this flow model.

Keywords: Vulnerability assessment, Hospital, Protection, IDEFØ modeling, Linear programming.

1. Introduction
Around hundred terrorist attacks against hospitals have been counted all over the world in 43 countries during these last 33 years (Ganor and Halperin Wernly 2013). Hospitals are an attractive target for terrorists because an attack will produce a large number of causalities due to the large number of patients, relatives and employees. Furthermore, an attack will receive wide media coverage and it will distress most of the inhabitants. The terrorist attacks are perpetrated by bombs, armed assaults, dispersion of biological agents, chemical agents, radiological agents… In the past, they took place: in the United Kingdom (Musgrave Park British Army Hospital in 1991) where it caused 2 deaths and 11 injured people, in Rwanda (Kigali main hospital in 1994) where 100 persons died, in Russia (Budennovsk hospital in 1995) where it caused 129 deaths and 415 injured people, in Iraq (Tikrit Hospital in 2011)

where 11 people were killed and 30 people were injured, and recently on 8 march 2017 at least 30 people were killed in the army hospital of Kabul.

As many public places (e.g., Universities, Town-halls, shopping centers) hospitals are open spaces. Patients, employees, and relatives can access a lot of care units without control and can be in contact with many people. Terrorists can have a good perception of the care system and most of the time the protective measures are apparent. The most crowded places are often the most vulnerable areas where terrorist attacks can be the most damageable, regarding the ease of access and the potential damages.

To protect hospital against terrorist attacks, the weak points of the infrastructures, of the care organizations, of the employee practices, must be studied and counter-measures must be proposed. As hospitals are complex and heavy human organizations, a vulnerability assessment method based on quantitative tools should be proposed. Our contribution is structured as follows. In section 2, we refer to the previous works on vulnerability assessment, no matter the activity area. In section 3, we propose an approach to analyze and assess the vulnerability of hospitals against terrorist attacks based on the identification and evaluation of: critical assets, threat sources, critical asset attractiveness, terrorist attack scenarios, and counter-measure solutions. A modeling tool is suggested in order to identify critical assets in section 4.1, and an evaluation tool for scenario risk analysis is proposed in section 4.2. For confidentiality reasons, no section dedicated to an example is developed, but some illustrations are given mainly in the section devoted to the presentation of our approach.

2. Previous works on vulnerability assessment

Studies about risk assessment are numerous on the last ten years. They propose qualitative techniques, quantitative techniques, and hybrid techniques (both qualitative and quantitative), to analyze and assess risk situations. A survey of the main works in order to analyze and classify risk analysis and assessment methods has been published by Marhavilas, Koulouriotis and Gemeni (2011). The authors consider the risk as a measure under uncertainty of the consequences of a hazard. Regarding methods, they conclude that: there is a plethora of technical papers which are dedicated to transportation, chemical processes, construction, maintenance, etc.; the quantitative methods are widely used; the industry is the main user of the analysis and assessment methods.

Fewer works have been published on vulnerability assessment, because the vulnerability refers more to external risks than to internal risks, and the environment is less predictable than the organization of industries. The vulnerability assessment can be seen as an extension of risk assessment for reduction of the external events' consequences on the structure of a production system, whatever could be the system: manufacturing, transportation or care system (Birkmann et al. 2014). More synthetically, the authors propose that the vulnerability of a system exposed to hazard determines whether it translates into disaster.

The processes to assess risks or vulnerabilities have common tasks. Both try to identify critical components/critical assets, to identify events or threats, to generate scenarios, to analyze their frequencies and consequences, to calculate a risk measure which combines the likelihood and the severity of the scenario (Shahid 2009; Bajpai and Gupta 2005). Vulnerability assessment finalizes the investigation process with an analysis of counter-measures and security measures in order to reduce the system vulnerability in terms of

infrastructure, human lives, environment and activity protection. Vulnerability Assessment identifies the weaknesses of the system which can be exploited by adversaries. It reduces these latter, by proposing mitigation, preparation, response and restoration solutions.

Regarding the external events, they can be from natural origins (flood, earthquake, etc.) or from human origins (pollution, crime, terrorist attack, etc.). The criteria to evaluate the consequences of such events are multiple and concern human lives, infrastructure damages, environmental impacts, loss of economic activities, etc. A weighted risk analysis is required (Shahid 2009), possibly with an AHP approach if the damages cannot be all expressed in monetary values (Saaty 1980).

Regarding the likelihood of the external events particularly for terrorism, it is quite difficult to find historical data about terrorist events, because terrorist attacks mainly occur in countries at war. 103 terrorist attacks against hospitals have been perpetrated worldwide (Ganor and Halperin Wernly 2013) from 1981 to 2013. For France, one of the most affected members of the European Union, no terrorist attacks have been perpetrated against hospitals, but 56 terrorist attacks have been committed against administrative or public services (e.g., police stations, schools) for the period from 1975 to 2006 (De Villepin 2005) . But for 2015, the statistics of Europol (2016) specify that 73 terrorist attacks have been perpetrated in France. According to the Institute for Economics and Peace (IEP 2016), the last terrorist index for France is equal to 5.603/10. As terrorist attacks still remain very rare events, data are most of the time very poor and scattered, so a likelihood measure based on the frequency of past occurrences of such events would be inadequate (Stewart 2010). Some authors propose to consider the ease of causing threats by potential adversaries, to better evaluate the likelihood of terrorist attacks (OWASP 2016; Ben Othmane 2015; Wheeler 2011). The ease of causing threats, is based on motivations and capabilities of attackers, and can vary with the attractiveness and the ease of access to the target. As very few detailed statistics are available for terrorist attacks against hospitals, we propose to consider such criteria.
As specified in the review of Marhavilas, Koulouriotis and Gemeni (2011), the chemical industries investigate a lot the field of risk analysis and assessment. The American Petroleum Institute (API) and the National Petrochemical & Refiners Association (NPRA), have developed a Security Vulnerability Assessment methodology (SVA), in 2003, for the petroleum and petrochemical industry (Moore 2006). The SVA methodology helps managers to identify, analyze and manage the physical security vulnerabilities of an industry. The four step approach of the SVA methodology is dedicated to the process of risk analysis and assessment, for vulnerability and security studies. It defines a qualitative method.

We inspire from the weighted risk analysis method (Shahid 2009) and the SVA methodology (Moore 2006) in order to define a vulnerability assessment method for hospital protection. Both are based on scenarios and they consist of 3 components: scenario identification, evaluation of the scenario likelihood and scenario consequences. Our approach will be quantitative oriented, considering the integrated decision making tools. As hospital is an open space whose infrastructure is implemented on several buildings, we support our method with a modeling tool and an evaluation tool, based respectively on IDEFØ and Linear Programming. The choice of IDEFØ method has been approved by several authors in the field of risk management (Shimada and Gabbar 2008; Carnaghan 2006). IDEFØ models define a suitable base for system reengineering (Bevilacqua 2012). The use of a linear program which represents the IDEFØ flows, is a logical continuation. In the next sections, we

present our vulnerability assessment approach, and we detail the contribution of IDEFØ and Linear Programming to support our contribution.

3. A vulnerability assessment approach against terrorist attacks

Our vulnerability assessment approach is composed of 5 steps:

1. Define critical assets: Brainstorming on the care units and on the technical units of the hospital, we define and locate the critical assets i.e. the units which are the most likely and the easiest to be exposed to an adversary's threat and which are the most damageable regarding to patients, employees, and the added value, etc. An IDEFØ model enables us to locate these critical assets.
2. Find threat sources: Reviewing historical data on terrorist attacks, we specify the terrorist profile, their potential actions, their capabilities, their motivations, and the threat history.
3. Calculate critical asset attractiveness: Perform an analysis based on pairing of each critical asset and each threat source, in order to identify potential vulnerabilities per adversary, and to better evaluate the ease of causing threats per adversary.
4. Define Threat Scenarios: Based on the attractiveness of the critical assets, the most likely (i.e. the easiest target for the most motivated adversary) scenarios with the worst consequences are constructed, specifying: the terrorist profile, the terrorist action, the hazard release, the type of damages, and the security/safety barriers.
5. Assess Threat Scenarios: scenarios are simulated to evaluate their consequences, to study possible counter-measures implementation in order to reduce the risk to an acceptable level. The last two steps are repeated until all relevant scenarios are mitigated.

3.1 Critical Assets

To identify the critical assets, we suggest a brainstorming on hospital areas/functions (care or technical units) by physicians, nurses and engineers, which are more likely to be exposed to a terrorist threat and which have more impacts on the hospital activity. This brainstorming is supported by a "as-is" model of the hospital which maps the potential critical assets and their environment. An IDEFØ model is used for the critical asset identification and location.

To evaluate the criticality of the hospital area/function (called critical asset), the criteria below can be selected: the number of people involved (P), the added value (remuneration of economic activity or chargeback) to hospital (V), and the ease of access i.e. the context (C). The asset severity ranking will be measured through a weighted sum and be equal to $Ar = a1 * P + a2 * V + a3 * C$ with $a1 + a2 + a3 = 1$. The criteria P, V and C will be set from 1 (very low) to 5 (very high). The Analytical Hierarchy Process (AHP) method could be used, in particular to determine the criteria weights ai (Saaty 1980). Table 1 shows some critical assets of the hospital.

Critical asset	Criticality/Hazards	Ease of Access	Asset severity Ranking: Ar
Emergency department	The emergency department (ED) treats acute patients and then dispatches them to medical and surgical units. It is one of the main entrances to hospital. The emergency department is the main actor for sustaining emergency management plans.	The emergency department is accessed by any people, directly from outside.	5

Intensive Care Unit	The Intensive care units (ICU) treat acute patients from ED and elected patients from operating theaters. They define bottlenecks on the patients' pathways. They use high technology and expensive medical equipment. They are located in several hospital areas.	The main resource used by ICU, is medical gaz. It is stored outside because it is inflammable.	4
Etc.			

Table 1: the Critical Assets

3.2 Threat Sources

To define the threat sources, we review the historical data on terrorist attacks (including criminality which could acts as a henchman to launch cyber-attacks for example), and their dynamics. The attacks can occur in similar contexts (same nation, same sector, same social context…) or can occur in different contexts (country at war or not, private/public sector…).

Adversary type	Threat History	Potential actions	Adversary capability	Adversary motivation	Threat ranking: Tr
International terrorists	Missionary hospital, Jibla, Yemen, December 30 2002; The Tikrit Hospital Attack, Iraq, 2011; Christian worship center and hospital, Nwokyo, Nigeria, April 15 2014; Christian hospital, Kabul, Afghanistan, April 24 2014 (Ganor and Halperin Wernly 2013).	Armed assault; Hostage/Kidnapping; Bombing and damage/destruction of equipment and buildings; destruction of human life; Release of nuclear or biological or chemical materials; Contamination of humans, equipment, buildings.	High level of organizational support; Good financial backing; Network of members; Highly developed communication capabilities; Weapons and explosives.	Adversary is highly motivated (extremist); prepared to die for their cause; Intent to cause maximum damage to hospital assets including loss of lives and economic disruption.	5
Etc.					

Table 2: the Threat Sources

To evaluate the adversary hazardousness, we propose to use the following criteria: the financial means (F), the knowledge of the system (K), the technology expertise (E), the level of motivation (M). The threat ranking will be also measured through a weighted sum and be equal to $Tr = b1 * F + b2 * K + b3 * E + b4 * M$ with $b1 + b2 + b3 + b4 = 1$ and $F, K, E, M \in \{1, 2, 3, 4, 5\}$. The AHP method could also be used to calculate the weights of the threat ranking.

Table 2 presents per terrorist profile, their threat history (context, i.e. location and date of attacks), their potential actions, their capabilities, their motivations, and the threat ranking Tr. If available, the threat history could be used to estimate the frequency of the threat occurrence.

3.3 Critical Assets Attractiveness as likelihood

We can now evaluate the attractiveness of the critical assets per adversary (i.e. the ease of causing a threat), i.e. we specify the objective of a potential attack and the Attractiveness Ranking. The attractiveness ranking Lr is function of the criticality of a critical asset and of the adversary hazardousness, It can be expressed as the product of the previous rankings on the interval from 1 to 5, i.e. Lr = (Tr*Ar)/5. The higher the attractiveness will be, the more important the likelihood of an attack on this critical asset will be. The attractiveness combines the motivation and capabilities of the adversary and the criticality and ease of access of the target.

3.4 Threat Scenarios

Knowing the critical assets attractiveness, we can brainstorm on scenarios of terrorist attacks: the most likely scenarios with the worst consequences are constructed, by specifying the terrorist profile, a potential terrorist action, the hazard release, the type of damage, and the existing security/safety barriers. Regarding security/safety barriers, only the existing counter-measures of the hospital are considered. In the next step, some new counter-measures will be proposed.

3.5 Scenario assessment

As a set of 7 terrorist scenarios has been developed (bombing attack in Emergency Department, gun attack against a VIP in Operating Rooms, electricity grid failure, medical gas tanks destruction, SARS threat, Anthrax threat, CESIUM 137 threat), on one hand some risk assessment knowledge is required to evaluate the resulting impact of the scenario events, as objectively as possible, and on the other hand some vulnerability assessment knowledge is needed to understand, to reduce, and to eliminate the resulting impact of adverse events. This step is supported by a linear model which represents the flow propagation into the hospital (e.g., traffic, contamination, evacuation). The linear flow model is solved with the IBM ILOG Cplex solver (2015).

3.51 Risk assessment

The objective of the risk assessment is to calculate the risk of the different scenarios. Our risk assessment approach applied to scenario estimations is based on best practices in hazard matrix applications. Nevertheless an innovation has taken advantage on the one hand of the criteria (adversary capabilities, adversary motivations, criticality of assets, ease of asset access, human losses, infrastructure damages, operational damages, and image damages) used for estimating the likelihood and severity criteria and on the other hand of the quantitative evaluation tool used (the linear flow model). Each terrorist scenario is fully developed, its likelihood (ease of causing a threat, and adversary motivation) as well as its severity (losses and damages) are estimated systematically and deeply. The combination of likelihood and severity shall provide an index representing the best combination of both criteria. The following Threat Risk Matrix in Table 3 below has been developed. The matrix shows how the risk index shall be calculated on the terrorist scenarios.

Scenario	Description	Likelihood: Lr	Human Losses	Infrastructure Damage	Operational Damage	Image Damage	Severity: Sr
1	Bombing attack in Emergency Dpt.	5	2	2	4	5	3.25
2	Gun attack in O.R. against VIP	2.4	2	1	2	4	2.25

3	Medical gas tank destruction	3.2	2	3	4	3	3
4	SARS Threat	5	5	1	5	5	4
Etc.							

Table 3: The Threat Risk Matrix

The infrastructure damage index is set to: 1 for a single day breakdown for one building, 2 for several days breakdown for one building, 3 for several days breakdown for several buildings, 4 for the activity cessation for one building, and 5 for the activity cessation for several buildings.

The Human losses are set to: 1 for 1 killed, 2 for less than 5 killed, 3 between 5 and 15 killed, 4 between 16 and 50 killed, and 5 for more than 50 killed.

The operational damages are set to: 1 for a single service interrupted during one day, 2 for a single service interrupted during several days, 3 for several services interrupted during one day, 4 for several services interrupted during several days, 5 for most services interrupted during several days.

The image damages are based on the reduction of incoming patients after attack. They are set to: 1 for 1% reduction, 2 between 2% and 5% reduction, 3 between 6% and 10% reduction, 4 between 11% and 30% reduction, 5 for more than 30% reduction.

In general the risk model assumed for the matrix in Table 3 above, is the risk of terrorist attack modeled by formula: R = Lr x Sr, where the risk R is the product of the likelihood Lr (i.e., the ease of causing a threat per critical asset, ranking from 1 to 5) and the severity of the hazard Sr (i.e., the impact of the terrorist attack as weighted linear combination of four different severity criteria). In the example presented in Table 3, each severity criterion is supposed to have the same weight so the severity (last column) is calculated as the average of the 4 previous values.

3.52 Vulnerability assessment

The objective of the vulnerability assessment is to reduce the risk of the different scenarios, by defining: counter-measures, emergency management plans, and safety practices, etc. Most of the researchers agree on the following four phases to reduce the impact of a disaster (as the result of a terrorist attack): mitigation, preparedness, response, and recovery (Altay and Green 2006). Mitigation and preparedness are the pre-disaster activities, and response and recovery are the post-disaster activities. The mitigation phase serves the purpose to minimize the potential number of casualties and reduce the potential losses of property, by acting before that the disaster occurs. The preparedness gets that all relevant stakeholders are ready for the disaster, specifying emergency management plans, and training people according to these latter. The response includes the arrangement of resources and working procedures, according to the emergency management plans to protect the life, property, and environment. The main objective of the recovery phase is to restore activity and reconstruct the resources after the disaster.

The vulnerability assessment investigates on: the implementation of human, physical and information counter-measures at the mitigation level, the use of emergency management plans and the resource dimensioning at the preparedness level, the decision support during the response phase and the recovery measures. For example, an access control can increase the

difficulty for an adversary to access a critical asset, and decreases the likelihood of the threat. Or, a biological sensor can reduce the human losses, detecting a human contamination earlier (for instance the detection of Anthrax spores). Emergency management plans organize the use of human, physical and information resources to face the disaster in order to minimize the human losses and the damages. They coordinate the stakeholders; they provide behavior procedures for each actor; etc. All these counter-measures, emergency management plans, and safety practices, can be evaluated by our linear flow model. Comparing the 'as-is' configuration with the 'to-be' configuration, a cost-benefit analysis can be made in order to choose the best security and safety barriers and reduce the risk impact to an acceptable level.

4. Decision making tools

4.1 IDEF0

IDEFØ (1993) is a method designed to model the events, data, and activities of an organization or a system. IDEFØ is derived from the graphical language: Structured Analysis and Design Technique called SADT (Ross 1977). The IDEFØ model helps to organize the analysis of a system and allows promoting good communication between the analysts and the users. It enhances user involvement and allows us to obtain consensus models (Bevilacqua 2012), which is a basic requirement when actors are multidisciplinary such as physicians, nurses, technicians, engineers, administrative staff, managers, etc. The analysis of the system is represented as a collection of hierarchically organized diagrams with a limited number of elements: boxes which represent activities and arrows to model physical, information, order flows, etc.

IDEFØ will assist us in identifying care units and services accesses and the propagations of flows (e.g., staff, patients and relatives). An IDEFØ model will be created for our hospital analysis and it will be used first to identify the critical care or technical unit accesses, and second to generate a dynamic model in order to evaluate a scenario by calculating the patients' traffic, or the contaminated patients crossing an infected area, etc. The analysis viewpoint follows the patient's way.

The hospital, which is chosen as our case study, covers an area of about 300 thousand square meters and is composed of 11 buildings which accommodate 49 specialty clinics and over 6000 employees. Each care unit uses dedicated processes. An analysis of the 49 processes and of their interactions cannot be done exhaustively, and without a global approach which allows to focus on a limited number of care units. A first decomposition of the hospital per building and later of the buildings per floor has been carried out (Figure 1), it allows us to follow the patient's ways in the hospital. A second decomposition of some care units located at the leaves of the previous tree has been done (Figure 2), it represents the patient's care processes related to critical assets (e.g., the Emergency Department, the Operating Theatre, the Intensive Care Units).

Regarding the decomposition that is used, the boxes and the arrows have different meanings for the critical asset analysis. For the patient pathway decomposition, a set of buildings, a building or a floor of a building is modeled by a box. The control data (arriving on the top of the box) and the output data (leaving the box on the right side), allow us to represent the patient flows. No input data (arriving on the left side of the box) is used. External data (with an external origin or an external destination) or internal data (with an internal origin and an internal destination) have also different meanings. External control data specify patients

entrances from outside of the diagram i.e. from another building or from outside the hospital. External outputs represent exits from a building or from the hospital. Internal data (controls and outputs) specify the patients flows in the building (accesses between the different floors) or the flows between a set of buildings (i.e. by an internal tunnel). The mechanism arrows (arriving on the bottom of the box) are dedicated to define the building or the building floor where a box is located in order to specify the horizontal dimension (i.e. accesses by tunnel or connecting corridor) and the vertical dimension (i.e. accesses by stairways or lifts). Such details are quite important to extract the access matrix required to construct the dynamic model (see Section 4.2). For the by-process decomposition, an activity is modeled by a box. The control data and the input data represent the patients entrances. Control data show the flow which triggers the activity. Output data specify activity results i.e. mainly patients exits. Mechanism data are resources required by the activity.

First a building of the hospital (Figure 1) is shown to illustrate patient pathway decomposition. Second the care process of a critical unit identified in this building is illustrated on Figure 2.

The IDEFØ model allows us to locate the care units in the hospital. It defines a hierarchical map and presents an environmental view of the infrastructures, of a building, and of a care unit, thanks to the patient pathway decomposition. The details of care units are given via the by-process decomposition: the activities, the patient flows and the resources are modeled. The IDEFØ diagrams enable us to understand the environment of care units or technical units in order to appreciate their weak points regarding the patient accesses, the available resources, the absence or presence of countermeasure activities… This is a very suitable base, firstly, for the identification of the critical assets, and secondly, for the system reengineering in the framework of counter-measures implementation (Bevilacqua 2012).

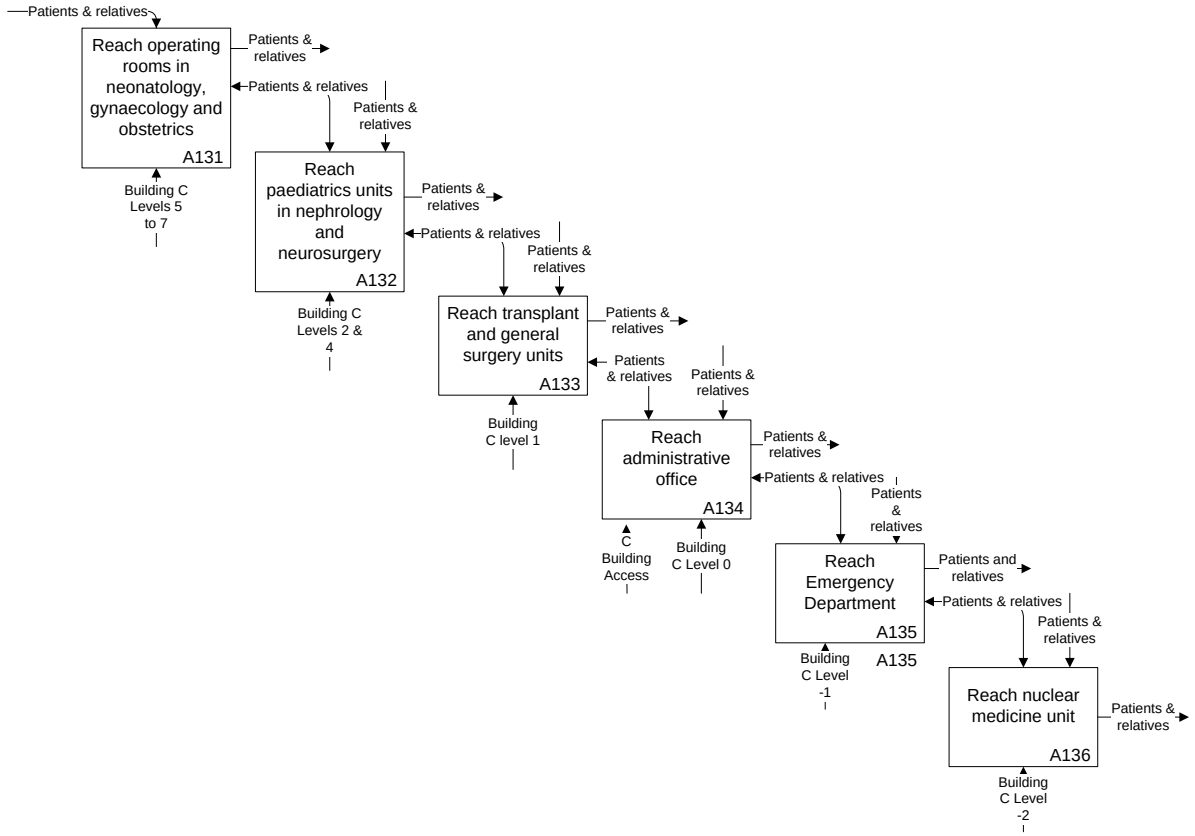

Figure 1: One of the 11 buildings of the Hospital

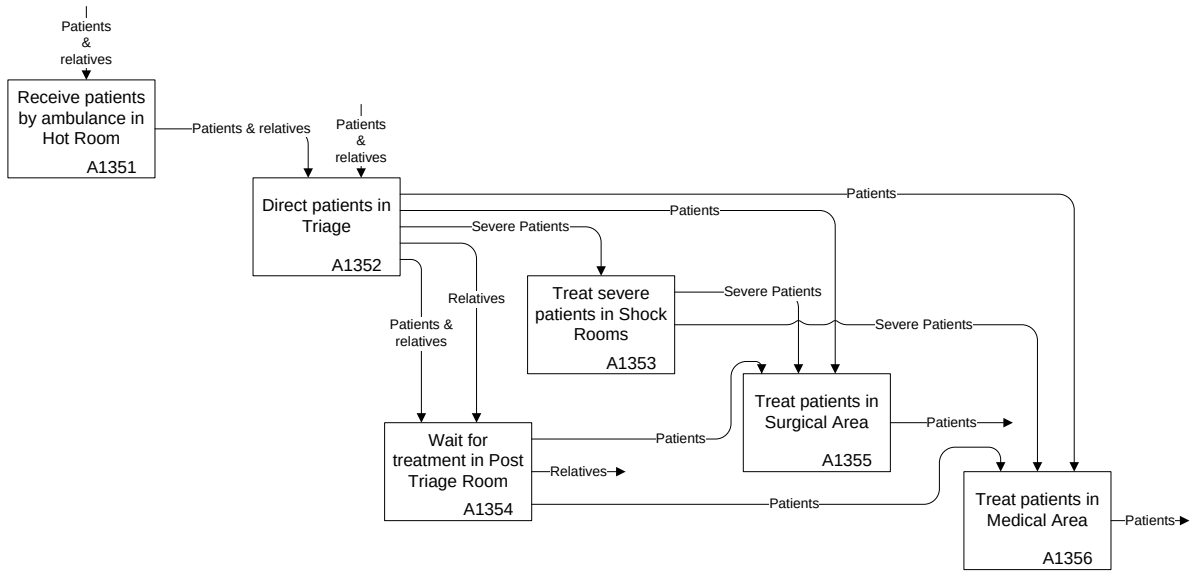

Figure 2: The Emergency Department

The use of IDEFØ language defines a very useful tool to obtain a hierarchical and synthetic map of the hospital following the patient pathway decomposition. The accesses between care units are clearly represented and locations of care units are well shown. These pictures are user-friendly and will allow us to specify a graph where vertices are the care units and arrows are their patient accesses. For the process descriptions of the care units, IDEFØ defines a powerful tool to specify: the sequence of activities, the patient flows between these latter, and the required resources. Instead of using different languages, we obtain a multiple-

decomposition model which enables us a unified and coherent description of the accesses and the care unit processes of the hospital with the same tool.

4.2 Linear Programming

The patient pathway decomposition of the hospital model is composed of 12 diagrams of care units and services. The decomposition tree is of 4 levels and has 47 leaves which represent 47 services/units or sets of them. 199 direct accesses between sets of services/units have been modeled. 9 other diagrams of activities allow us to model the processes of the Emergency Department, the Operating Theatre, the ICU, etc., which define critical assets regarding to terrorist attacks. The patient pathway decomposition shows a static picture of the hospital. In order to study the dynamic of the hospital by simulating terrorist attacks, a simulation tool has been designed which requires a limited number of parameters (care unit admissions and care unit discharges). To evaluate the different scenarios of terrorist attacks, we study the patient traffic in the hospital. First we export from our IDEFØ model the different accesses between the leaves (services/units) of the decomposition tree of the patient pathway analysis. The result is modeled by a binary matrix where the lines/columns represent the leaves, and the intersections between lines and columns identify the presence (1) or absence (0) of a direct access. Such a binary matrix can be used to calculate a vulnerability criterion based on the crowding of places (Miniati and Iasio 2012). This matrix is converted to a graph and a multi-period flow problem is studied on this graph. In valuating on one hand the patient inputs to the hospital and on the other hand the care units admissions which are both located at the leaves of the IDEFØ model, the hospital entrance flows can be studied. In defining on one hand the patient exits of the hospital and on the other hand the care units discharges which are both located at the leaves of the IDEFØ model, the hospital departure flows can also be studied. These two flow problems have been modeled by a linear program. The IBM ILOG Cplex solver (2015) has been chosen to solve it. In the next subsection, the linear model is presented and in the following subsections, the benefits of this model are discussed.

4.21 The flow model

Parameters:

- N: Number of services/units (number of leaves of IDEFØ's tree, N is equal to 47);
- T: Number of periods (120 hours i.e. 5 days, or more);
- i, j, k, p, q: Indices;
- H: Length of stay for inpatients;
- L: Length of stay for outpatients;
- Acc(i,j): If there is an access to go directly from unit i to unit j, it is equal to 1, 0 otherwise; The accesses are extracted from the IDEFØ's model;
- Input(i,p): Number of people (inpatients, outpatients, and relatives) incoming in i directly from outside (entry point) on period p;
- Output(i,p): Number of people (inpatients, outpatients, and relatives) exiting from i directly to outside (exit point) on period p;
- Inp(i,p): number of inpatients (patients which stay at least one night in the hospital) on period p at service/unit i;
- Outp(i,p): number of outpatients (patients which stay less than one night in the hospital) on period p at service/unit i.

Variables:

- XG(i,j,p): Number of people going from i to j on period p;
- XR(i,j,p): Number of people returning from i to j on period p.

Model:

$$Minimize\ Z = \sum_{p=1}^{T}(\sum_{i=1}^{N}\sum_{j=1}^{N}(XG(i,j,p) + XR(i,j,p))) \quad (1)$$

Subject to:

$$\sum_{j=1\,|\,j\neq i}^{N} XG(j,i,p) * Acc(j,i) - \sum_{j=1\,|\,j\neq i}^{N} XG(i,j,p) * Acc(i,j) + Input(i,p)$$

$$= Inp(i,p) + Outp(i,p) \quad i = 1,\dots,N \quad p = 1,\dots,T \quad (2)$$

$$\sum_{j=1\,|\,j\neq i}^{N} XR(i,j,p) * Acc(i,j) - \sum_{j=1\,|\,j\neq i}^{N} XR(j,i,p) * Acc(j,i) + Output(i,p)$$

$$= Inp(i,p-H) + Outp(i,p-L) \quad i = 1,\dots,N \quad p = 1,\dots,T \quad (3)$$

$$XG(i,j,p) \in R^{+}, \qquad XR(i,j,p) \in R^{+}, \quad i,j = 1,\dots,N \quad p = 1,\dots,T \quad (4)$$

Comments:

This linear program minimizes the traffic of the whole hospital over the whole horizon (equation 1). In equations 2, the flow entrances from neighboring units, minus the flow exits to neighboring units, plus the entrances to i from outside ("Input" data represent the inpatients and the outpatients, relatives are considered as outpatients), are equal to the inpatient absorption by care unit i (the inpatient admissions are modeled by "Inp" data), plus the outpatient absorption by care unit i (the outpatient admissions are modeled by "Outp" data). Equations 2 are conservation flow constraints, they model the entrances of care unit i. Equations 3 are the opposite equations, they model the departures from care unit i. In equations 3, the flow exits to neighboring units, minus the flow entrances from neighboring units, plus the exits from i to outside (the inpatient exits and the outpatient exits are regrouped within the "Output" data), are equal to the previous absorption of the care unit i for inpatients who are now released ("Inp" data represent the previous admissions of inpatients who entered H periods before p, according to the length of stay equal to H), plus the previous absorption for outpatients who are now released ("Outp" data represent the previous admissions for outpatients who entered L periods before p, according to the length of stay equal to L). The values of Inp and Outp data for periods prior to 1 can be used to model the hospital occupancy.

The dynamic model of the hospital represents 47 units or services modeled by IDEFØ boxes located at the leaves of the decomposition tree. Solving the multi-period traffic problem for 120 periods which represent 5 days of 24 hours leads to 560 161 decision variables and 11 286 constraints. The linear program has been solved with IBM ILOG Cplex (2015), the computation time is around 1 minute and the weekly hospital traffic is equal to 47 182 crossings of patients and relatives over the whole horizon. The most crowded place has a maximum traffic per hour of 336 patients and relatives, considering a direct patient access to care units. It can define the most vulnerable place.

Our linear program is a dynamic model of the patient pathway decomposition drawn from the IDEFØ model. Some critical care units have been described following a by-process decomposition (see Figure 2, for the Emergency Department). Their diagrams allow us to define a sub-matrix of activity successions for each care unit whose activities have been modeled. The description of care units leads us to extend our patient flow model by integrating the linear subprograms of the flows in these care units. Each linear subprogram represents the activity sequence, the flows through activities, and the resource capacity constraints dedicated to these activities. The linear sub-models try to maximize the care unit throughput.

4.22 Results

We use a CBRN (Chemical Biological Radiological and Nuclear) agent attack scenario as a hazardous example to show how our flow model helps the decision maker to evaluate the risk severity. For this scenario, the propagation of a CBRN agent in the hospital is simulated with our flow model.

The scenario is described as follows: A European citizen affiliated to an international terrorist organization is a medical doctor with a background in virology. He/she pretends to be funded by a famous pharmaceutical company, and approaches the Chief executive of the hospital for a PhD in virology. He/she has been affected to the P3 laboratory (laboratory working with microbes which can cause serious and potentially fatal disease via inhalation route) and works there for a while. He/she has access to the P3 laboratory and to the repository of the SARS viruses. One night, he/she takes some material from the SARS vials, and grows up enough viruses. He/she prepares a dispersion solution. Dressed as a cleaner, with enough PPE (personal protective equipment) to be protected but not "strange", he/she sprays the dispersion solution over the surfaces of the general admission center in the time of major influx of patients. All the people passing by the place (almost all the outpatients and the inpatients, over a four hour horizon due to the estimated time for survival of the virus on the surfaces) have contact with the virus. According to the infection rate, 10% of contacts get the infection. Infected people transmit the infection from man-to-man through air-droplets, four days after. The virus contacts take place in the whole hospital (including staff) and out of the hospital, from man to man. We can presume that there will be an increased incidence of severe pneumonias for the most vulnerable people, and then there will be an evidence of the same strain of virus at the investigations. No treatment and no vaccine are available. Only the support to vital functions is possible. Then some cases will start inside the hospital and will be reported in other hospitals. The Preventive Medicine Department will be informed. Quarantine measures and active case finding policies will be implemented. An unusual SARS epidemic is declared with impact on the whole city and eventually the need to transfer ICU patients out of the hospital region because of shortness of ICU beds. After some time lost looking for the single first case that started the epidemic, an anonymous letter reaches the hospital saying that it was a malicious act, and to prove this the check of the vials inside the P3 lab can be done. The fake PhD student has disappeared.

Regarding the simulation with our flow model, we suppose that there is a SARS attack at the beginning of period 10 for a warm-up reason (i.e. to have enough traffic), at the general admission center of the hospital. The SARS virus is transmissible between humans after 96 hours (4 days). Since all the patients (inpatients and outpatients) should go to the general admission center first, all the patients have the possibility to be infected. Here, we suppose

that 10% of the patients may be infected. From period 10 to period 13, the simulation calculates that 1357 patients passed through the general admission center. Therefore, the total number of infected patients is about 136 (136≈1357*0.1). At the beginning of period 14, the SARS virus is ineffective because of its lifetime. But the infected patients still have the possibility to infect others 4 days later mainly outside the hospital. Considering human transmission, the whole hospital is closed for 14 days to be decontaminated, and the operational loss (lost turnover) is estimated to 21 millions of Euros.

For the physical countermeasures of the SARS attack, first, we can reinforce the access control system of virus bank, by limiting virus accesses only to authorized persons or accompanied persons under the control of authorized persons. Today, access control systems have become more and more sophisticated. Here, we refer to the biometrics access control systems. Biometrics access control systems always adopt the fingers to record the information. Second, we can employ a dedicated security guard to protect the laboratory during the night in order to prohibit its access as human countermeasure. Third, we can use an intelligent video surveillance system able to detect and identify abnormal and alarming situations by analyzing object movement as information/physical countermeasure. Logically, the combination of these three countermeasures has the best effect. Our cost/benefit analysis (Cellini and Kee 2010) specifies that the cost of using a security guard is higher than using biometrics access control or using an intelligent video surveillance system for a similar benefit. So, using a security guard is not a good choice. The cost/benefit analysis concludes that the biometrics access control is better than the two others independently to other scenarios. So, using biometrics access control seems to be more reasonable.

4.23 Discussion

Our flow model allows us to evaluate the traffic in all care units and more generally in all areas of the hospital. The impact of bombing attacks in the most vulnerable places, i.e. the most crowded places, can be easily studied considering the traffic. As seen before, if a CBRN attack is perpetrated in some areas, we can calculate the number of contaminated people from the beginning period of the anonymous attack until the period of locking the contamination areas. In the case of the activation of an internal emergency management plan for the evacuation of a care unit (e.g., intensive care unit, following the medical gas stock destruction) or a building (e.g., after an electric power failure), we can calculate, firstly the number of people to be evacuated, and secondly the time required to evacuate patients, relatives and staff, by simulating a virtual care unit which represents the evacuation organization (i.e. the implementation of the internal emergency management plan). Some practices can also be investigated such as open spaces. For example, if we limit the hospital accesses, we note that the traffic increases in some areas which become more vulnerable.

Regarding the severity criteria, our flow model enables us to calculate the number of deaths or injured people, i.e. the human losses. The infrastructure damages can be indirectly estimated, considering the damaged and contaminated areas or equipment. If the hospital knows the cost of a hospitalization day in a care unit, operational damages can be evaluated considering the number of evacuated people to external hospitals, and/or considering the number of periods of closure of the care unit and its patient capacity (cleaning time, or decontamination time). Image damages will be appreciated in a more subjective way, because they are long-term consequences, but they can be approximated by a potential loss of turnover.

Our flow model also enables us to evaluate the impact of security measures. Regarding the patient pathway description (the map) of the hospital, the removal of accesses between buildings allows the cordoning off of a building (e.g. after an attack on its electricity grid), and the isolation of a contaminated/deteriorated care unit can be simulated by deleting its accesses with other services (e.g. after an attack of the emergency department by a suicide bomber). Furthermore, prohibiting the outside access of the emergency department is required to activate the external emergency management plan and receive mass casualties after an external terrorist attack in the city. Concerning the by-process description of care units, the people flows can be differentiated (staff, patients, relatives). Access controls can be easily simulated enabling or not a given flow between activities, these latter are most of the times associated to locations (rooms, halls). As we use linear programming to simulate heavy and complex systems (numerous care units, with dedicated processes), our data are all deterministic but they are sufficient for simulating most of the scenarios. Our static (IDEFØ) model or our dynamic (flow) model can inspire countermeasures by analyzing the obtained results, but they are most useful for assessing and comparing countermeasures to implement.

5. Conclusion

Our challenge is to design, to support, and to experiment a vulnerability assessment approach for critical infrastructures in the health care sector, in order to reduce the vulnerabilities of the hospitals, by proposing counter-measures, emergency management plans, and best practices. Our approach is firstly based on the estimation of the threat likelihood, secondly on the evaluation of the severity of terrorist attack scenarios, and finally on the study of potential countermeasures to reduce the attack impacts. We have chosen a quantitative assessment, based on complex and large system modeling, and attack simulation by a mathematical model.

Hospitals have not yet been first strike targets for major terror attacks in the EU, but the Paris attacks of November 13th 2015 demonstrate that calamitous attacks can occur without a pattern of previous strikes. 130 people were killed and 368 injured in the Paris attacks, which was not predictable from prior history. So, we propose to evaluate the likelihood of threats, on one hand by considering the motivations and capabilities of terrorists and on the other hand by regarding the attractiveness of the targets (critical assets of the hospital) in terms of ease of access and potential damages. Hospitals are human and complex systems, which are organized as open spaces to facilitate care access to patients. It appears quite difficult to identify their weak points and to estimate the consequences of a terrorist attack without using quantitative tools.

Our approach, firstly estimates the threat likelihood, by defining critical assets, finding the threat sources, and calculating critical asset attractiveness per adversary; secondly, it evaluates risk severity, by defining threat scenarios, and assessing the threat scenarios, and finally it reduces the vulnerabilities by evaluating counter-measures to implement. The IDEFØ method is used, to identify all the care units and services which define the critical assets of the hospital. It allows us to produce a hierarchical map of the hospital and to model the processes of the critical assets, i.e. the most accessible and damageable care units or services. By extracting the direct links between care units from the IDEFØ model, we can produce a multi-period flow model in order to calculate the traffic in the hospital and show for example the

most vulnerable places, where a terrorist attack can produce the most human damages. A linear program allows us to solve this flow problem and simulate attack scenarios.

Moreover, the linear program enables the human decision maker to calculate the human losses, the operational damages to the infrastructure and the financial losses as a result of the decisions made. By running different possibilities through the linear program, the decision maker can devise and refine more efficient emergency management plans.

The next step will be to adapt our approach to more specific terrorist attacks such as cyber-attacks. Information flows indeed do not follow the same pathway as patients, relatives and staff.

References

Altay, N., and W.G. Green. 2006. OR/MS research in disaster operations management. European Journal of Operational Research 175: 475–493.

Bajpai, S., and J.P. Gupta. 2005. Site security for chemical process industries. *Journal of Loss Prevention in the Process Industries* 18: 301–309.

Ben Othmane, L., R. Ranchal, R. Fernando, B. Bhargava, and E. Bodden. 2015. Incorporating attacker capabilities in risk estimation and mitigation. *Computers and Security* 51: 41-61.

Bevilacqua, M., F.E. Ciarapica, and C. Paciarotti. 2014. A BPR approach to hydro geological risk management. *Natural Hazards* 71: 1995–2012.

Bevilacqua, M., F.E. Ciarapica, and C. Paciarotti. 2012. Business Process Reengineering of emergency management procedures: A case study. *Safety Science* 50: 1368–1376.

Birkmann, J., S. Kienberger, and D.E. Alexander. 2014. Introduction Vulnerability: a key determinant of risk and its importance for risk management and sustainability. In Assessment of Vulnerability to Natural Hazards A European Perspective, edited by J. Birkmann, S. Kienberger, D.E. Alexander. Amsterdam: Elsevier. ISBN 978-0-12-410528-7: IX-XIII.

Carnaghan, C. 2006. Business process modeling approaches in the context of process level audit risk assessment: An analysis and comparison. *International Journal of Accounting Information Systems* 7: 170–204.

Cellini, S.R., and J.E. Kee. 2010. Cost-effectiveness and cost-benefit analysis. In Handbook of practical program evaluation. San Francisco: *Jossey-Bass*. 3rd Edition: 493-530.

De Villepin, D., 2005. French Government White Paper on Internal Security to Face Terrorism (Livre blanc du gouvernement sur la sécurité intérieur face au terrorisme). Accessed April 4. http://www.diplomatie.gouv.fr/IMG/pdf/LIVRE_BLANC_terrorisme.pdf.

Europol. 2016. European Union Terrorism Situation and Trend Report. Accessed April 4 https:// www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2016.

Ganor, B., and M. Halperin Wernli. 2013. Terrorist Attacks against Hospitals Case Studies. International Institute for Counter-Terrorism (ICT) Israel. (Working paper 25). Accessed April 4. https://www.ict.org.il/Article/77/Terrorist-Attacks-against-Hospitals-Case-Studies.

IBM ILOG CPLEX Optimizer. 2015. Accessed April 4. http://www-03.ibm.com/software/products/ en/ibmilogcpleoptistud.

IDEFØ. 1993. Integration Definition for Function Modeling (IDEFØ). Draft Federal Information Processing Standards 183. Accessed April 4. vernikov.ru/media/K2/ item_attachments/idef02.doc.

IEP. 2016. Global Terrorism Index 2016. Institute for Economics and Peace. Accessed April 4. http://economicsandpeace.org/wp-content/uploads/2016/11/Global-Terrorism-Index-2016.2.pdf.

Marhavilas, P.K., D. Koulouriotis, and V. Gemeni. 2011. Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000-2009. *Journal of Loss Prevention in the Process Industries* 24: 477-523.

Miniati, R., and C. Iasio. 2012. Methodology for rapid seismic risk assessment of health structures: Case study of the hospital system in Florence Italy. *International Journal of Disaster Risk Reduction* 2: 16–24.

Moore, D.A. 2006. Application of the API/NPRA SVA methodology to transportation security issues. *Journal of Hazardous Materials* 130: 107–12.

OWASP. 2016. Risk rating methodology. Accessed April 4. https://www.owasp.org/ index.php/ OWASP_Risk_Rating_Methodology.

Ross, D.T. 1977. Structured Analysis (SA): a language for communicating ideas. *IEEE Transactions on software engineering* SE-3: 16-34.

Saaty, T.L. 1980. Analytical Hierarchy Process: Planning, Priority Setting, Resource Allocation. New York: *Mc Graw-Hill*.

Shahid, S. 2009. The weighted risk analysis. *Safety Science* 47: 668–679.

Shimada, Y., and H.A. Gabbar. 2008. Development of Activity Models of Integrated Safety and Disaster Management for Industrial Complex Areas. In Knowledge-Based Intelligent Information and Engineering Systems. *Lecture Notes in Computer Science* (Berlin: Springer) 5179: 1-8.

Stewart, M.G. 2010. Risk-informed decision support for assessing the costs and benefits of counter-terrorism protective measures for infrastructure. *International Journal of critical infrastructure protection* 3: 29-40.

Wheeler, E. 2011. Risk exposure factors. In Security Risk Management. Amsterdam: Elsevier 105-125.