"Co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union"

Report No: DR/2/001

Analysis of Risk Management Planning and Perception to Counter the Terrorist Threat within the Health Sector of European Union Critical Infrastructure Protection.

Version: 1.0

Date: 09 APR 2015

Authors: Pierluigi Ingrassia, Marta Caviglia, Ahmadreza Djalali

Approved by: Chris Arculeo

Table of Contents

Glossary

Critical National Infrastructure (CNI) – Physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in EU States. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services (EC, 2004).

Critical Information Infrastructure protection (CIIP) – In its Communication on Critical Information Infrastructure protection (CIIP) European Commission launched an action plan involving also Member States and the private sector focusing on the protection of Europe from cyber disruptions by enhancing security and resilience. (EC, 2009)

European Programme for Critical Infrastructure Protection (EPCIP) – In its EPCIP communication of 12 December 2006, the Commission set out an overall policy approach and framework for critical infrastructure protection (CIP) activities in the EU (EC, 2012).

Personal Protective Equipment (PPE) - Equipment designed to be worn or held by the worker to protect him against hazards encountered at work. A number of items are excluded from the definition, such as equipment used by emergency and rescue services, self-defence or deterrent equipment. Such equipment must be used when the existing risks cannot be sufficiently limited by technical means of collective protection or work organization procedures.

Executive Summary

Set against the backdrop of the increasing terrorist attacks throughout Europe, the likelihood of a terrorist attack against an EU Hospital is also heightened. Recent events in France and Denmark have brought to light the growing terrorist threat inside the European Union Member States (EU MS); a threat that cannot be ignored, as potential attacks can be addressed towards all EU MS and against disparate targets.

In this respect, it is reasonable to consider EU Health Care facilities as potential primary targets: hospital can be very attractive to terrorist since they are seen as vulnerable and unprotected, relatively easy to access, and with a significant number of potential casualties. To the same extent, hospital themselves make an attractive secondary target during a second "*attack*" planned by terrorists after a first, when the response system is already activated. Hence, it is critical to develop systems that ensure a resilient healthcare and public health system capable of withstanding the disruption that will follow such attacks.

The EU has issued direction (EC, 2008) to implement critical infrastructure protection CIP in all EU MS; however, according to recent literature and results of WP1, EU Health Care facilities are not always considered as part of Critical National Infrastructure (CNI); moreover, it is still not clear if all EU Hospitals designated as CNI are preparing or are actually prepared to face terrorist attacks using effective contingency planning in accordance with either EU directive or any national/international guidance.

There is a clear need for information about current Hospital preparedness in order to develop and validate decision-making tools designed for mitigation and increased resilience of EU Hospitals as a critical infrastructure, with improved protection capability and security awareness. To this regard, it is also crucial to gain knowledge about the current awareness and involvement of hospital staff during crisis management, as they play a critical role in ensuring a safe and secure infrastructure and effective response.

Hence, the aim of this research was to determine the situation of crisis risk management plans within the EU health sector including hospitals, in respect of terrorist attacks.

A survey composed of 58 questions was sent to 137 hospital disaster coordinators, security managers and resilience officers, spread in the 28 EU country, using SurveyMonkey. Target of WP2 was to reach at least 3 Hospitals in every EU country, with a total of 84 Hospitals. The availability of emergency/crisis management plans, specific preparedness

education/training, previous experiences, security measures and equipment, point of weakness and strengths were examined.

Response rate was 56%. The findings revealed that a majority (94%) of hospitals have documented emergency/crisis management plans, provided emergency management training and education programs (90%), and generally felt that they had implemented effective security measures to prevent and manage consequences of different type of threats, including terrorism.

However, 53% of the participants underlined the absence of national/local information or guidance on how to reduce Hospital vulnerability to attack or the consequences of an attack outside or inside the hospital; moreover, crisis management capability seems to be highly influenced by financial shortcoming (68%), low priority (59%) and poor knowledge and competencies of personnel (51%).

1. Introduction

1.1 In recent years, government and hospital leaders have recognized the increasing importance of hospital preparedness in response to both natural and man-made disasters, especially chemical, biological, radiological, nuclear, and explosive (CBRN-E) threats that will be conducted by terrorists; the need for hospitals to be prepared to respond to such events has therefore increasingly become a priority for disaster planners. In 2012, an European study demonstrated that health system preparedness for disaster response in the 27 European Union member countries was barely at an “acceptable level” (Djalali et al, 2012). Self-assessed average level of disaster management preparedness was different among the EU countries, with highest levels in United Kingdom, Luxemburg, and Lithuania and lowest in Portugal, Malta and Ireland. With regard to different elements of the disaster management system, results of the study showed the highest level of preparedness in the health information element, whereas hospitals and education and training elements had the lowest level of preparedness, with lack of competency-based training and education being the main gap in health disaster preparedness in the EU.

The last EU Terrorism Situation and Trend Report (TE-SAT) reported that a total of 152 terrorist attacks occurred in five EU Member States in 2013, involving mainly France (63), Spain (33) and the UK (35). (EU, 2014)

Terror-related mass casualty events acutely strain healthcare facilities where they occur, as frequently hospital are significantly affected by a large number of casualties. Moreover, the complex terrorist scenarios witnessed in recent years, showed a new trend in terrorist attacks known as the “second strike”: a second “attack” planned by terrorists after a first, when the response system is already activated and becomes the primary target. Hospital themselves make an attractive secondary target of attack, since they can distract security and response staff from the primary target of attack, and also confound the removal and treatment of the wounded from the site of the primary attack.

According to Ganor and Wernli (2013), approximately 100 terrorist attacks have been perpetrated towards hospitals worldwide between 1981 and 2013, causing 775 deaths and 1,217 injured casualties. Among the 100 attacks, 11 involved European Hospitals and were perpetrated mainly through armed assaults and bombings.

1.2 With the adoption of the European Program for Critical Infrastructure Protection (EPCIP) in 2008, and the following review of the directive 2008/114/EC in 2012, the European Union has established a procedure for the identification and designation of European Critical Infrastructures and a common approach for the assessment of the need to improve their protection. Although the approach was essentially all-hazards, priority has been given to the threat from terrorism.

Results of WP1 have however underlined that, despite Critical Infrastructure Protection (CIP) activity is underway in many of the EU Hospitals, the overall collective approach is still uncoordinated, and some of the EU MS do not consider Health facilities among Critical National Infrastructure (CNI), thus leading to a disparate status of CIP across Europe.

We may assume that preparedness against terror threats is not part of the daily routine of all civilian general hospital and its complexity often requires a major management effort; it can be reasonable, therefore, to expect a wide range of different preparedness and awareness among EU hospitals, depending on various aspects such as: health care structure, geographic and demographic differences, country, city, previous experiences, presence/absence of available standards and guidelines, financial means, priority level.

1.3 The purpose of the THREATS project is to provide the EU MS with the most efficient and reliable decision-making tools to be familiar and minimise critical healthcare infrastructures' vulnerability to terrorist attacks, by increasing awareness and preparedness against terrorist attacks targeting hospitals and healthcare infrastructures. It is therefore essential to establish common and uncommon features regarding EU Hospital preparedness and response in respect of terrorist attacks.

Our aim was to analyse and synthesise the current situation within the EU Health sector in respect of terrorist attacks, with a specific focus on the state of the art of threat assessment, existing crisis management plans, exposure consciousness and risk perception of hospital as CI against terrorist attack and point of strength and weakness in the development of response and security activities.

2. Methodology

2.1 This study is an observational, cross-sectional study. The survey was conducted between November 2014 and March 2015. All 28 EU countries were included in this study.

In order to evaluate EU hospital awareness, planning and preparedness in response to terrorist attacks, we have created a standardized survey composed of 58 questions, subdivided into 6 different sections: general framework; emergency/crisis management plan; previous experiences; training, exercise and testing; security measures and equipment; barriers and facilitators.

The survey includes also a consent form, an introductory part to collect general information of the respondent and a definition part to explain the definitions of Critical Infrastructure and Personal Protective Equipment (PPE) (Appendix 1).

2.2 The questionnaire addresses the findings of WP1 (*Threat, risk analysis and security assessment research of the state of the art regarding threats and risks to the heath sector and how it is protected as part of the critical national infrastructure within Europe*) and is built on standards and measures extracted from available scientific literature. The literature review was conducted using both specific search engines (PubMed, Scopus) and general search engines (Google).

The aim of the research was to collect information that could be employed to explore the different aspects of hospital response to terrorist attack and build the various sections of the survey.

2.3 Elements of the questionnaire. The questionnaire consists of six different sections and elements, as following:

General Framework: this section has the purpose to collect general information on current conditions of EU Hospital as Critical Infrastructure, in respect of awareness, vulnerability assessment, available indicators and guidelines employed to manage terrorist threats and their consequences.

Emergency/Crisis management Plan: this section focuses on the existing emergency/crisis management plan in the EU Hospital, with specific regard to the frequency of revision, reference to any available guidelines, frequency of testing,

inter-organizational crisis management and presence of specific security elements in respect of terrorist threats.

Previous Experience: this section has the purpose to analyse any previous experience and exposure in terms of terrorist attack, and the Hospital consequent response and risk management, with focus on the implementation of specific security measures.

Training, Exercise and Testing: the main task of this section is to analyse the presence of training educational program and the participation of the Hospital staff to any national/international simulation/exercise in response to terrorist attack.

Security Measures and Equipment: this section explores the existing Security Measures of the Hospital in respect of CBRN and Cyber threats, and the correlated use of Personal Protective Equipment.

Barriers and facilitators: the last section of the survey has the purpose to investigate existing internal and external weakness and difficulties or the presence of factors that simplify and facilitate the preparedness and management of terrorist attack.

2.4 To standardize and validate the survey content, the Delphi method was used (Linstone H, 2002). Fifteen different international experts in the field of hospital resilience and safety were contacted and their feedbacks were analyzed, synthesized and used to improve the survey. A second version of the survey was again sent to the experts, and consensus on the structure and the contents was made to finalize the questionnaire.

2.5 A database of EU Hospitals was created, utilising the national and international stakeholders connections with THREATS consortium. The e-mail contact of 145 hospital disaster coordinators, security managers and resilience officers were recognized, spread in 23 of the 28 EU countries. Despite our efforts, we couldn't obtain any useful contact in the following countries: Cyprus, Czech Republic, Lithuania, Luxembourg, Slovenia.

2.6 SurveyMonkey has been selected as the as the simplest way to distribute the survey. Identical e-mail requests were sent to 145 European Health care contacts on the 24th of November 2014; the e-mail included the explanation of the project, privacy

and security issues and the LINK necessary to access to the survey. The lack of initial feedback required a further reminder which was sent on the 7th of December 2014. Since security issues seemed to be one of the main concerns preventing participants to respond to the survey, an additional email with an exhaustive explanation of security issues, use of personal data and processing of security information has been sent. A further reminder was then sent on the 15th of January 2015.

THREATs project is a progressive and cumulative study and the body of knowledge is likely to grow as more information becomes known and as awareness of THREATS grows across the CIP and Health Sector communities. Therefore report D2.1 will be reviewed in May/June 15 in order to include new information and adjust the findings as necessary.

3. Results

3.1 Forty-seven participants from sixteen different EU States have answered the survey. Forty-five of them gave their consent to be nominated to the study, whereas two of prefers to be anonymous. Academic educational level reported shows a majority of MD (36%), followed by MSc (27%), PhD (23%) and BSc (14%). As shown by the figure below, participants work mainly in university and public hospitals.

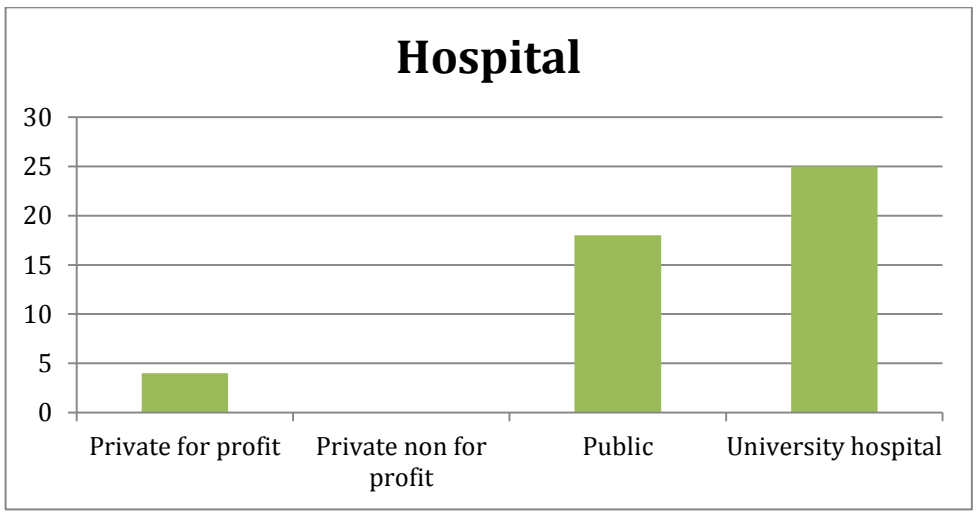

Fig.1. Affiliation of hospitals, which answered to the THREATS questionnaire

3.2 *General Framework*: twenty-one participants (66%) come from a country/region that has a national or local threat level indicator for terrorist attacks, and in most cases its update/circulation is guaranteed by the national government or public media.

However, percentage descends drastically regarding the presence of a specific threat indicator/level for terrorist attacks for the Health service/Hospital, which is absent according to the 57% of the participants (fig.2).

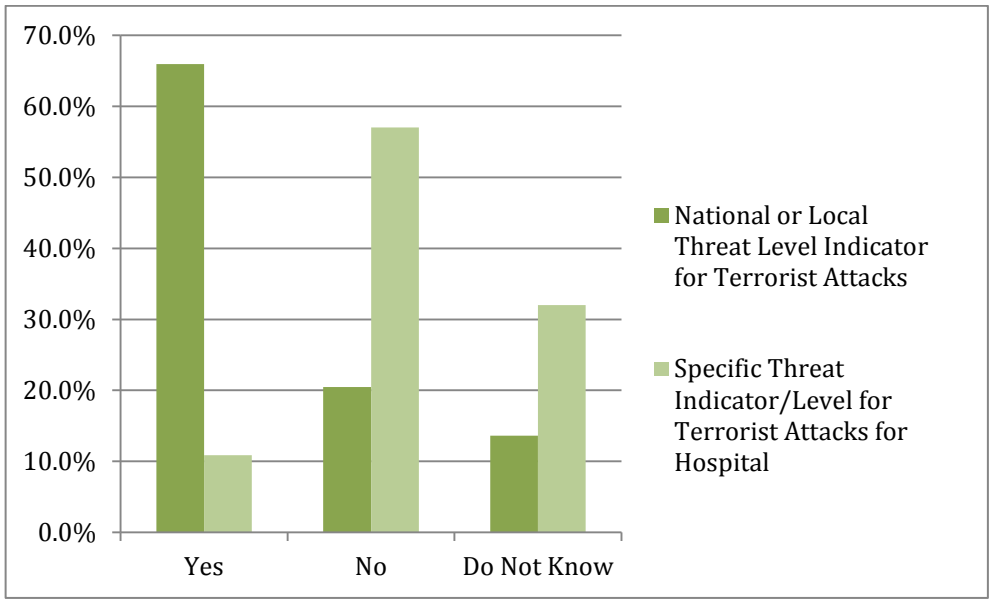

Fig.2. Percentage of the presence of national or local threat level indicator for terrorist attack compared to percentage of hospital that have specific threat indicator/level for terrorist attacks

In the majority of cases (68%) the Health Service or Hospital is also designated as part of the Critical Infrastructure, with high security priority. Information or guidance on how to reduce its vulnerability to attack or the consequences of an attack outside or inside the hospital are available according to 40% of participants (fig.3); in those cases, the Police or the Counter Terror Unit are the principal provider of such information.

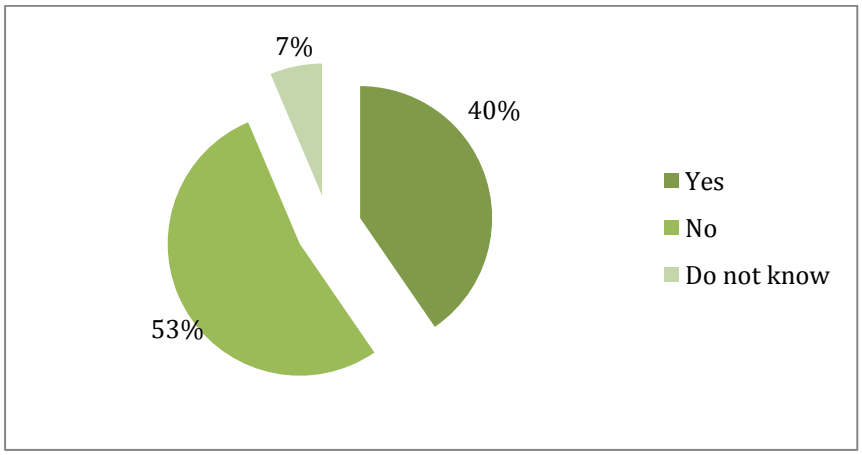

Fig.3. Presence of information/guidance on how to reduce hospital vulnerability to attack or the consequences of an attack outside or inside the hospital.

Security intelligence is involved only in the 23% of the cases in the management of terrorist threats; 51% of participants confirm the presence of a Hospital manager responsible for managing the threat and risk of terrorism. This role is undertaken in most cases by the Head of Security, the Disaster Coordinator or the Risk Manager.

In over 60% of cases the Health service/ Hospital has implemented some protective measures to reduce the risk or consequences of a terrorist attack outside or inside the hospital; participants described the presence of emergency/disaster plan and operational procedures to face extraordinary events and some training of security personal, despite the absence, in the majority of cases, of any national or regional funding (61%) to reduce the vulnerability or consequence of a terrorist attack. Nevertheless, about 45% of the participants assert that no inspections or checks are made to assess the vulnerability and consequences of a terrorist attack outside or inside the hospital; similarly, 45% of participants deny the implementation of training and awareness regarding the threat, vulnerability and consequence of a terrorist attack on the facility.

3.3 *Emergency/Crisis management Plan*: an emergency/crisis management plan is present in the 96% of cases, which is revised and tested (Full-Scale Exercise, Mock Disaster Drills, Tabletop Exercise, Functional Exercise, etc.) with a certain regularity (annually or biannually). Participants declare that the revision of the plan is based mainly on national (60%), regional (20%) or international (11%) guidelines; in the majority of case (82%) revision are also influenced by the result of exercises and tests, through the evaluation and identification of strengths and areas of improvement. These improvements concern: changes in policies and procedures (82%); security equipment upgrades (33%); additional security measures (31%). However, a mechanism for monitoring the continuous correction of gaps that identified in the exercises is present only in 46% of cases. In the 98% of cases, participants reported that the hospital didn’t rely on a private sector/agency to manage and develop the emergency/crisis plan.

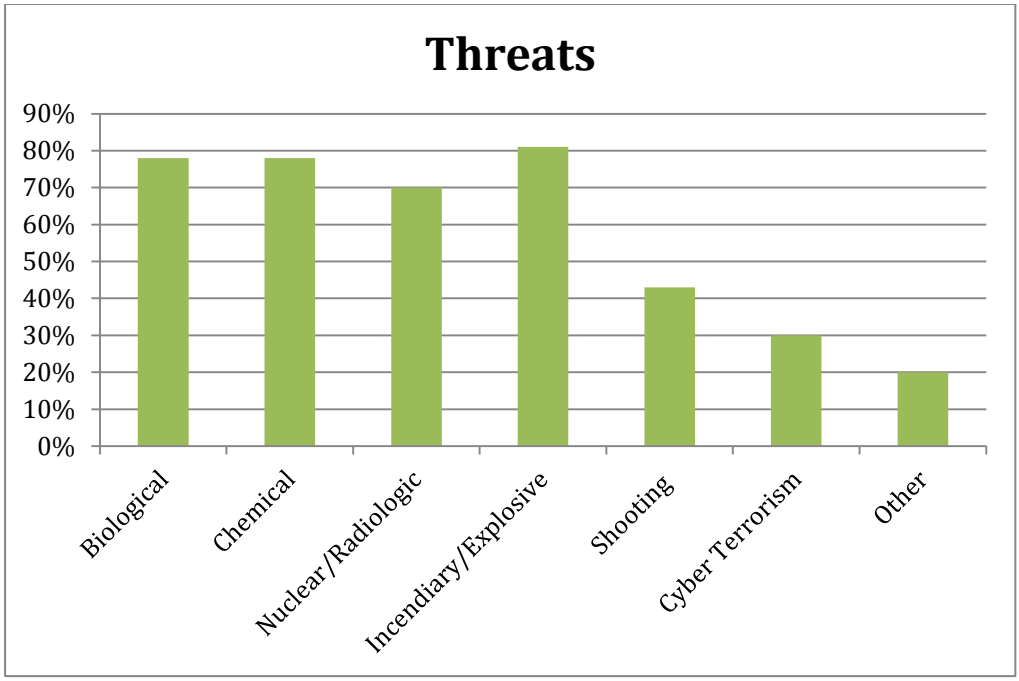

Fig.4 Most common threats covered by the crisis/emergency plan

Fig. 4 shows the principal threats covered by the crisis/emergency plan; when asked which entities does the hospital's plan specify contacting in the context of terrorism incident, participants answered as follows:

- Emergency Medical Services (68%)
- State or local public health department (61%)
- State or local law enforcement (68%)
- Fire Department (64%)
- Other hospitals/local hospital association (43%)
- Disaster-response agencies (27%)

About 60% of responders assert that the emergency/crisis management plan is not promulgated to other stakeholder agencies. The remaining 40% of participants state that the plan is shared with other hospitals, fire departments, and local authorities. Measures included in the emergency/crisis plan are the following:

- Definition and integration of the hospital's role in community wide planning (70%)
- Designation of an Emergency Management Team (88%)
- Each area of the hospital has department-specific actions or roles to fulfill in the event of emergency response (80%)
- Communication of hospital status, requests for assistance and supplies, to the local Emergency Operations Center and other area hospitals (80%)

- Business continuity (59%)
- Outlying hospital to accept inpatients during a declared attack (59%)
- Rapid increase of supplies, equipment and personnel in case of terrorist attack (68%)

In respect of the safety of staff, patients and other inhabitants in case of a terrorist attack to hospital, the plan provides information for partial (78%) or complete (36%) evacuation; lockdown procedures (50%); creation of area of safe refuge (36%); procedures for sheltering-in place (31%).

3.4 *Previous experiences:* only three participants declared that the hospital has experienced a mass-casualty situation following a terrorist attack in a different site; two of them in UK, one in Croatia. To face the event, the three hospitals used a written disaster plan and the hospital operations are described as well coordinated at every level.

	Needed	Not Needed	Implemented	Not Implemented
Back-up plans to accept casualties if all beds were occupied	66%	33%	66%	33%
Continuity of the essential services	66%	33%	66%	33%
Partial/complete evacuation	66%	33%	33%	66%
Stockpiling drugs and medical supplies	66%	33%	33%	66%

Tab.1 Percentage of measures needed and implemented in the hospital during the response to a terrorist attack.

As Tab.1 shows, back-up plans to accept casualties if all beds were occupied and continuity of the essential services have been implemented in the 66% of cases. Partial or complete evacuation and stockpiling drugs and medical supplies are described by participants as not needed in one of the three cases (33%), needed but not implemented in the second (33%) and implemented in the third (33%). In that occasion, the three hospitals have managed to be completely self-sufficient in terms of back-up energy, water and food supply, have activated appropriate security precautions to face the possibility they may be a secondary target of the attack.

Regarding cyber-terror, among the forty-four total participants, the majority (63%) has never experienced any network branches (malware,...), whereas the 26% has experienced at least one known data breach in the past five years.

When asked to report any other experience of terrorism or other serious event that has affected their hospital, two participants refer to have experienced several bomb threats; other two report previous experience with dispersion of hazardous materials.

3.5 *Training, Exercise and Testing:* 90% of the participants declares that their facility has an ongoing emergency management training and education programs, based on face-to-face training and lectures (80%), presentations tabletop exercises (70%), full-scale rehearsals (57%) and online training module (25%). Nevertheless, specifically regarding terrorist attacks, the 66% of participants denies the participation in any internal or external simulation/exercise. Moreover, hospitals are involved in National Level Exercise Programs only in the 27% of cases (Fig.5).

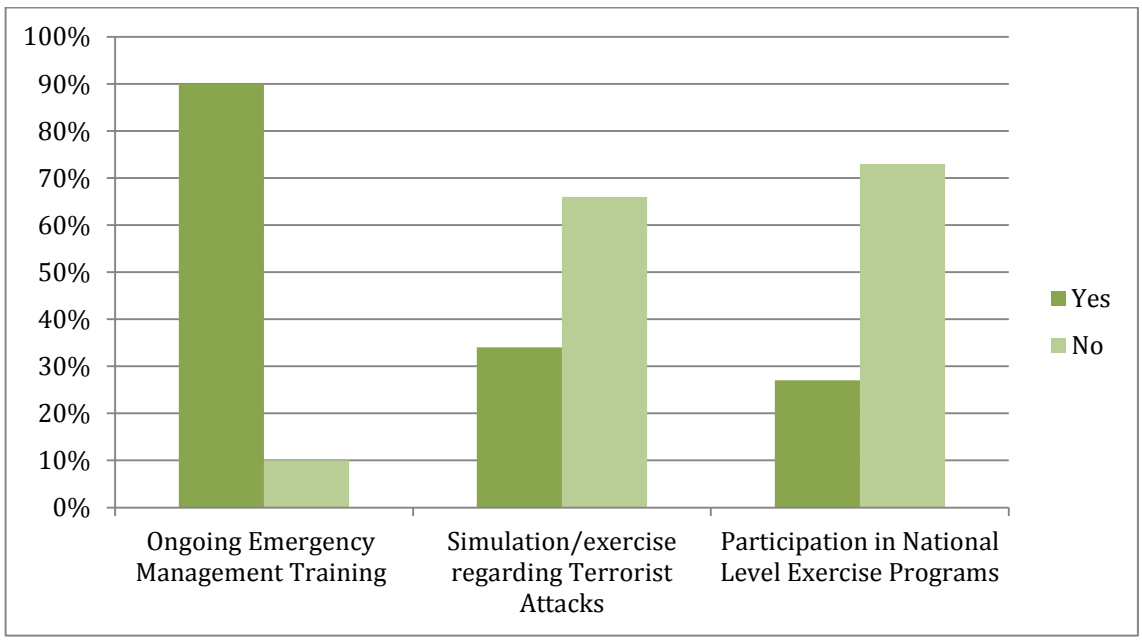

Fig.5. Percentage of hospitals that participate to any simulation/exercise regarding emergency management and terrorist attacks

Thirty participants assert that the hospital has established program of continuing education to encourage/promote awareness of emergency procedures among hospital staff. In 77% of cases, key personnel in the hospital have been trained in how to implement a formal Incident Command system, with different disparate answers regarding the percentage of personnel actually receiving training.

In the majority of cases (66%), the hospital does not provide training on how to recognize and respond to suspicious activity, including unidentified packages and persons exhibiting suspicious behaviour.

3.6 *Security Measures and Equipment:* the following activities and precautions to improve hospital safety appear to have been adopted:

- access to the sensitive area of the hospital restricted to authorized personnel only (84%)
- alarm system to detect unauthorized entry or attempted entry at critical components (61%)
- specific training of security personnel, including the proprietary security force, contractual security personnel, off-duty law enforcement officers (58%)
- gate control system to control the access of vehicles (66%)
- closed circuit television cameras with record and archive capability (68%)
- screening of visitors who seek to enter the hospital after regular visiting hours, monitoring center (42%)
- suggest screening of visitors in normal visiting hours (21%)

In 46% of cases Hospitals use a security assessment framework to assess physical facilities, conducted with a frequency of once a year or more (83%) whereas a large part of participants (28%) answered "*Do Not Know*".
Backup radio systems are present in the 79% of cases, in all ERs (33%) or in dedicated areas (46%), and the 67% of responders confirms the establishment of special modes of communication (such as VHF Radios, Satellite phones, Digital Radio Systems) to sustain communications with the local emergency management agency, tested periodically in the majority of cases (56%).

Regarding Cyber and Information Security, the following precautions seems to be implemented:

- Each employee has an individual account with a unique username and password (97%)
- Restricted unauthorized access to the network (78%)
- Monitored network activities for unauthorized use (70%)
- Patient confidential information management (81%)
- Internet firewall software and virus protection are installed on every computer (81%)

- Physical locks on devices and their communication ports to prevent tampering (38%)
- Routine and periodic evaluation, including updating security patches and disabling all necessary ports and services (59%)
- Secure connection to the Internet (72%)
- Development and evaluation of strategies to maintain critical functionality during adverse conditions (51%)

All hospitals provide identification badges to all employees and volunteers; in 59% of cases, when hiring personnel, background, employment eligibility and professional references are appropriately verified according to standardized guidelines; in 62% of cases when terminating employment, employees are required to turn in photo IDs, keys, access codes, and other security-related items.

Only 36% of hospitals have a checklist to use for threats or suspicious calls or to report suspicious activity, which is reported to the security personnel in the majority of cases. As fig.6 shows, in 70% of cases the hospital stockpiles PPE against CBRN (Chemical, biological, radiological and nuclear) threats, but only in half of the cases the hospital personnel, in particular staff of ED department, receive specific training in proper use of it; in addition, 61% of hospital are also equipped with decontamination facilities.

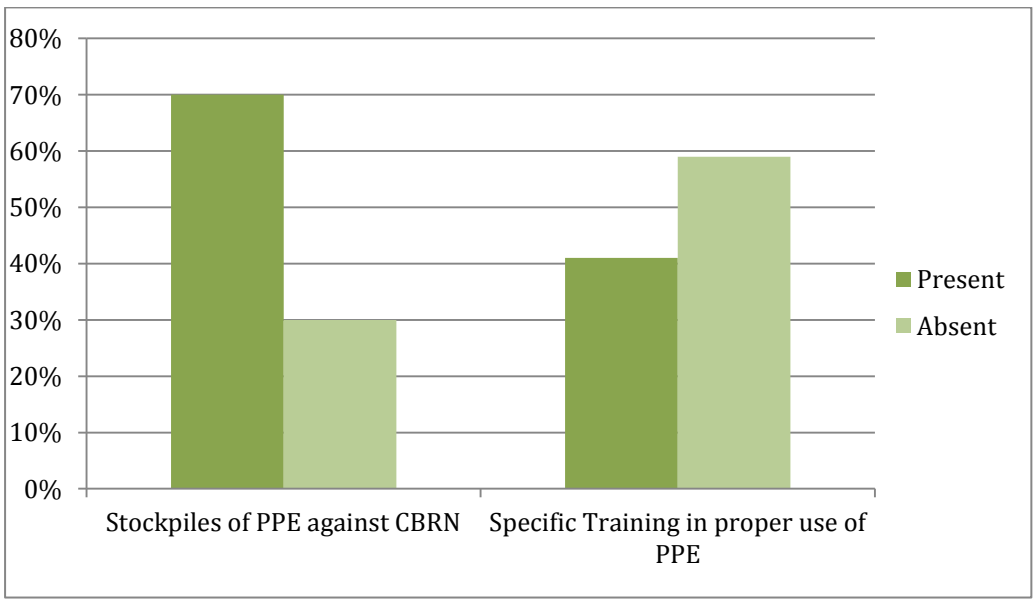

Fig.6. Comparison between the presence/absence of PPE stockpiles and the presence/absence of specific training in their proper use.

Barriers and facilitators:

- The **main** barriers to crisis management capability seems to be financial shortcoming (68%), followed by low priority (59%) and poor knowledge and competencies of personnel (51%), (Fig.7).

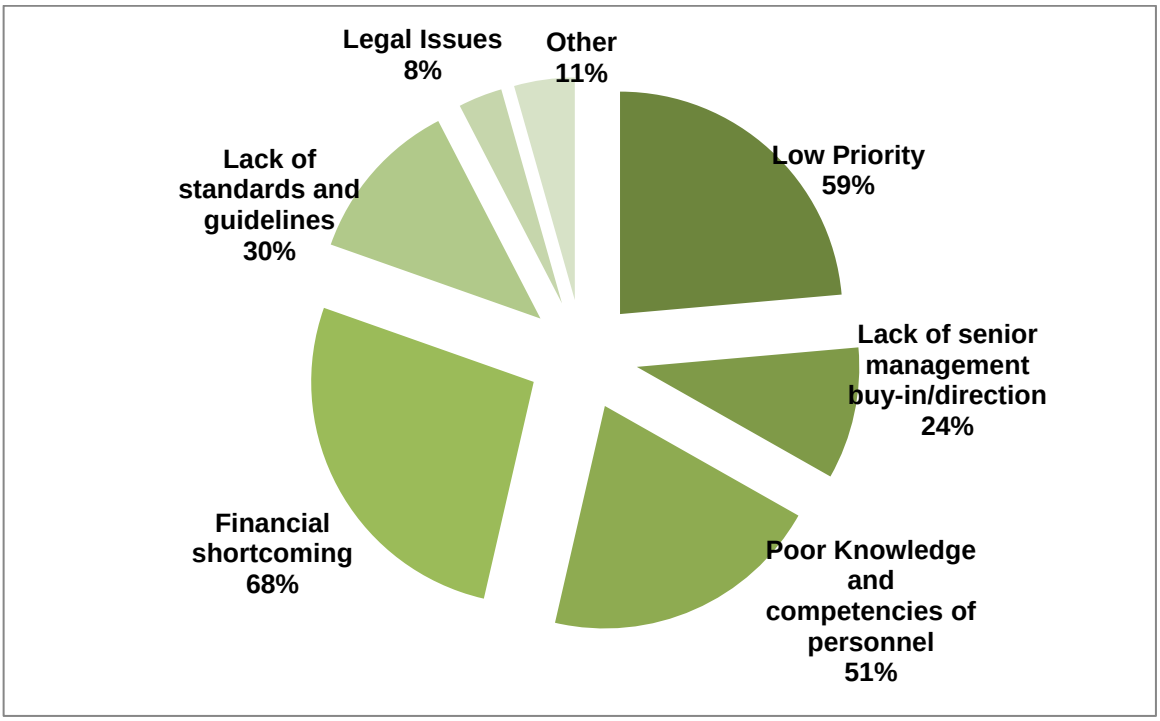

Fig. 6. Main barriers to crisis management capability

- In *most* of cases (49%), the security budget come from internal financing, against a 38% of funding coming from external financing and a 13% from both. (Fig.7)

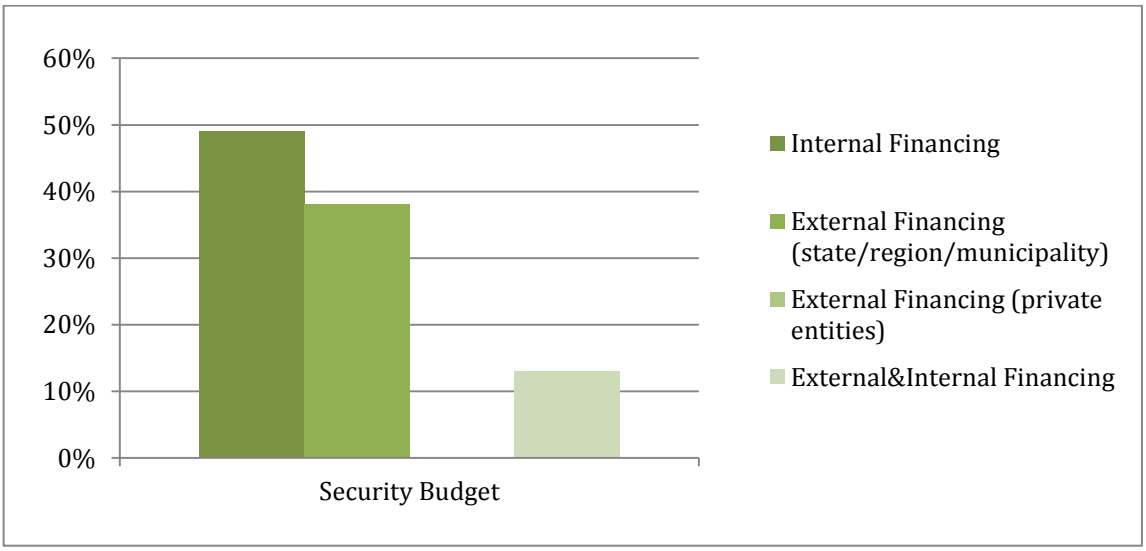

Fig.7. Sources of security budget

- Less than 5% of hospital budget is spent on security management in 53% of the hospital interviewed. (Fig.8)

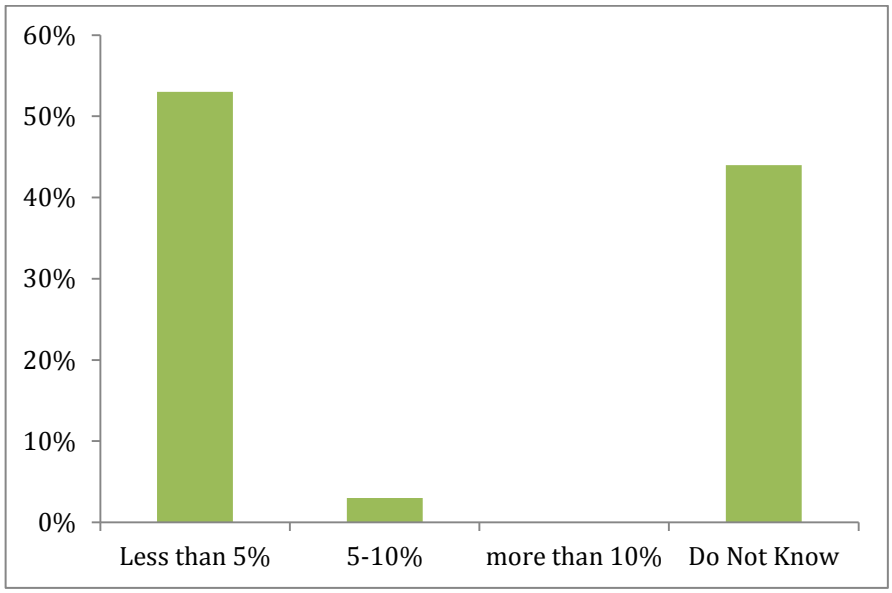

Fig.8 Percentage of hospital budget spent on security management

.

- Less than 5% of hospital budget is spent crisis management respectively in 61% of the hospital interviewed. (Fig.9)

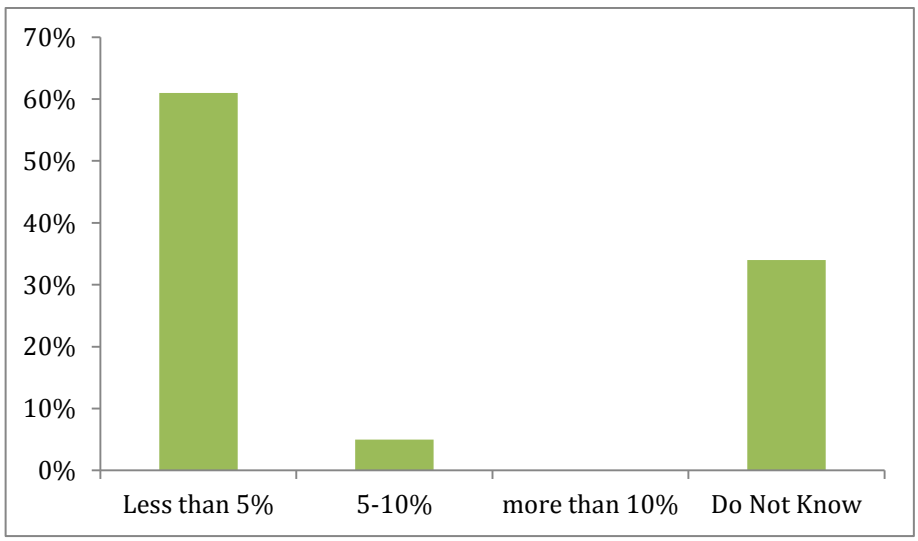

Fig.9 Percentage of hospital budget spent on crisis management

- Globally, security budget has not increased in the last 5 years (64%)

- Fig.10 shows answers to the question “How high priority is hospital security to top management or directors?”; the 46% of participants answered ‘Neither high nor low

priority'; according to 20% of them could be considered as Low priority, and according to 20% of the responders it could be considered as High priority.

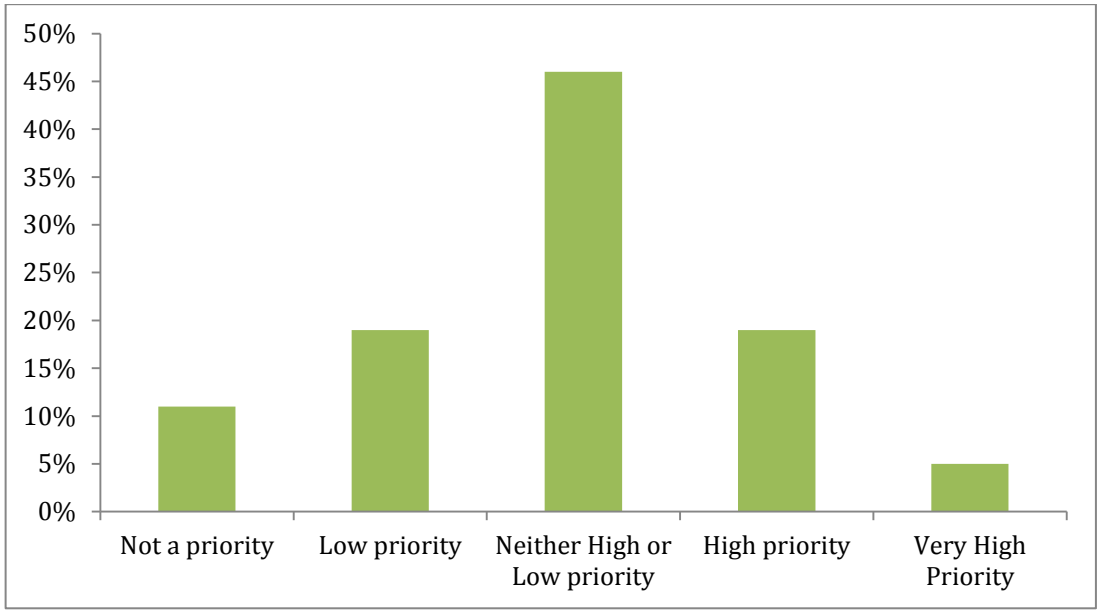

Fig.10 Priority level given to hospital security by top managers or hospital directors

- In 31% of cases, hospitals can rely on the presence of counterterrorism guidelines; 69% of hospitals encourage key personnel to participate in conferences about emergency/crisis management and in 54% of cases hospital personnel include people with any knowledge/training in the field of terrorism response or mass casualty events.

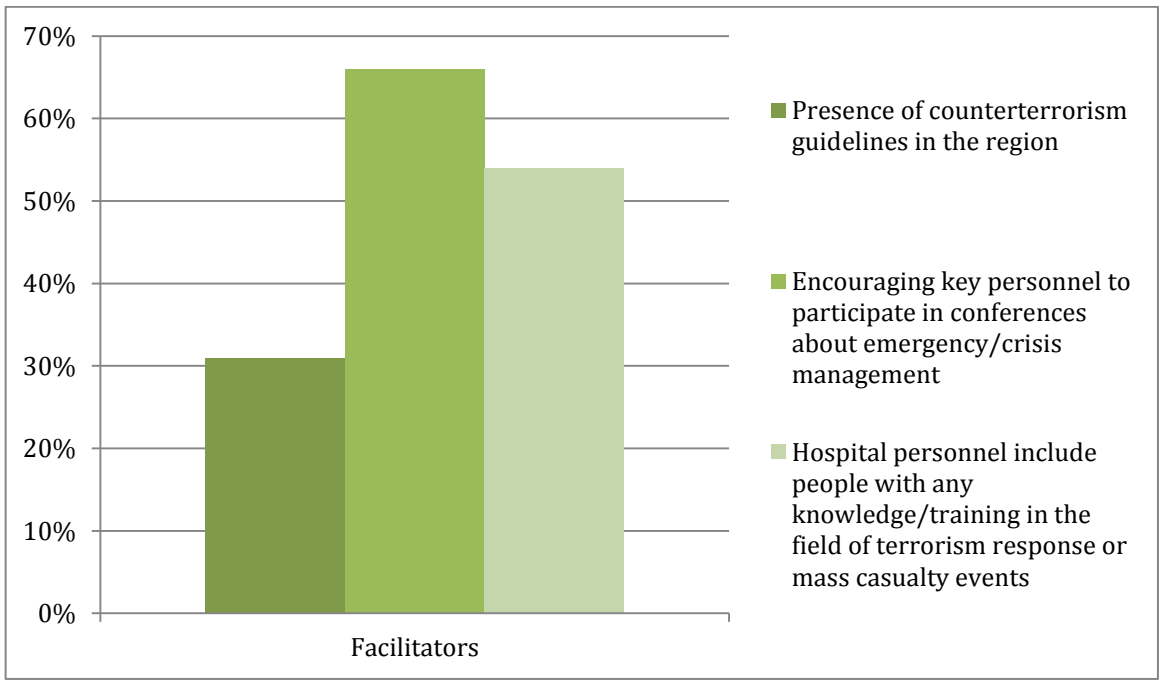

Fig.11 Main facilitators to emergency/crisis management

4. Discussion

The findings of this research suggest that the need to implement specific measures to reduce hospital vulnerability and face the consequences of terrorist attack towards hospitals is generally well-recognized by the majority of the EU hospitals interviewed; nonetheless, some point of weakness regarding the management of such threats have to be highlighted, and will be further discussed and analyzed later.

According to results, the majority EU MS recognize Health Services/Hospitals as CNI; many participants to the survey often describe their hospitals as "*top-level*" or "*high-priority*" in terms of integration inside national program of protection. Nonetheless, comparing these data to WP1 findings, some discrepancies emerge: as a matter of fact, among the 32 participants who confirmed their hospital to be part of CNI, only 10 of them actually come from EU MS who include the Health Sector as CNI. Remaining cases come from countries who don't include health as CNI, or where CIP policies don't provide any references to health infrastructure. This entails the presence of a general misconception of CNI and lack of awareness and knowledge about CIP among EU MS.

Results emphasize the role of the national government in the update and circulation of threat level indicators for terrorist attacks in a moderate percentage of cases. Despite the presence of specific threat indicator/level for terrorist attacks, the majority of participants reported a lack of information or guidance on how to reduce hospital vulnerability to such threats; similarly, assessment of hospital vulnerability are made only half of the cases, as well as implementation of training and awareness to reduce such vulnerability.

Results also show that emergency/crisis management plans are available in almost every Health Service/Hospital. Findings of WP1 and data provided by private organisations highlighted that lack of CIP strategies, policies and directive at government level in some EU MS drive private agencies, including companies which provide specific services such as utilities, to manage CIP, often developing contingency plans. Focusing on Health care sectors, according to results of this survey, almost every EU Hospital did not commit the development of the emergency/crisis plan to private agencies.

Findings of this questionnaire underlined how the emergency/crisis management plan of hospital interviewed covers a broad range of threats in the hospital , from CRBN-E attacks to Cyber Terrorism; this in accordance with the all-hazard approach

fostered by the World Health Organization Regional Office for Europe, who recently developed an hospital emergency response checklist to assist hospital administrators and emergency managers in responding effectively to the most likely disaster scenarios. (WHO, 2011)

According to the majority of participants, response to those events include the implementation of a number of effective protective measures in order to guarantee business continuity of the facility and safety of staff, patients and other inhabitants. Regarding CBRN-E threats, most of the hospitals ensure the presence of decontamination facilities and PPE, though results show an evident lack of training on the proper use of PPE among hospital personnel and the scale and availability of these resources may not match the needs of a mass decontamination event.

Inter-organizational coordination between the hospital and other relevant entities, such as EMS and local authorities, fire department and other hospitals, is also frequently reported; however, less than half of the hospitals interviewed actually promulgates the emergency/crisis management to other stakeholder agencies.

Nonetheless, only three hospitals have ever experienced a mass-casualty situation following a terrorist attack in a different site, therefore capable to testify if those theoretical measures can translate into effective practical responses. All the three participants, two of them from UK and one from Croatia, described the response as well-coordinated at all levels. The Croatian hospital reports also that the facilities itself was exposed to a direct attack, with 4 personnel killed.

A couple of other UK hospital reported to have received various threats in the past, that didn't turn into real attacks:

> *"We have had numerous bomb threats and other terrorism threats which have likely been from individuals not capable of posing actual risk. Police dealt with all incidents"*

> *"Telephone bomb threat made to hospital"*

The occurrence of cyber terrorism among EU Hospital seems to be quite relevant, as result shows a percentage of about 30% of responders who did experience network branches. Almost all EU Hospital interviewed report the implementation of specific precaution to enhance cyber and information protection (CIIP); this in concurring with the findings of WP1 indicating a prioritization by some states to focus upon CIIP.

Our results show also that the emergency/crisis plan is frequently tested, although in many EU MS the exercise rarely involve terrorist attack, as testified by the following comments from two Danish Hospitals:

> *"Training and awareness is regardless type of event but we have never trained a terrorist attack on the facility"*
>
> *"The Danish hospitals are not so involved with handling terrorist attacks. Preventive measures are directed against more probable disasters such as power outages, heavy rain, handling many patients, coordination with municipalities etc."*

Moreover, in less than half of cases (47%) security personnel receive specific training on how to recognize and respond to suspicious activity, including unidentified packages and persons exhibiting suspicious behaviour.

On the contrary, other EU MS such as UK, are quite attentive towards terrorism and specific training is provided to security personnel and medical staff. A number of initiative have been developed to train Health Service and Hospitals in respect of terrorist attacks, such as Project Argus: a multimedia simulation created by National Counter Terrorism Security Office (NaCTSO) and delivered by Counter Terrorism Security Advisers (CTSAs) throughout the UK that aims to raise awareness of the threat from terrorism. One of the UK Hospital interviewed has previously participated to this program, simulating a: "*Terrorist attack on a crowded place and a single gunman within the hospital*". Other UK hospital training experience involved "*multiple bomb attacks in the city centre*", "*chemical and shooter attacks*" and "*Marauding Terrorism and Firearms Attack (MTFA)*".

The role of training and exercise of hospital staff aiming to test and improve the emergency/crisis plan seems to be therefore well known and well utilized, as very often hospitals use outcomes of those exercise to revise the emergency/crisis management plan, in addition to guidelines provided at international/national/local level.

The majority of hospitals describe a series of factors representing barrier on crisis management capability: most important point of weakness seems to be financial shortcoming, indicating that hospitals are constrained by the availability and capacity of existing resources required for their preparedness regarding the management of threats. In the majority of hospital interviewed, the security budget comes mainly from internal financing, whereas few hospital manage to obtain funds from external

public sources, such as the state, the region or the municipality. Previous studies have reported the importance of financial resources in hospital disaster preparedness (Sauer et al, 2009); as a matter of fact, financial issues can highly affect hospital preparedness. To this regard, participants underline the fact that less than 5% of the hospital budget is actually spent on security, as well as on crisis management, with a global absence of increase of the security budget in the last 5 years.

Another important point is that security frequently represents a low priority subject when compared to other issues. Some of the comments written by participants report:

> *"The health care organization is slim. There is much that needs to be given priority in health care, therefore it is difficult to release staff to attend even a course."*
>
> *"Hospital site management tend to take all resilience issues seriously however, they need to compete with everyday high pressure operational issues."*
>
> *"Releasing key clinical staff is impossible due to pressures of work at the hospital"*

In this case, as the second comment explains pretty well, 'Low Priority' does not necessary mean 'Low Interest' by the hospital management: even if EU Hospitals do have documented and functional preparedness plans, are willing to provide specific preparedness education/training and generally encouraging key personnel to participate in conferences about emergency/crisis management, daily workload frequently exceeds the staff possibilities to be adequately prepared for extra-ordinary events. Nonetheless should be underlined that providing education and awareness does not necessary imply the participation at large scale conferences or time consuming exercises. As an example, the so call on the job training (OJT), taking places during normal working hours, could be a good and inexpensive solution, with a very low operational and business impact; awareness could be included as part of shift change briefing and brief lectures could be delivered in staff rooms during break-times.

Lack of standard preventive information or guidance on vulnerability reduction plays also a role: few hospital can rely on the presence of counterterrorism guidelines. This

was also underlined by the results of WP1, together with the lack of a common standard and measure of performance.

Limitations

To synthesize the state of the art of threat assessment, existing crisis management plans, exposure consciousness and risk perception of EU hospital as CI against terrorist attack, our survey has been addressed to a high number hospital disaster coordinators, security managers and resilience officers in various EU hospitals. However, provisional results are based on feedbacks obtained by only forty-seven responders. This lack of response can be correlated with various factors, among which we underline the difficulties to recognize and get in contact with responders in smaller EU States (such as Malta and Luxembourg) and the lack of feedback from many potential participants due to security concern regarding sharing of sensitive data. Thus, provisional results may not be entirely representative for the actual situation within the EU Health sector in respect of terrorist attacks.

Other limitation can include the so called “response bias”, meaning that some factors may have affected participants during the process of responding to surveys, influencing they responses. Those bias may emerge when individuals aim to present themselves in a favourable light and want to keep a consistent and rational image of themselves; or it might help them to complete the survey quickly and efficiently by simply "copying" their previous answers (Peer E, 2011).

Moreover, although the research team attempted to reach the most appropriate target group by trying to identify disaster coordinators and responsible for hospital resilience, it is not possible to ensure that all responders had enough knowledge to answer all questions in the most accurate way.

Suggestions

Further studies can be done in order to better understand the role of hospitals and their efficacy during the response to terrorist attacks, in terms of command and control and cooperation with stakeholder agencies. Even though the majority of hospitals asserted to have an emergency plan, it was rarely designed or tested against the terrorist threat; therefore, it is still unknown how they are likely to respond and cope in the event of different terrorist attack.

5. Conclusions

The majority of the hospitals interviewed claimed to be recognized as CNI, even though only a moderate per few of them actually come from EU MS who include Health Sector in CIP policies. Globally, the need to implement security measures and protocols to cope with the consequences of terrorist attack is generally well-recognized and managed; nonetheless, limited or no information is provided by the government on how to reduce hospital vulnerability to terrorist attack. Little evidence was provided on what, if any, intelligence is shared between security organizations and the health care system regarding threat , capability and intent of terrorist activity.

Emergency/Crisis plan is present in almost the totality of hospitals, and it is frequently tested, though it is not often promulgated to stakeholder agencies and reviewed only in a moderate percentage of cases. Even though hospitals generally have ongoing emergency training programs, these rarely involve terrorist attack; moreover, lack of funding, low priority and poor knowledge and competencies of personnel are appointed as the main barriers on crisis management capability. There was little evidence of a dedicated counter terrorist management function or structure within the health care systems.

There was little or no health care specific guidance or directives regarding vulnerability reduction of terrorist attacks to hospitals.

There was limited awareness of the inventory of CBRN substances held within hospitals and the protection arrangements to prevent these being utilized for terrorist attacks either within or outside the hospital.

6. References

Djalali A, Della Corte F, Foletti M et al. Art of Disaster Preparedness in European Union: a Survey on the Health Systems. PLOS Currents Disasters. 2014 Dec 17. Edition 1

European Commission (1989) *Council Directive on the minimum health and safety requirements for the use by workers of personal protective equipment at the workplace.* Available from: www.europa.eu/legislation_summaries/employment_and_social_policy/health_hygiene_safety_at_work/c11117_en.htm

European Commission (2004) *Communication from the Commission to the Council and European Parliament: Critical Infrastructure Protection in the fight against terrorism.* Brussels: European Commission. Available from: www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:**2004**:0**702**:FIN...

European Commission (2004) *Communication on Critical Information Future EuropeInfrastructure Protection (CIIP),"Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience"*. Available at: www.ec.europa.eu/digital-agenda/en/news/policy-critical-information-infrastructure-protection-ciip

European Council (2008) *Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* Brussels: Official Journal of the European Union.

European Commission (2012) *Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP).* Brussels: European Commission. Available from: www.ec.europa.eu/dgs/homeaffairs/pdf/.../epcip_**swd_2012_190_final**.pdf

European Union (2014) *Terrorism Situation and Trend Report (TE-SAT).* Available at: www.europol.europa.eu/content/te-sat-2014-european-union-terrorism-situation-and-trend-report-2014

Ganor, B. and Wernli, M. (2013) International Institute for Counter-Terrorism (2013) *Terrorist Attacks against Hospitals Case Studies.* [s.l.]: ICT. Available from: www.ict.org.il/Article/77/Terrorist%20Attacks%20against%20Hospitals%20Case%20Studies

Linstone H, Turoff M. The Delphi Method Techniques and Applications. ©2002 Murray Turoff and Harold Linstone. Available from: http://is.njit.edu/pubs/delphibook/delphibook.pdf

Peer E, Gamliel E. (2011) Too Reliable To Be True? Response Bias as a Potential Source of Inflation in Paper-And-Pencil Questionnaire Reliability. Available from: http://pareonline.net/getvn.asp?v=16&n=9

Sauer LM, McCarthy ML, Knebel A, Brewster P. Major influences on hospital emergency management and disaster preparedness. Disaster Med Public Health Prep. 2009;3(2 Suppl):S68-73.

WHO (2011) Hospital emergency response checklist: an all-hazards tool for hospital administrators and emergency managers. Available from: http://www.euro.who.int/__data/assets/pdf_file/0008/268766/Hospital-emergency-response-checklist-Eng.pdf

Appendix A

THREATS
Terrorist attacks on Hospitals:
Risk & Emergency Assessment, Tools & Systems

THREATS: Terrorist attacks on Hospitals: Risk and Emergency Assessment, Tools & Systems

Co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union

Hospital emergency/crisis management plans for terrorist attacks

Consent Form

Dear Madam/Sir,
You are invited, because of your knowledge and expertise, to take part in the study "*THREATS - Terrorist attacks on Hospitals: Risk and Emergency Assessment, Tools and Systems*". The study has been approved by the European Commission, under the program CIPS. Please see our Web site www.threatsproject.eu .
Your answers will assist our project to deliver the risk reduction toolbox we are developing to protect Hospitals in the European Union from terrorist attacks outside or inside the hospital.
Taking part in this survey is completely voluntary; information provided will be safeguarded, secure, anonymous, and reputational issues managed. You can withdraw from the study whenever you like. The survey will take about 30 minutes to complete.
In case you agree to contribute to study, please, confirm your consent.
Statement of Consent:

□ *I consent to contribute in this study and answer the survey*
□ *I don't consent to contribute in this study*

Name and Surname:_____
Position:_____
_____
Gender

How many years is your work experience in hospitals?

Academic education level: PhD ☐ MD ☐ MSc ☐ BSc ☐

Field of education: Medicine ☐ Nurse ☐ Health management ☐ Other (please, specify):….

Hospital:_____

_____

- Private for profit
- Private non for profit
- Public
- University Hospital

Country:_____

_____

City:_____

_____

Table of contents

Definitions

Critical Infrastructure: processes, systems, facilities, technologies, networks, assets and services
essential to the health, safety, security or economic well-being of the State and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence.

Personal protective equipment (PPE): refers to protective equipment(clothing, helmets, goggles, or other garments) used as barriers between a person and a hazard.

General Framework

1. To the best of your knowledge, does your country/region have a national or local threat level indicator for terrorist attacks?

- Yes
- No
- Do not know

If yes, is it a National or Regional warning system, and how is it circulated/updated?

- National
- Regional

2. Is the Health Service or Hospital designated as part of the Critical Infrastructure of your country/region?
- Yes
- No
- Do not know

If yes, how is it categorized?

3. Is there a specific threat indicator/level for terrorist attacks for the Health service/Hospital Nationally or Regionally?
- Yes
- No
- Do not know

4. Is the Health service/Hospital provided with information/guidance on how to reduce its vulnerability to attack or the consequences of an attack outside or inside the hospital?
- Yes
- No
- Do not know

If yes, what guidance/tools are provided and by whom?

5. Is the Health service/Hospital provided with security intelligence regarding terrorist threats?
- Yes
- No
- Do not know

If yes, who provides this information and who receives the information?

6. Is there a manager within the Health Service/Hospital who is responsible for managing the threat and risk of terrorism?
- Yes
- No
- Do not know

If yes, what is their job title/responsibility?

_____
_____
_____
_____

7. Which protective measures has your Health service/ Hospital implemented to reduce the threat or consequences of a Terrorist attack outside or inside the hospital?

_____
_____
_____
_____

8. What funding is available to your Health service/Hospital to reduce the vulnerability or consequence of a terrorist attack?
   - National/Regional funding
   - No funding
   - Do not know

9. What inspections/checks are made of the Health service/Hospital to assess the vulnerability and consequences of a terrorist attack outside or inside the hospital?

_____
_____
_____
_____
_____
_____

10. What training and awareness in the Health service/Hospital has taken place regarding the threat, vulnerability and consequence of a terrorist attack on the facility?

_____
_____
_____
_____
_____
_____

Emergency/Crisis management Plan

11. Does the hospital have an emergency/ crisis management plan?
   - Yes
   - No (skip to question 24)

12. How often is the emergency/crisis management plan revised?
   - Never
   - Once a year

- Other (specify)

_____
_

13. Did the hospital refer to any guidelines to write/revise the emergency/crisis management plan?

- Yes, regional or local guidelines
- Yes, national guidelines
- Yes, international guidelines
- Yes, other medical facilities guidelines
- No

If yes
(specify)_____
_____

14. Did the hospital rely on a private sector/agency to manage and develop the emergency/crisis plan?

- Yes

(Specify)_____
_____

- No

15. How often does the hospital test the emergency/crisis response plan (Full-Scale Exercise, Mock Disaster Drills, Tabletop Exercise, Functional Exercise, etc.)?

- Never been tested
- Once a year
- Other
  (specify)_____
  _____

16. Are the test results reviewed and evaluated to identify strengths and areas for improvement?

- Yes
- No

If yes, what improvement where made in the past?

- additional security measures
- security equipment upgrades
- changes in policies and procedures
- others
  (specify)_____

17. Is there a mechanism for monitoring the continuous correction of gaps that were identified in the exercises?

- Yes
- No
- Do not know

18. Does the emergency/crisis response plan specifically address each of the following types of attacks?
- Biological
- Chemical
- Nuclear/Radiologic
- Incendiary/Explosive
- Shooting
- Cyber terrorism
- Other
(specify)_____

19. Which of the following entities does the hospital's plan specify contacting in the context of terrorism incident?
- Emergency Medical Services (EMS)
- State or local public health department
- State or local law enforcement
- Fire Department
- Other hospitals/local hospital association
- Disaster-response agencies
- Other
(specify)_____
_

20. Is the emergency/crisis management plan promulgated to other stakeholder agencies?
- Yes
- No

If yes, who else needs to know the plan?
_____
_____
_____
_____

21. Which of the following are included in the hospital emergency/crisis plan? *Mark all that apply*
- Definition and integration of the hospital's role in community wide planning
- Designation of an Emergency Management Team
- Each area of the hospital have department-specific actions or roles to fulfill in the event of emergency response
- Communication of hospital status, requests for assistance and supplies, to the local Emergency Operations Center and other area hospitals
- Business continuity
- Outlying hospital to accept inpatients during a declared attack
- Rapid increase of supplies, equipment and personnel in case of terrorist attack

22. Which actions are considered in respect of the safety of staff, patients and other inhabitants in case of a terrorist attack to hospital? *Mark all that apply*

- Area of safe refuge
- Procedure for sheltering-in place
- Lockdown procedures
- Complete evacuation
- Partial evacuation
- Others

Previous experiences

23. Has the hospital ever experienced a mass-casualty situation following a terrorist attack in a different site?
- Yes
- No (skip to 32)

24. Did the hospital use a written disaster plan to face the event?
- Yes
- No

25. How would you describe hospital operations in that occasion?
- Chaotic and poor coordinated
- Somewhat coordinated
- Well-coordinated at every level

26. In that occasion, which of the following measures were needed/implemented by the hospital?

Back-up plans to accept casualties if all beds were occupied	○ Needed ○ Not needed	○ Implemented ○ Not Implemented
Continuity of the essential services	○ Needed ○ Not needed	○ Implemented ○ Not Implemented
Partial/complete evacuation	○ Needed ○ Not needed	○ Implemented ○ Not Implemented
Stockpiling drugs and medical supplies	○ Needed ○ Not needed	○ Implemented ○ Not Implemented

27. Was the hospital self-sufficient in terms of back-up energy, water and food supply?
- Yes, completely
- Yes, but not completely (*Mark all that apply*)
  - water
  - electricity
  - food supply
- No

28. Did the hospital consider it may be a secondary target and activate appropriate security precautions?

- Yes
- No

29. Has the hospital ever experienced any network breaches (malware,..)?
- Yes
- No

30. Has the hospital ever experienced at least one known data breach in the past five years?
- Yes
- No

31. Is there any other experience of terrorism or other serious event that they are willing to share with us?

_____
_____
_____
_____

Training, Exercise and Testing

32. Does your facility have ongoing emergency management training and education programs?
- Yes
- No

33. Does the hospital use any of the following to train personnel and improve the response against emergencies? *Mark all that apply*
- Tabletop exercise
- Full-scale reharsals
- Face-to-face training, lectures, presentations
- Online training module (e.g Mooc)

34. Has the hospital participated in any internal or external simulation/exercise in response to terrorist attack?
- Yes
- No

If yes, what kind of attack was simulated?
_____
_____
_____

35. Did the hospital ever participate in any national level exercise program?
- Yes

(specify)_____
_____
- No

36. What measures are implemented by the hospital to encourage/promote awareness of emergency procedures?
- Program of continuing education
- No education
- Others:

_____
_____

37. Have key personnel in the hospital been trained in how to implement a formal Incident Command system?
- Yes, all of the key personnel received a specific training
- Yes, a certain percentage of key personnel received a specific training (specify the percentage)

_____
- No

38. Does the hospital provide training on how to recognize and respond to suspicious activity, including unidentified packages and persons exhibiting suspicious behavior?
- Yes
- No

39. Who receives this type of training?

_____
_____
_____
_____

Security Measures and Equipment

40. Which activities and precautions are adopted to improve hospital safety? *Mark all that apply*
- access to the sensitive area of the hospital restricted to authorized personnel only
- alarm system to detect unauthorized entry or attempted entry at critical components
- specific training of security personnel, including the proprietary security force, contractual security personnel, off-duty law enforcement officers
- gate control system to control the access of vehicles
- closed circuit television cameras with record and archive capability
- screening of visitors who seek to enter the hospital after regular visiting hours, monitoring center
- suggest screening of visitors in normal visiting hours

41. Does the hospital use a security assessment framework to assess physical facilities?
- Yes
- No
- Do not know

If yes, how often do security assessment of physical facilities conducted?
- More than once a year
- Once a year

- Other
  (specify)_____
  _____

42. Does the hospital have a backup radio system the emergency rooms (ERs)?
- Yes, in all ERs
- Yes, but only in a dedicated area of ERs
- No radio system is present

43. In order to sustain communications with the local emergency management agency, have special modes of communication (i.e., VHF radios) been established?
- Yes

(Specify type of communication)_____
- No

44. Are the special modes of communication tested periodically?
- Yes

(Specify frequency)_____
- No
- Not sure

45. Which of the following precautions are adopted regarding Cyber and Information security?
- Each employee has an individual account with a unique username and password
- Restricted unauthorized access to the network
- Monitored network activities for unauthorized use
- Patient confidential information management
- Internet firewall software and virus protection are installed on every computer
- Physical locks on devices and their communication ports to prevent tampering
- Routine and periodic evaluation, including updating security patches and disabling all unnecessary ports and services
- Secure connection to the Internet
- Development and evaluation of strategies to maintain critical functionality during adverse conditions

46. Which of the following precautions are taken regarding personnel working in the hospital?
- when hiring personnel, background, employment eligibility and professional references are appropriately verified according to standardized guidelines (eg. "*A good practice guide on pre-employment screening- Document verification*")
- the hospital provides identification badges to all employees and volunteers
- when terminating employment, employees are required to turn in photo IDs, keys, access codes, and other security-related items

47. Do personnel have a checklist to use for threats or suspicious calls or to report suspicious activity?
- Yes

- No

48. What is the procedure for reporting suspicious activity and to whom?

_____
_____
_____
_____
_____
_____

49. Does the hospital stockpiles PPE against CBRN (Chemical, biological, radiological and nuclear) threats?
- Yes
- No

50. Did hospital personnel receive specific training in proper use of PPE?
- Yes, all the hospital workers received a specific training
- Yes, but only some key personnel received a specific training
  (specify)_____
  _____
  _____
- No

51. Is the hospital equipped with decontamination facilities?
- Yes
- No

Barriers and facilitators

52. What are the main barriers on crisis management capability? *Mark all that applies*
- Low priority
- Lack of senior management buy-in/direction
- Poor Knowledge and competencies of personnel
- Financial shortcoming
- Lack of standards and guidelines
- Legal issues
- Others
  (specify)_____

53. Where does the security budget come from?
- Internal financing
- External financing (state/region/municipality)
- External financing (private entities)
- Both internal and external financing

54. What percentage of the hospital budget is spent on security?
- Less than 5%
- 5-10%

- More than 10%
- Do not now

55. What percentage of the hospital budget is spent on crisis management?
- Less than 5%
- 5-10%
- More than 10%
- Do not know

56. Did the security budget increase in the last 5 years?
- Yes
- No

57. How high a priority is hospital security to top management or directors?
- Not a priority
- Low priority
- Neither high nor low priority
- High priority
- Very high priority

58. Which of the following applies to your hospital/region?
- Presence of counterterrorism guidelines in the region
- Encouraging key personnel to participate in conferences about emergency/crisis management
- Hospital personnel include people with any knowledge/training in the field of terrorism response or mass casualty events