"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

An Analysis of Risk Management Measures for the Protection of Critical National Infrastructure: An Examination of National Level Risk Management and Vulnerability Reduction Programmes Within European Union Member States

Version: 1.0

Date: 09 Jan 15

Authors: CD, SC

Approved by: CA

Table of Contents

Executive Summary

The field of critical infrastructure protection (CIP) is complex. The sectors that constitute national infrastructure are diverse, from finance and government to energy and water suppliers. Although many of the sectors that make up the national infrastructure are very different and owned and operated by independent companies, there is evidence to suggest they are connected in ways that are not immediately obvious, otherwise known as 'networked' infrastructure. Networked infrastructures incorporate a level of interdependency, described by Stapelberg (2008:22) as the 'bi-directional relationship between multiple different infrastructures'. The human element further complicates the field on two levels: the perception of risk will differ according to profession, experience and area of operation and expertise; and the impact of CIP failure upon the population and the potential quickly to degrade civil order and societal function provides a compelling interdependency between all sectors and the population.

This report has touched upon collaboration between stakeholders and illustrates some examples where joint effort between nations has helped to establish an effective partnership, particularly in the field of Emergency Response. More collaboration in all areas of CIP from policy writers to service providers has the potential to enable better working practices, improving the standard of protection overall and reducing the vulnerabilities that exist in nations which have a less developed CIP programme. There are challenges that will need to be addressed such as cultural differences and the perception of a North/South divide within Europe, if the development of a European Union level CIP programme is to gain traction.

Much of national infrastructure is provided by private business and public-private partnerships (PPPs) are becoming more common, but governments must ensure the private sector continue to meet the needs of the nation whilst legislation allows sufficient freedom of movement for private businesses to remain competitive. This encourages private companies to continue to invest in the delivery of their service, ensuring financial and human resource are utilised in a cost effective and competitive way and the specialist workforce are invested in to ensure the business matches developing technology to provide the service/product in the most efficient way. The business remains profitable and the infrastructure is assured.

Risk management is a core component of CIP that needs to be an ongoing process, as opposed to a one off. In many industries a risk assessment process conducted periodically, often annually or every 2-3 years, is sufficient to manage the risks within that area because many of the hazards and threats are constant. The field of CIP is different because the hazards and threats are less constant and the perception of risk alters as more knowledge relating to the sector or the hazards and threats is developed.

The THREATS research has identified 13 of the 28 European Union (EU) Member States (MS) that list Health as a sector of Critical National Infrastructure (CNI) but research has not provided clear evidence to illustrate how the risks are managed within the sector. THREATS has established three critical pillars that forms a baseline to develop the project further: physical protection of buildings and assets; security of people and protection of data and information. Evidence has been provided throughout the main body of this report to illustrate the general risks to the Health Sector; further detailed hazard and threat analysis will be conducted as part of Work Package 1 of the THREATS project. Each of the critical pillars has been discussed in order to validate the pillar and provide evidence of vulnerability and the potential impact to Health infrastructure.

A review of publically available literature written in English was conducted to support this research. The review identified limited data relating to Health as part of CIP, observations were also made of other CNI sector publications that often referred to other sectors, such as the European CII Newsletter that has published 17 issues and often mentions the Financial or Energy Sectors but has never mentioned Health. The literature review follows on from the work conducted for deliverable report 1.1 (D1.1) and provides additional confirmation that data is not available in a common language within the public domain that provides evidence that EU MS are developing their national CIP programmes and contributing towards a collective EU CIP plan.

It is conceivable that MS are reluctant to publish CIP related information due to matters of national security but the tension between public-private information sharing need not exist. The details relating to specific operational matters should be protected accordingly, the strategic/policy information does not undermine operational effectiveness but provides interested parties, including researchers and the public, assurance that measures are in place to manage and protect CNI.

The literature shows CIP to be disjointed across the EU with different protocols, methodology and a variety of terms and definitions. A concerted effort is required to develop commonality between MS, in a way that is sensitive to cultural and other issues that could be a barrier to greater coordination. The changing terrorist threat, or New Age Terrorism, provides a cogent case for better measures to protect CNI. All sectors have vulnerabilities in some form or other, whether it is a physical vulnerability at an isolated location or the vulnerability resulting from network interconnectedness or interdependency. Those vulnerabilities and interdependencies seldom stop at national boundaries but have the potential to ripple from one MS to another throughout the EU.

Emergency planning has had to develop quickly to catch up with the broad spectrum and scale of potential scenarios and events throughout the world in order to plan effective contingencies and responses to natural and man made emergencies. Fischbacher-Smith and Fischbacher-Smith (2013) provide some context to the efficacy of developing resilience within the Health Sector with the terrorist threat in mind. The potential impact of an attack against a hospital could be significant within the Health Sector but could also impact across sector and national boundaries.

There is a clear need for a more coordinated or joined up effort within the field of CIP. Collaborating on matters that have regional, national and international equities will be challenging and working towards a common language, standardised practices and a useful measure of performance will undoubtedly be difficult. However the successful use of international standards such as ISOs proves the utility of standardisation and recognition that an organisation is performing and has been accredited to an agreed set of criterion that are widely recognised.

The THREATS project is constrained by time and financial budget so the team have adopted a flexible research approach, information will be presented in regular deliverable reports throughout the project and readers are encouraged to engage with the research team at www.threatsproject.eu or via the LinkedIn page with any contribution they may have. Additional data will be reviewed and deliverable reports will be updated as necessary to ensure the project presents as accurate a picture of the Health Sector and hospitals as part of CIP as possible, which will inform the final THREATS project.

1. Introduction

1.1 Risk Management in CIP

In any business or organisation there will always be challenges when trying to identify which function or parts of a function have the highest priority or are most critical to the operation. This topic was discussed in D1.1 of the THREATS project and identified the sectors that are common to most Critical Infrastructure Protection (CIP) policies within the European Union (EU) as:

Communications

Emergency services

Energy

Financial Services

Food

Government

Health

Transport

Water

These sectors are common to most CIP programmes within the EU and are reflected in other CIP policies globally (Brunner and Suter, 2008). However, the sectors are diverse and are likely to have different threats affecting them; the level of accepted risk is likely to be different across a sector and the variety of sector elements or parts that may be vulnerable to specific threats at a specific time will be vast. The complexity of risk management within CIP is further complicated by the human element: risk perception is likely to differ at the policy maker/ academic level and the operator/service provider level. Furthermore the networking of infrastructures or the 'bi-directional relationship between multiple different infrastructures' introduces greater interdependencies, whereby networked systems can be 'mutually supportive' but also a 'failure of one may exacerbate the load placed upon another' (Stapelberg, 2008:22).

1.2 Collaboration

The literature relating to risk management is great, however the detailed risk management and vulnerability reduction literature relating to CIP is far smaller. That is not to say that it

does not exist, in fact the THREATS research team have already identified that CIP work is underway across the EU, but the level of coordination between nations is less clear and the availability of data written in English within the public domain is limited. However evidence now exists of collaborative efforts between European countries and EU MS when managing the response to civil emergencies within Europe and further afield, such as the Civil Protection Network (CIVPRO).

CIVPRO is one example of collective effort between multiple nations to share information; agree best practice, operating guidelines and standards and share the burdens associated with maintaining a capability at high readiness and the financial impact of initiating costly operations. CIVPRO is part of the Council of Baltic Sea States; membership includes the 11 States of the Baltic Sea Region and the European Commission. The council encourages wider participation and there are currently 10 countries with observer status, including the United States of America (USA) and the United Kingdom (UK).

The EU has an emergency response system similar to CIVPRO. The Civil Protection Mechanism is supported by all EU MS and includes membership of non-EU States: Iceland, Norway and Macedonia. The mechanism helps to coordinate the response to civil emergencies within Europe and worldwide, responses to serious events in recent time (see D1.1) have illustrated the benefit of joint effort coordinated through a single organisation.

1.3 Geographical Divisions within the EU

The effectiveness of multinational joint effort in the field of emergency response is encouraging yet the appetite to share effort in the field of CIP remains elusive. Bremberg and Bitz (2009: 290) suggest there is a ‘North – South divide’ in Europe with Northern member states (such as Netherlands, Sweden and UK) taking contradicting views on the development of EU civil protection to the Southern member states (such as France, Greece, Italy and Spain). According to the research cited by Bremberg and Britz the Southern European states are keen to develop a more prominent role for the European Commission to deal with EU civil protection but conversely, the Northern states are content with allowing the EC a limited role to deal with the ‘soft’ security issues in the EU, and are ‘reluctant towards further integration and stress the importance of keeping cooperation on an intergovernmental basis’. Maniati (2012) observes the Southern states to be more prone to

'natural catastrophes (earthquake, floods)' and 'vigorously strive' for EU integration, whilst the Northern states are more 'affluent and much more well prepared on the subject'.

1.4 Commercial Market

Cultural and national identity issues will no doubt cloud the EU CIP debate but the commercial aspect of the discussion must not be overlooked. The field of CIP is no longer a State or government monopoly as more services are provided by private organisations, from power to telecommunications suppliers. These organisations are commercial entities with a primary remit to make a profit for the company and shareholders and therefore the commercial aspect will often take precedence as described by Lazari (2014:8):

> In the field of CIP, most of the time, the concept of what is acceptable and what is not is tied to the variable of cost-effectiveness. The cost-effective variable of acceptability of risks characterises, in particular, those critical infrastructures that are not owned and operated by a government and, for this reason, run the business for profits (e.g. Banks, transport companies, internet service providers, telecommunication providers, etc.). The privately owned infrastructures, during their risk evaluation processes, used to take business-driven decisions that include the lack of commitment where they perceive an 'uncontrolled' waste of financial resources, e.g., in the field of security, that may not bring any benefit to the business continuity, while in fact, may seriously affect their competitiveness on the global market.

Lazari draws attention to the theory that National Infrastructure being owned and operated by private organisations is likely to be managed as a commercial concern, the decisions are likely to be business-driven and the priority will be for profit, unless legislation is sufficient and effective to manage the growing private sector of National Infrastructure.

The Health Sector in 24 of the EU MS is predominantly State owned and operated, although in Belgium, Cyrus, Luxembourg and the Netherlands the majority of healthcare is provided by the private sector (Chevalier and Lévitan, 2009:76). The distribution of State and privately owned hospitals across the EU is beyond the scope of this report but the presence of the private sector within the Health Sector must be considered, this is particularly important as the private health sector grows:

> With the exception of some Member States such as France and Spain, where the private sector's share in terms of hospital care capacity has remained relatively stable since the 1980s, the role of the private sector hospital care is increasing in the

> European Union.
> (Chevalier and Lévitan, 2009:76)

CIP is undoubtedly a field with public and private equities that will require careful coordination and management to ensure CNI is maintained at the optimal level and all stakeholder needs are represented appropriately.

1.5 Common Standards

Pragmatically there might be a case for a centralised body to regulate and direct EU CIP. Politically this may be a step too far for some MSs but embracing recognised standards and standardising practices within each of the infrastructure sectors could be a useful step towards improvements in the EU and provide better coordination when managing interdependency vulnerabilities. Newsome (2014:5) discusses the management of security and risk, explaining that some 'dissatisfaction' within the field has 'prompted more standardization, in the hope that many competing and loosely defined ways in which people manage security and risk can be replaced by the best ways'. Newsome further states:

> Standardization is the process of defining standards for behaviour and understanding. Standards describe how concepts should be understood and how activities should be performed. Standardization certainly helps interoperability and accountability and may replace inferior practices with superior practices.

Standardising practice and using a common system to measure performance within the field of CIP would take much effort and coordination but the benefits to all MS could be significant. However practices and procedures become deeply embedded within an organisation to form cultures, especially when the practice has been effective over an enduring period of time. There are also potential problems in governments or large organisations with multiple departments where different standards are used, the differences can 'interfere with coordination, and some standards can be inferior, not just different' (Newsome, 2014:6). Although Canada is outside of the EU it would be remiss of the research team to ignore good examples of CIP management. The Risk Management Guide for Critical Infrastructure Sectors (Public Safety Canada) provides a policy directive that manages the different perceptions and approaches to risk management across a field of divergent agencies and businesses. The policy addresses the issues of standard practice and common language in a narrative that is unambiguous and easy to follow. Standardisation is one area where the politically sensitive nature of trying to work across MS

borders is thrown into sharp relief: a degree of standardisation that may be desirable for purely organisational reasons but may not be acceptable to all MS.

1.6 Managing the Risk

Infrastructure assets vary in criticality that may be measured along various metrics in order to decide how to manage the risks to those assets (Centre for the Protection of National Infrastructure). A pragmatic approach in a world of limited resources demands that criticality be estimated and a threshold set for those assets that will be accepted as being critical. Within a sector, the level of risk may not be constant as threats and hazards often change, therefore risk management needs to be flexible and able to adjust to the changing risk landscape in order to remain proportionate and cost effective as described by Stapelberg (2008:24):

> The analysis of vulnerability in infrastructure systems is a major input to the risk assessment that must be performed to establish critical infrastructure protection priorities. Comparison of protection options is complicated because of uncertainty, as the vulnerabilities of infrastructure systems are not necessarily constant... dealing in uncertainty requires using probability estimates. If probabilities are used (e.g., the probability of a given type of intentional hazard, or attack on an installation's vulnerability), they typically cannot be obtained from empirical frequency distributions as events are uncommon or hypothetical. Instead, the probabilities must be derived using a combination of modelling, gaming, and analysis; all with a good deal of subjectivity. Further, the probabilities should change over time as knowledge of infrastructure systems interdependencies and their related vulnerability to risks induced by natural, technological, as well as intentional hazards improves.

Identifying the level of importance placed upon the Health Sector remains a challenge for the THREATS team because detailed data is not readily available within the public domain. Some EU MS CIP strategies do list Health as one of the sectors that forms the National Infrastructure and in some cases hospitals, medicine and vaccine production and storage are listed as the key components of the sector. It is problematic, however, trying to comprehend how the risk to the Health Sector is managed. In a MS this management may be across a network of hospitals that present a variety of risks common to the network in addition to specific risks relating to the local demographics and geography. In some MS, such as the UK, hospitals form a tiered delivery of service to the public. Tiers can vary from

outpatient or non-emergency treatment at small community type hospitals to larger hospitals that deliver a wide range of services, including trauma or acute care. The UK model includes Regional trauma centres that have high capacity in terms of available specialist care beds and high capability or immediate access to specialist diagnostic equipment (NHS). Regional trauma centres are usually sited close to main road transport infrastructure such as motorways and close to high density of population, for example Kings' College Hospital, London. This model is not unique to the UK but is common to other EU MS; research has identified acute trauma centres and general hospitals located close to centres of dense population and transport infrastructure, such as the Robert-Bosch-Krankenhaus in Stuttgart, Germany and the AKh in Linz, Austria.

The THREATS research has now identified 13 of the 28 EU MS that make any reference to Health as a sector of national infrastructure. In some cases translation difficulties were a barrier to gaining a deep understanding of CIP and indeed Health as a sector of CIP in a given country. The findings reported in D1.1 recorded any reference to CIP as a positive result, even though detailed data was not available. The difficulty with researching CIP management remains, in the absence of documented data that is written in a common language and accessible to the research team. Attempting to conduct deeper research into a specific sector, such as Health, will inevitably present challenges. The research team plan that as the project progresses and becomes more widely known within the Health Sector, practitioners and other experts will participate in developing the body of knowledge that will inform the final output of the project.

1.7 Critical Pillars

In the absence of a defined Health CIP strategy in the EU this report will propose specific areas for consideration that can be developed throughout the THREATS lifecycle. As stated in D1.1, THREATS is intended to be progressive and cumulative by building upon what is currently known and developing the body of knowledge. Existing information not previously identified by the research team will be included in the subsequent research tasks or in some cases added to a written report, to ensure what is presented is as complete as reasonably practicable within the scope, financial and time constraints of the project.

In order to establish a frame of reference from which to develop CIP within the Health sector THREATS has identified 3 critical pillars:

Physical protection of buildings and assets

Security of people

Protection of data and information.

The literature relating to physical protection of buildings and assets is extensive (see Atlas, 2013; CPNI: Physical Security; RIBA, 2010 and Whole Building Design Group, 2014). During the last decade there have been significant technological and procedural advances in physical security in response to the changing global terrorist threat, particularly in the aviation transport industry. The aviation industry has experienced direct terrorist attacks to airport buildings, such as the attack at Frankfurt Airport in 1985, Glasgow Airport in 2007, Domodedovo Airport 2011 and the recent attack at Karachi Airport in 2014, these have forced governments and airport authorities to develop security measures that may reduce the risk of terrorist attack, without disrupting business activity. Creating sterile areas or buffer zones where public transport interfaces with the building, such as drop off and pick up points, has reduced the likelihood of a 'ram raid' type attack such as the Glasgow incident. Other measures have been implemented to 'harden' the building super structure such as toughened glass that can withstand a certain level of direct and blast impact (Dolan, 2001:74-79). Security surveillance, screening of passengers, control of access and other procedures have been put in place to form a layered security plan whereby no single measure will defeat the threat but consecutive layers of security further reduce the level of risk or at least make attack planning and execution more difficult for the terrorist.

The development of protective security measures to protect the most critical elements by the implementation of a hierarchy of measures is now common in protecting infrastructure, data and people. Many of the measures and practices implemented throughout the aviation industry are now reflected in the wider commercial world and airport style measures are commonplace in many corporate establishments such as Canary Wharf in London. The Canary Wharf estate operates a comprehensive security strategy where vehicle access is controlled by manned check points, services and deliveries are separated from the public areas and managed in a controlled space, visitors to buildings are screened and access is controlled to reduce the risk of unauthorised access. The estate has a baseline level of security that is flexible and responds to the national alert state or to specific threats and can be increased or decreased accordingly. The security is carefully managed to ensure the customer/tenant expectation and experience is managed appropriately (Flenley, 2003). Many other commercial venues, such as large shopping centres, throughout the EU have adopted similar measures but data relating to the measures is not readily available.

It may seem surprising that comprehensive security measures are not common in the hospital environment. Some may suggest that hospitals are supposed to be open access to anyone needing medical assistance and a controlled environment might impede the openness and accessibility, other suggestions may include the perceived immunity from terrorist attack under international law and the Geneva Conventions but the THREATS research has already identified evidence which contradicts such theory. Hospitals are public spaces that, relative to their size, often have significant density of population, particularly during visiting times and could therefore be considered a soft target.

Fischbacher-Smith and Fischbacher-Smith (2013:331) observe 'the hospital system (like many public services) is permeable and open', the security measures that are in place to protect the hospital infrastructure, patients, staff and visitors:

> ...would appear to be underpinned by a key assumption, which is that no one would actively seek to cause harm within a hospital. This view, however, is based on framing the problem through a Western-centric moral lens that would condemn indiscriminate killing of innocents, especially of those who are already ill.

Fischbacher-Smith and Fischbacher-Smith provide compelling evidence to support their theory, including the Dunblane school massacre (UK) in 1996 that resulted in the murder of 16 children and their teacher. Before 1996 this type of event would not have featured high on the 'potential scenario list' for emergency planners but other events worldwide have illustrated in graphic detail how terrorists can exploit soft targets and do not discriminate between gender, age or social group. The Columbine High School (USA) attack in 1999 left 12 students and a teacher dead following a sophisticated attack perpetrated by two senior students at the school. The coordinated attack included small arms fire, incendiary bombs to divert the emergency responders and multiple improvised explosive devices. Although the motive behind the attack was unclear, the intent to cause maximum damage and the extensive planning effort was clear to investigators. The Beslan school siege (Russia) in 2004 lasted for three days and resulted in the death of 385 people, of which 186 were children. The authors list other terrorist attacks throughout the world that demonstrate how vulnerable public buildings and spaces can be.

In addition to high density of population other potential opportunities may present the hospital environment as a worthy target for terrorist aims. Hospitals, by definition, have

substances that could be harmful to health, including biological and radiological material. It is highly likely that harmful material is protected by the appropriate level of security, but the general security of hospitals is potentially less sophisticated. Many hospitals operate a control of access system whereby members of staff are issued with a swipe card that enables them to access only the areas required to fulfil their role. Some hospitals have invested in the latest technology; including 'online wireless access control' that provides a greater level of control for the security team (Professional Security Magazine, 2014:19). However, the incidence of theft of equipment from hospitals illustrates the porosity of current security measures in general, opportunists will play a part in the overall picture but there is evidence to indicate that theft is also conducted by organised gangs whom 'steal to order', further demonstrating the ability to penetrate the hospital defences as part of a planned targeting process (DAS Safe Guard, 2010:9-10).

Access control systems provide a layer to security that should be deployed as part of a multi-faceted strategy of physical systems and procedures in order to reduce the vulnerability from a single point of failure. For example, access control systems are vulnerable to the insider threat; personnel with authorised access to controlled areas and hazardous material could be a potential security risk. An example of such a threat was realised in the Glasgow airport bombing which was carried out by an employee of the National Health system in the UK, his status as doctor gave access to a large amount of biological and radioactive material and medical gases (Guardian, 2007). Moreover, the insider threat provides ample opportunity for attack planning, enabling terrorists to map a potential target from within and spend time identifying vulnerabilities and learning organisational procedures and responses as well as gaining valuable access codes and information.

The events in the USA in the aftermath of the terrorist attacks at the World Trade Centre in New York during 11th September 2001, now known as 9/11, included a series of anthrax letter attacks (see http://www.fbi.gov/anthrax/amerithraxlinks.htm) in October 2001.These attacks included the use of Anthrax spores posted to addresses throughout the USA including political leaders. The origin and perpetrator of these ANTHRAX letters has not been fully resolved and the possibility that an individual or group of people with authorised access to biological agents and substances had used their legitimate privileged access for terrorist purposes exists.

The vetting and monitoring of health sector staff and contractors who have privileged access to key infrastructure assets and material is of growing importance and this along with the development of a security culture and awareness within this sector will need to be addressed as part of the overall reduction of risk within the sector. This issue is a significant one, which will be faced with many challenges in terms of civil liberties, ethics, culture and societal acceptance. Fischbacher-Smith and Fischbacher-Smith (2013:337) suggest all levels of staff working within the hospital environment 'have the potential to be involved in terrorism or other malicious acts' suggesting robust vetting procedures are conducted at the earliest point in the recruitment process, though vetting of Muslim doctors for radicalism may prove ineffective and will doubtless create a civil liberties problem (Al Alawi and Schwartz, 2008).

The current level of staff vetting or screening is perhaps less effective than managers think which has resulted in people working within the Health Sector without the necessary qualifications and experience or with other problematic issues affecting their suitability (DS Safe Guard, 2010: 7 and 9). Some of the screening methods currently used, such as criminal record checks (CRB) will only check against the name for criminal conviction history, it does not confirm the identity of the applicant. This provides a potential opportunity, for bogus job applicants or those seeking employment in order to gain 'insider' status, to navigate the screening process undetected by simple use of identity theft.

The security of people: staff, patients and visitors are a critical consideration. The general public need to feel safe in order to use the hospital facility otherwise the health sector will not be able to maintain the wellbeing of the population. Health service staff need to feel safe and secure in the work place. Events which undermine the safety and security of hospital staff are likely to affect patient services: if staff adopt methods of practice which make them feel safer in the workplace these are liable to slow down the patient 'turn round' times, for example additional layers to patient screening before being permitted to enter a secure zone and staff working in pairs or small teams, are measures that will increase a sense of safety but will reduce capacity.

The roving threat, whether a gunman or bladed weapon wielding terrorist is a serious threat and events throughout the world from Mumbai in 2008 to the Westgate shopping centre attack in Kenya during 2013 and the more recent attack at Karachi Airport in 2014 provide a

clear indication that attacks on public places with guns, explosives or bladed weapons is a viable option for the potential terrorist, as part of a team or lone wolf. The likelihood of success for the terrorist is high and the impact upon the local community is often devastating, with effects rippling out wider on a global scale. Greater awareness of the roving threat needs to be included in contingency and response planning that should include procedures for sheltering in place and evacuating to a designated space within the building otherwise called 'invacuation'. Hospital staff must understand their immediate duty of care to their patients, the public and themselves during the first vital few moments once they realise they are under attack.

In this age of information there is a huge reliance upon Information Technology and intra/internet based systems for the management of information. Notwithstanding patient confidentiality issues relating to unauthorised access or dissemination of confidential data, the wider impacts could include the disruption of key services and other utility functions that are managed via an IT based system such as security surveillance and control of access.

The type of threats that could affect the Health Sector will be addressed in the next research task of THREATS but other areas of vulnerability will be included here. It is worth considering dependencies, which services and utilities are vital to the efficient functioning of the hospital. Many large-scale hospitals have energy and water secondary supplies provided from on-site storage facilities but the capacity of on-site storage is limited and will enable the hospital to continue to function for a limited period of time only. Therefore an attack on services or utilities that are critical to the hospital is a potential method of attack against the Health Infrastructure, especially if the damage is extensive enough to exceed the maximum tolerable period of outage, whereby the damaged function is not recovered within the critical timeframe and is then beyond effective recovery.

1.8 Interdependencies

Interdependencies exist within the wider field of CIP and may exist within the Health Sector. The network of hospitals that form the frontline of primary care within regions could present an area of interdependency if the various medical disciplines are spread across a series of hospitals in a regional area. The capacity is shared across the network and the impact from a complete failure at one of the hospitals, resulting from a significant terrorist attack that causes the hospital to stop functioning, is likely to be experienced throughout the shared

network. The extent of the impact is likely to be reflective of the Business Resilience or Business Continuity Plans that have been put in place to respond to disruption.

The public are a potential interdependency because the effect of an insecure health service is likely to have a negative effect on hospital attendance. This in time could undermine public health that is likely to have an effect on societal wellbeing, thus undermining the principle that CIP is built upon:

> Hospitals are part of the very fabric of the supporting infrastructure that exists within cities and provide a range of core under-pinning processes by which cities function. A range of public health, primary care, acute and emergency services also keep urban areas (relatively) healthy and disease free. Any erosion of the capabilities to provide health care, would therefore impact on the performance of a range of other services and activities. A city that loses its abilities to contain disease will very quickly start to see a denudation of its core functions as those who provide such service become too ill to work.
> (Fischbacher-Smith and Fischbacher-Smith, 2013:335)

This introduction provides a short insight to the importance of the Health Sector within CNI and the impact that could be felt across multiple CNI sectors in the event of a serious terrorist attack against a hospital. Currently hospitals provide open access to the public and do not benefit from the same level of building ‘hardening’ currently experienced within other sectors such as the aviation industry and airports. Hospitals therefore present a soft target to a determined terrorist group. The interdependencies or interconnectedness between Health and other sectors has been summarised to provide context when contemplating the complexities of managing risk vulnerabilities within CIP and the potential seriousness of not applying equal protective measures to all sectors within a protection programme.

2. Literature Review

2.1 Methodology

In order to assess the literature on the management of risk in the Health sector, Annex A of Deliverable Report 1.1 (D1.1) was taken as the baseline for MS that have identified Health as a part of the National Infrastructure. The date of that report is therefore the date for which the baseline may be applied, and should there have been changes in MS policy since then these may not be adequately reflected in this report. The nature of the research question was somewhat paradoxical in that it was both very wide, encompassing 28 MS, and very narrow, looking at how the health risk in particular was managed as a part of the CNI. The fear must always be that because the understanding of the researchers is inevitably better on some of the large and influential MS (e.g. Germany, Sweden) than it is on some of the newer MS (e.g. Slovenia) that some information will not have been gathered. This is in line with the observation of the Centre for European Policy Studies (CEPS) report on Protecting CI in the EU where the authors observed that countries like the UK and Sweden were far more advanced in their CIP policy than were some of the other MS (CEPS, 2010: i). CEPS also found that the pattern of CIP coverage by MS in general was very fragmented (CEPS, 2010: 4). The Netherlands has also commented on the variable development of CIP worldwide (Ministry of the Interior and Kingdom Relations, 2004: 8). The aim of the THREATS project is to provide guidelines on critical healthcare infrastructure; information that is widely shared as best practice should have been uncovered by the best efforts of the researchers. Sharing best practice is a vital aspect of promoting CIP (CEPS, 2010).

2.2 Member States

As was apparent from D1.1, the number of MS that have identified Health as a part of the CNI is limited, and amongst those that have, few have noted much detail of the CNI assets being considered available. This lack of detailed consideration of Health as a part of CNI also seems to be reflected, for example, by the fact that none of the 17 issues of the European CIIP Newsletter have an article on Health as CI, even though this publication frequently has articles about other areas such as energy and finance. Similarly the CEPS report on sector specific plans did not consider Health as a sector (CEPS, 2010). There are issues of secrecy and the national interest which may make it unlikely that detail of Health CNI assets would be readily and publically available online (Cabinet Office, 2014: 7-9). There is a tension here between the need for CIP to be shared with policy makers, public

agencies and private agencies to provide a common operational picture and the need for sensitive information to be protected (CEPS, 2010).

In some MS such as Malta, Health is explicitly defined as a sector of CNI but the information on the government website is generic, showing an approach to all CNI but not differentiating the treatment of Health in any way (Malta Critical Infrastructure Protection Unit a). Malta CIP has various links on its website to bodies responsible for transport; water, energy and mineral resources; communications; financial services and the police (Malta Critical Infrastructure Protection Unit b). However, the absence of a link to a Health body may be seen as weak or tangential evidence that Health is not highly regarded as a part of Malta's CNI.

In general there is an asymmetry in the frequency with which specific sectors of CNI have been represented in the documents publically available. Some MS, such as the Czech Republic, while identifying CNI as an issue on the government website, do not break CNI down into any sectors (Hasičský záchranný sbor České republiky). Where sectors have been identified by MS, a majority of the documents that are available concern CII (Agence nationale de la sécurité des systèmes d'information; Presidency of the Council of Ministers, 2013 and Departmento de Seguridad Nacional, 2013). The Estonian government website only references Critical Information Infrastructure and no other sectors (Republic of Estonia Information System Authority.) There has been a EU drive on cyber security since 2009 (Commission of the European Communities, 2009). In some MS the main focus of the CNI efforts described on the Government website are with regard to energy, for example Bulgaria (Ministry of Economy and Energy). There is a tendency, therefore, for Health not to be one of the more widely discussed sectors of CNI in the materials surveyed. This may be in part because Council Directive 2008/114/EC on the identification and designation of ECIs and their protective measures was limited in its scope to transport and energy (European Council, 2008: L345/75).

Overall the representation of Health as being a part of the CNI is inconsistent amongst Member States, and even where Health is seemingly identified it is not apparent exactly how the Health risks are managed in respect of the National Risk.

2.3 Where Health sits in CI

When Health has been identified as being a part of the CNI it has been differently categorised by different MS. In Finland the National Emergency Supply Agency identifies Health as being part of the CNI (National Emergency Supply Agency a) This website does differentiate two facets of CNI: critical infrastructure and production critical to society; Health is covered by the second of these two categories (National Emergency Supply Agency, b).

Production critical to society includes:

- Food supply
- Energy production
- Health care
- Production supporting military defence
- Promotion of the general prerequisites for operation of export industries (National Emergency Supply Agency b).

Whilst this may imply that Health assets such as hospitals would be CNI assets, this is not expanded on in the Finnish materials found by the researchers.

In Germany health is identified as a part of the supply services sector in the CIP plan (Federal Ministry of the Interior, 2009: 42). In so far as it is possible and appropriate to make cross border comparisons, this does seem to put Health in Germany on a similar footing to Health in Finland. Germany's 2009 CIP strategy states that health is a part of the status quo of German Society, suggesting therefore that it is a part of the infrastructure that would need repairing:

> Germany has a close-meshed network of infrastructures that are of vital importance to the country's society. The provision of the population and of business and industry with energy, IT and transport services, with health care and financial facilities and with drinking water and food supplies is very good. A stable constitutional and legal system provides for the general conditions ensuring peaceful community life in security and prosperity also in the event of crises.
> (Federal Ministry of the Interior, 2009: 4).

Poland unconventionally lists "health protection systems" as part of the CNI (Rządowe Centrum Bespieczeństwa). The RCB website lists the aims of the CIP as being:

- preventing the malfunctioning of critical infrastructure;
- preparing for crisis situations that could adversely affect critical infrastructure;
- response in the event of destruction or disruption of critical infrastructure functioning;

- reconstruction of critical infrastructure.

The website refers to the fact that there should be National priorities, objectives, requirements and standards, and detailed criteria which identify objects, installations, facilities and services included in the critical infrastructure. (Rządowe Centrum Bespieczeństwa). Whilst these seem laudable and wise suggestions, there is little detail of whether and how this has been done in the publically available material.

The United Kingdom has an established Counter Terrorism Strategy (CONTEST) (HM Government, 2011). This Counter terrorism strategy includes the 4 key pillars of

- PREVENT
- PURSUE
- PROTECT
- PREPARE

Under the heading PROTECT CNI assets are identified and a vulnerability reduction programme is coordinated by the Centre for the Protection of the National Infrastructure (CPNI). CPNI works with sector owners in devising vulnerability reduction plans via a Cross Sector Working Group (CSWG). The National Health Service (NHS) is represented on the CSWG. Cabinet Office (2010) is primarily concerned with the risk from flooding, but in Annex A it does define a criticality scale for National infrastructure running from CAT5 to CAT0, with CAT3 being set as the threshold of criticality. This vulnerability reduction programme is also supported by the National Office for Counter Terrorism (NaCTSO). A Public Services agreement (PSA 26) has been established to ensure a multi departmental and sectoral ownership commitment to the objectives of reducing the vulnerability of the UK to international terrorism.

This review has identified that the Health Sector has been identified as part of the National Infrastructure, that it has identified CNI assets within it and that it has established a vulnerability reduction programme. This programme includes a National and Regional structure of personnel and resources within the Health Sector at Primary Care Trust level whose primary function is to enhance the protective security of CNI assets within the Health sector of the United Kingdom. It has established a Health Protect structure to oversee this vulnerability reduction programme with senior staff known as Local Security Management Specialists established in all Primary Care Trusts within the NHS. The management of intelligence to aid in the risk management and to aid threat assessment is also incorporated

into this structure. This requires a close cooperation with a multi agency approach to intelligence gathering, analysis and dissemination.

In the drive to look at EU MS it is important to recognise that countries do have a history prior to entry into the EU, and that some MS established their initial approach to CIP before entering the EU. The Romanian government, for example, established the Centre for Information on Security Culture (CICS), on September 30, 2003. It resides within the Romanian Intelligence Service and is intended to be an interactive and multidisciplinary information system. One stated aim of the CICS is to notify society about national security issues. It states that its main goal is to:

> ...adopt a correct attitude towards the participation of specialized institutions and citizens in the development of the new security environment.
> (Romanian Intelligence Service, 2003: 4)

This document references cooperation with public bodies to ensure knowledge transfer in the area of security, which again seems appropriate, but it was not clear to the researchers how this was carried out on the ground (Romanian Intelligence Service, 2003:21).

2.4 Subdivisions of Health CI

The patterns of information available on CIP in MS as well as being fragmentary vary somewhat. Many MS such as Austria have not declared explicit details of Health as a part of the government website but do make reference to Health in the contribution to another document. In Austria's case the OIIP (Österreichisches Institut für Internationale Politik) were co-authors of the Recommended Elements of Critical Infrastructure Protection for policy makers in Europe (RECIPE) manual (2011). RECIPE identifies Health as one of eleven potential CI sectors, and subdivides it into

- Medical and hospital care
- Medicines, serums, vaccines and pharmaceuticals
- Bio-laboratories and bio-agents.
  (RECIPE, 2011:17).

In the Netherlands from the Government website the fourteen sectors identified as being a part of the CNI include Health which is subdivided into

- Emergency and hospital care,
- Medicines and vaccines (see Government of the Netherlands).

Although the quick scan of Dutch CIP initiated in 2002 originally saw Health as being a single sector, it was subsequently defined as being divided into:

- Urgent care and hospital care
- Medicines
- Serums and vaccines
- Nuclear medicine

(Ministry of the Interior and Kingdom Relations, 2004:10).

Although the terror threat level in the Netherlands was raised in March 2013 to substantial (OSAC), there is little evidence of how this is managed in terms of protecting the Health infrastructure.

In Sweden the Health sector is identified as part of the CI and Vital Societal Functions and is defined as:

> The Health, medical and care services Emergency medical services, pharmaceutical and equipment supply, childcare, disabled and elderly care, primary health care, psychiatry, social services, disease control for animals and people etc.
> (Swedish Civil Contingencies Agency 2014)

Denmark does have official publications that identify sectors of CI (Danish Emergency Management Agency, 2006). Appendix A of the Danish Emergency Management Agency (DEMA) Risk And Vulnerability Assessment guide (2006:21) identifies Health as a part of society's critical functions as being broken down into:

- Primary health services
- Hospital services
- Care of vulnerable people
- Monitoring infectious diseases
- Medications preparedness
- Medications production.

In the 2004 Government report on the Finnish Security and Defence policy social and healthcare functions are considered and it is stated that "the most important" of these in terms of "the population's health and functioning capacity" must be protected (Prime Minister's Office, 2004:149). This policy document asserts that hospitals and health centres must have CBRN strategies and be prepared to quarantine large numbers of people in the event of a strike. Government reserves are to be used to supply vaccines and other drugs in the case of an emergency. Ambulance and air ambulance services would be expanded in the case of an emergency (Prime Minister's Office, 2004:149-150). In 2006 the Security and

Defence Committee issued another resolution listing five areas of focus in the strategy for protecting functions vital to society, one of which is Health protection (Prime Minister's Office, 2004:60). Finland has several documents touching on CIP available and it is asserted by Finland that a nationwide emergency social service system, encompassing Health CI, will be fully operational by 2007. The current researchers have not been able to ascertain whether this target was met (Security and Defence Committee, 2006:41). This document also addresses the question of the availability of pharmaceuticals as well as medical devices and supplies as organised by the Ministry of Social Affairs and Health (Ibid: 19). It references the obligatory stockpiling of medicines, the emergency stockpiling of pharmaceuticals, vaccines, medical devices and supplies along with international and Nordic agreements and projects (Security and Defence Committee, 2006: 42). An example of this would be the avian influenza scare in 2005; Finland's parliament allocated EUR 20 million for stockpiling antiviral drugs (Embassy of Finland, Washington D.C., 2005). It seems to be an emergent theme that medicines and vaccines need to be considered as a potential part of CNI, this being mentioned by Austria and Denmark as well as Finland (RECIPE, 2011:16; DEMA, 2006: 21.) It is not apparent from the documents found how the governments in question can be confident that they are stockpiling appropriate drugs.

What is apparent from this review is that Health CI may include more than hospitals but may also include places where drugs and vaccines are stored and possibly bio laboratories. What does not seem to fall out from the review, however, is detailed guidance to the Health sector on strategic or practical CNI identification or protection.

2.5 Management approach

Many MS that do consider Health as a part of CNI operate a sector responsibility principle. One such is Denmark who organise CNI such that the institution with day to day responsibility for a sector is also responsible for the management of that sector in the case of a disaster:

> Within their respective fields of administration, Individual ministers shall plan for the maintenance and continuation of society's functions in the event of major accidents and catastrophes, including actions of war, and in order to provide support to the defence forces.
> (Danish Preparedness Act, 2009).

In a similar approach to that taken by Denmark, in Estonia the critical infrastructure protection is devolved to the ministry/administration in charge of a specific function (European Commission a). Estonia is administratively divided into fifteen counties and there are two hundred and twenty seven local governments (European Commission a). The responsible ministry directs and co-ordinates the emergency planning of that function at all levels (national, regional and local); in the case of health this is the Ministry of Social Affairs.

The Swedish government tasked the Swedish Civil Contingencies Agency (MSB) with developing a National Strategy for the Protection of Vital Societal Functions. The MSB have issued a guidance document relating to their development of action plans to protect critical infrastructure in Sweden. The document (Swedish Civil Contingencies Agency, 2014: 18) identifies all entities that own or operate CI in Sweden, and states that it is the responsibility of the owner or operator of the asset to identify the CI and vital social functions. These would be municipalities, county councils, county administrative boards, national authorities and private sector operators.

2.6 Shortcomings

Shortcomings in CIP have been remarked on in a few instances in the literature. An article about Bulgaria identified in D1.1 does identify Health as being a sector whose running at a basic level is necessary for the functioning of society at both a public and a private sector level (Nickolov, 2005: 106). This paper, which is primarily concerned with CII, does identify a lack of government strategy and organisation with respect to CII in Bulgaria (Nickolov, 2005:109-111). Although Bulgaria only joined the EU in 2007, the researchers could find no evidence of a drive on CIP since that date. Tagarov and Pavlov, criticise the Bulgarian approach for being so wide that it tries to protect the whole economy against terrorist attacks and other disasters rather than focussing on the population and CNI (2007:45). In the UK it has been observed that the Health Sector is not regulated in the same way as the water and energy sectors. A different approach is therefore needed in order to ensure the resilience of the Health sector than certain other sectors (Cabinet Office, 2013). The Netherlands have warned that CIP needs to be on going and not one-off (Ministry of the Interior and Kingdom Relations, 2004:6) but it is apparent from this review that many MS have not yet made an initial assessment of Health as CNI and surely not an on going programme of mitigation.

2.7 Interdependencies

RECIPE identifies Health as being a sector where it is highly likely that sector-interdependency is such that in a crisis situation strain in that sector would have important knock on effects elsewhere in the CNI (2011:36). This document therefore clearly encourages policy makers to consider Health as a potential part of CNI, although lacking in statutory force to require them to do so. There is also a German green paper available in English that considers the devising of scenarios that would impact on CNI (Göbel, Reichenbach, von Neuforn and Wolff, 2008). Although one of the scenarios considered is a pandemic in Germany, an attack on a hospital is not considered (Göbel et.al, 2008:32-38). The pandemic scenario is one that is perceived to have many 'knock on' effects on other areas of CNI not just health, once again reminding us that Health is an area where the interdependencies may be hard to track but vitally important (Guthrie and Konaris, 2012:9). The German green paper raises the important question of whether the definition of critical infrastructure is suboptimal in the face of new and globalised risks (Göbel et.al, 2008:44). Rinaldi et al. (2001:14-16) have categorised interdependencies for critical infrastructures:

- Physical: the material outputs of the infrastructure affect the functioning of another
- Cyber: the information outputs of the infrastructure affect the functioning of another
- Geographic: dependency on local environmental effects that affects simultaneously several infrastructures.
- Logical: other dependencies.

The definition of responsibility for CNI as belonging to the asset owner or operator which is found in several MS (see above 2.4) has the drawback that as an approach it does not easily lend itself to comprehension of interdependencies as has been identified by the Netherlands (Ministry of the Interior and Kingdom Relations, 2004:11). Particularly, asset owners may have poor comprehension of the assets that depend on their asset for adequate functioning.

2.8 EU Cooperation

There are more examples of CIP at a local than a pan-European level, and it has been argued that the fragmentary nature of the EU means that the CIP is less developed here than in the USA (Giannopoulos et al 2012:38). One exception may be Finland that is a part of the Civil Protection Network (CIVPRO) part of the EUROBALTIC Programme for Civil

Protection initiated by the Council of the Baltic Sea States. This is an example of what CEPs has described as an 'island of cooperation' in CIP (2010:3). Finland has called for the EU's health care activities to be developed in cooperation to improve European preparedness for infectious diseases:

> Finland highlights the importance of international cooperation, an open and transparent information exchange, the World Health Organization and other international health organisations in the development of prevention, early warning and monitoring systems.
> (Prime Minister's Office Finland, 2009:89).

In 2012 Finland expanded this view to emphasise the especial need for international cooperation in respect of biohazards (Prime Minister's Office Finland, 2012:48 and 87).

The Netherlands highlights the importance of International cooperation in the EU, NATO and elsewhere and asserts that this exchange shows many similarities in policy and in the type of approach taken to CIP (Ministry of the Interior and Kingdom Relations, 2004:8).

2.9 Risk Report

Most of the CIP risk assessment work that has been done is sectoral and mostly at asset level (Giannopoulos et al, 2012:4). The fourth German risk report (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2011)), identifies some measures that might be taken to strengthen the resilience of the health sector, including acknowledgment that there is a possibility of a hospital being a target for a terrorist attack. It stresses the importance of coordinating the emergency plans of countries, counties and Municipalities with those of hospitals. This is especially important and problematic in a MS like Germany, which is governed on a highly federated model. The way that civil protection laws are framed in a MS also impacts on the resilience of the Health sector. In the German report a significant concern is identified that it is only emergency physicians and emergency services that are able to provide medically qualified help and make initial arrangements in the first phase of any catastrophic event.

This German document recommends an analysis of the overall system in terms of:

- Reception and treatment capacity;
- Availability of materials;

- Availability of personnel;
- Spaces infrastructure (accommodation);
- Ensuring a regional or national plan for transporting patients elsewhere

Measures to improve improvement increase enlarge the current situation are also identified:

- Extension of KatS regulations; can't find anything about these
- Reporting obligations of health professionals;
- Creation of medical material reserves and transportation capacity
- Expansion of drug storage in the hospital;
- Requirements for infrastructure reserves in hospital planning.
- Binding material and medical support security of supply in the case of events with potential risk for a major incident (Panic, terrorist event).

According to the RECIPE approach identifying whether Health assets (or any others) are a part of CNI involves four steps of:

- Applying criteria which are specific to that sector
- Assessing the degree of criticality
- Assessing dependency issues
- Applying crosscutting criteria

(RECIPE, 2011:16-17).

CEPS observes that sector understandings of risk and CNI protection are inadequately reflected in technical standards, and that a holistic comprehensive approach to risk management that transcends sector barriers is desirable but is currently lacking (CEPS, 2010:85).

The Netherlands has adopted an approach of taking a broad and non-prioritised approach in defining CNI, which they argue helps to uncover all of the interdependencies (Ministry of the Interior and Kingdom Relations, 2004:6).

It can be argued with some justice that an adequate risk assessment is the main pre-condition for successful CIP (Gianopolousi et al, 2012:3). Most of the documents found seemed to follow a qualitative rather than quantitative approach to CIP and risk assessment (Danish Emergency Management Agency, 2006:4; Prime Minister's Office Finland, 2004:51 and 162-3). The use of qualitative methodologies acknowledges the role of cognition and

personal experience in the perception of the severity and likelihood of risk. The experience of the assessors and the visibility of the underlying assumptions are therefore of great importance in the quality of the risk assessment (Danish Emergency Management Agency, 2006:4). Qualitative methodologies may assess outcomes in various terms, for example the Finnish white paper talks in terms of enhanced interoperability; deployability and sustainability (Prime Minister's Office Finland, 2004:51).

There is however a risk that qualitative measures may be excessively abstract and general (TENACE, 2014:126). Proponents of quantitative methods may argue that these approaches allow for more detailed consideration of the likelihood of an event and more precise calculation of its consequences than do quantitative methods (Flammini et al, 2009:1-2). These calculations of likelihood and impact are based on prior occurrences. This, whilst it seems a reasonable defence of quantitative methods, rather underestimates the 'black swans' nature of terrorist attacks on health infrastructure, i.e. that the highest risks come from unpredictable and unprecedented events (CEPS, 2010:6). It has also been argued that quantitative methods allows for greater precision than the traditional 'high, medium, low' risk validation approach (Flammini et al, 2009:1-2). The caveat to that must be that the accuracy of any mathematical model may only be as great as the wisdom of the people who inform it; raising the question of whether quantitative methods can be more accurate than qualitative when the risks and interdependencies of CI are still relatively poorly understood.

In 2013 the NHS in the UK published Core Standards for Emergency Preparedness, Resilience and Response (EPRR), which have since been revised (NHS England, 2014). The NHS core competencies for EPRR core standards matrix includes:

Enable an identified person to determine whether an emergency has occurred

- Specify the procedure that person should adopt in making the decision
- Specify who should be consulted before making the decision
- Specify who should be informed once the decision has been made (including clinical staff).

Decide:

- Which activities and functions are critical
- What is an acceptable level of service in the event of different types of emergency for all your services

- Identifying in your risk assessments in what way emergencies and business continuity incidents threaten the performance of your organisation's functions, especially critical activities.

In CIP planning there is the 'paradox of vulnerability' which states that sophisticated nations that have (seemingly) robust systems do not expect an unlikely major event, so that if one does occur the impact is disproportionately catastrophic (Federal Ministry of the Interior, 2009b: 10-11). Sadly many recent terrorist examples show us that the 'against all odds' event such as two planes flying into the World Trade Centre can nonetheless occur.

3. Methodology

3.1 Research Approach

It was already established in D1.1 that the public domain information on Health as a part of the Critical National Infrastructure (CNI) of each Member State (MS) was not extensive.

As with the previous deliverable the scope of the research was limited to publicly available data written in English. This approach was adopted to ensure time and resource was managed across the whole project and the team responsible for the delivery of Work Package 1 (WP1) are UK based English speakers with very limited access to translation resources. Disclosure and other security issues may explain the paucity of data available.

Once again each EU MS government website was visited and a search for relevant information conducted. Further Google and Yahoo searches were carried out using key words to elicit relevant data including: Critical Infrastructure; Critical Infrastructure Protection; Critical National Infrastructure. These terms were then broadened in a divergence search to include terms such as: National Infrastructure; Infrastructure; Vital National Assets; Services and Utilities; National Contingency Plans; Emergency Management Plans; Emergency Response Plans; Health Infrastructure; Hospital Protection; Hospital Contingencies; Public Health Protection and Counter Terrorist Contingencies. Each of these terms was searched for again with the inclusion of the term 'Health' in it. Once again a straightforward test of utility was carried out whereby documents were briefly assessed by the research team in terms of reliability (i.e. information from a credible source) and relevance to the aims of the project.

As this deliverable follows on the heels of D1.1 the websites and documents identified in the appendix of that document were all revisited. Additionally a snowballing technique was applied, following relevant links from the MS websites and from the literature harvested to ensure a reasonably comprehensive search.

3.2 Additional Searches

The research team acknowledged the research parameters, searching for data that was written in English and available in the public domain, introduced constraints to the research approach that could preclude relevant information that has potential to alter the overall findings or change the team's perception of the CIP status within the EU, including a bias for

UK based practices. The project has partner agencies in Italy and France whom were asked to conduct a limited search for data via online resources, looking in detail at specific hospital Emergency Management Plans in order to identify any reference to ‘terrorist attacks against the hospital’. The findings of that search are contained within the findings of this report.

In recognition of the need for greater detail and to overcome the limited publicly available data and information available further detailed interviews and questionnaires with key health security and critical infrastructure protection agencies will be conducted over the coming months and will produce follow up and addendum to this report.

4. Findings

4.1 New Age Terrorism

The new age of terrorism with the emergence of Islamist influenced terrorist groups and other ideological groups perpetrating acts of extreme violence in order to create fear and propagate their ideologies worldwide has become more prominent in recent years (see for example Neumann, 2009). It is often argued that terrorism is more ad hoc, lethal and likely to use CBRN weapons than was previously the case, (although note that not all writers share this view, eg Crenshaw, 2006). It is more conceivable today that terrorists could actively target a hospital because it provides all the ingredients of a spectacular event: the chances of success are very high due to limited protective measures; it is comparatively easy to plan an attack using open source information and hospitals are large employers vulnerable to an insider threat. The literature illustrates how the terrorist threat has been taken seriously in other sectors such as the aviation transport sector and significant progress has been made to try and mitigate the risk. The International Civil Aviation Organisation (ICAO) requires airports to prepare emergency plans and to maintain emergency services according to the categories of aircraft using the airport (A Framework for Major Emergency Management, 2006). Currently there is no evidence to suggest the Health Sector has taken similar protective measures.

4.2 Emergency Planning

Emergency planners have made provision for hospitals and health infrastructure to respond to mass casualty and terrorist incidents off-site (see for example RECIPE, 2011; Ministry of the Interior and Kingdom Relations, 2004; Swedish Civil Contingencies Agency, 2014). It is not apparent, however, that they yet recognised the threat to the hospital, including the second strike attack scenario. Emergency Response Plans are extensive but do not include terrorist attack on-site and hospitals are yet to provide ‘active shooter’ or ‘marauding gunman’ type training to hospital staff and implement emergency plans to ‘shelter in place’ or evacuate within the building to a safer area, otherwise known as ‘invacuation’. Evidence does exist in many Hospital Emergency Plans, including some plans which were sampled in Italy, that consideration has been given to man-made threats but the evidence suggests the planning is limited to ‘bomb threats’ via telephone and tangible evidence to illustrate deeper consideration of contemporary threats has not yet been identified. Additional research will be conducted during the research for D2.1, which will hopefully provide valuable insight to the reality of Health CIP. The literature suggests emergency planners and managers could be

slow on the uptake in part due to a failure to recognise the contemporary threat or at least viewing that threat 'through the Western-centric lens' but other literature indicates the presence of bureaucracy within contingency planning (Fischbacher-Smith and Fischbacher-Smith, 2013:335).

4.3 Disjointed CIP

CIP across EU MS remains fragmented though the research shows developments in some MS but limited or no progress in others. The inclusion of Health as a sector of CNI is equally disparate. Some MS list Health as a sector within CNI but the evidence to support progress in this area or the existence of effective strategies is lacking, exactly how the health risks are managed is not apparent. The way Health is categorised varies from State to State. In some MS Health is managed as 'production critical to society' whereas other MS consider Health to be 'critical infrastructure'. The variation in approach and limited emphasis on Health, in some areas, is not helped by the EC identification of European Critical Infrastructures (ECIs) as stated in the EC directive (2008, L345/75) that focuses primarily upon transport and energy.

Some MS have made good progress within their national CIP programmes and are exemplar in the CIP field by implementing a national level or strategic level directive underpinned by regulatory compliance, supported by an agency that can provide expert advice and support but enables the service provider or operatives to embrace best practice and remain commercially competitive. An example would be the UK: the CONTEST strategy provides the framework and top down directive to CNI sectors to work within agreed guidelines in order to maintain the CNI. The UK government has established CPNI, supported by other agencies and initiatives, to support CNI and provide expert advice, support and security assessing and testing. Importantly, Health is listed as a sector of CNI and the government has established risk and security managers at regional level within a Trust area whom manage the risks at operational level but are connected with CPNI at strategic level and as part of a national network.

The inclusion of Health as a sector within CNI is a good starting point from which to develop the sector within the CIP programme. Some MS have developed the sector descriptors to include medicines and vaccines, for example Finland and The Netherlands. It is hard to assess the efficacy of the stockpiling of emergency supplies for use during pandemic events,

such as the avian flu scare in 2006 as a risk mitigation activity as the literature does not provide evidence to suggest that governments can be confident they are stockpiling the appropriate drugs. The development of CIP of the Health sector within the EU may be hampered by lack of cross EU cooperation; lack of agreement on what is critical and poor understanding of the necessarily complex interdependencies and cross cutting criteria in this area.

5. Conclusions and Recommendations

5.1 Sharing Information

The intelligence or information generated by government security services is vital to ensuring CNI sectors are aware of changes within the current terrorist threat landscape. There will always be challenges with managing sensitive information and creating useful and useable intelligence bulletins which will enable CNI owners and operators to adjust protective measures to respond to the changing threats. The literature indicates relationships already exist in some areas of the EU between security services and CNI providers, through organisations such as CPNI in the UK, but this needs to be reflected in all EU MS. Furthermore, to optimise effect interested parties must ensure the relationships are fused at the appropriate level of management to ensure the 'knowledge worker' or true expert, such as the Local Security Manager, is actually included in the network of information.

5.2 Managing Health CIP

This report has aimed to provide a cogent, albeit brief, summary as to why Health should be managed as part of CNI. Health is dependent upon other sectors, such as power and water supply, to enable continuity of service delivery. Meanwhile the wider CNI is dependent upon Health to ensure the health and wellbeing of the population, the workforce and civil order and governance are maintained. This illustrates the interconnected relationships that exist between Health and other sectors of CNI, reported throughout the literature as interdependencies.

All Sectors of CNI need to be carefully managed to ensure risk management and vulnerability programmes are appropriate and proportional to specific areas within the sector. Health Authorities need to recognise and take ownership of the CNI assets within their sector and adopt suitable strategies to safeguard accordingly.

The evidence relating to the existence of vulnerability reduction programmes within the EU Health Sector is very limited. Some evidence has been identified and included in the main body of this report, but if the evidence were to be annotated onto a map of Europe there would be large and significant gaps. It is worth relating back to D1.1 that highlighted the

vulnerability within a network of interdependent elements, the network is only as strong as the weakest link. Vulnerability reduction programmes need to be established in all EU MS to ensure the sector identifies the hazards and threats and manages the risks effectively.

The use of common language, standard practices and standardising CIP management protocols will go some way to encouraging better coordination within the EU. The establishment of Health CNI vulnerability risk reduction governance and management structures will support developing EU MS to improve their CIP and enable collective effort to develop best practice.

5.3 The Risks

The Health Sector has some unique challenges where public access must be assured and a supportive and inclusive environment be created for patients, staff and visitors. The inventory of hazardous substances, personal data, research laboratories etc. must be protected. It must be recognised that most hospitals represent a crowded place where large numbers of people access and congregate and where the risk of such vulnerabilities to terrorist attack are managed down. It is therefore imperative that sector specific guidance and operational requirements are developed and available to assist the overall security management risks within these buildings and properties. The threat of person-borne, vehicle-borne and stand alone improvised explosive devices (IEDs), along with the insider threat of unauthorised access to areas containing hazardous materials, pharmaceutical, biological substances and sensitive data requires specific guidance to be produced for the health care sector. The protection of patients from such terrorist attacks must also be identified and managed including V.I.P protection and sensitive or high threat status patients (for example military personnel or patients being treated for a previous targeted terrorist attack).

5.4 Vulnerability Reduction

This specific guidance should include a security culture awareness programme to ensure staff at all levels within health organisations are aware of the issues and ‘buy in’ to the initiatives and objectives of the vulnerability reduction programme. The success of these programmes are entirely dependent on the managers, staff and stakeholders within the

health sector and therefore a significant investment must be made in the education, culture and understanding of these groups in respect of the reduction in the vulnerability of the sector to terrorist attacks.

As part of a vulnerability reduction programme key performance indicators should be developed for Health CNI risk reduction (for example, such as a reduction in unauthorised access, a reduction in theft or a reduction in data breaches) to ensure that objectives set are being met or where not met the reasons and solutions to ensure future compliance and improvements are achieved. This performance review and KPI regime should be a jointly agreed and established programme between the local or national government and health authorities; it is a truism that if something is not measured it will not happen nor be achieved.

All of these programmes and initiatives in achieving a vulnerability reduction programme within the Health Sector CNI will need to be funded and adequately resourced. This funding will be required to be found either within existing budgets, new monies found or funded through direct government funding sources. These can only be achieved as part of a wider CIP programme either funded at central or local level. Some countries have separate funding streams to support national or regional counter terrorism strategies and policies. Many countries do not have such centrally available funding streams and if no new or available monies are available funding for these counter terrorist programmes and initiatives can be facilitated utilising existing security funding resources. It could form part of the general security awareness raising within the health sector and securing general security budget streams for specific CNI protection or vulnerability reduction programmes.

6. References

Agence nationale de la sécurité des systèmes d'information. Available from: http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf [Last Accessed 16th October 2014].

[Anon.] (2014) Antrim Area Hospital. *Professional Security Magazine.* **24** (5), 19.

[Anon.] (2010) £1m of equipment stolen as gangs target hospitals & 'steal-to-order'. *DAS Safe Guard: Newsletter of the Dorset and Somerset Counter Fraud and Security Management Service.* (February 2010),9. Available from: http://www.dascfs.nhs.uk

[Anon.] (2010) Medic Guilty of £46k NHS Fraud. *DAS Safe Guard: Newsletter of the Dorset and Somerset Counter Fraud and Security Management Service.* (February 2010), 9. Available from: http://www.secure.uk.com/WS-Secure-UK/Downloads/publications/SafeGuardFeb10.pdf

[Anon.] (2010) NHS an East Target for Thieves. *DAS Safe Guard: Newsletter of the Dorset and Somerset Counter Fraud and Security Management Service.* (February 2010),10. Available from: http://www.secure.uk.com/WS-SecureUK/Downloads/publications/SafeGuardFeb10.pdf

[Anon.] (2010) Fraud That Put Lives at Risk. *DAS Safe Guard: Newsletter of the Dorset and Somerset Counter Fraud and Security Management Service.* (February 2010),7. Available from: http://www.secure.uk.com/WS-Secure-UK/Downloads/publications/SafeGuardFeb10.pdf

Atlas, R. (ed.) (2013) *21st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention*. 2nd ed. Boca Raton: Auerbach Publications.

Bremberg, N. and Britz, M. (2009) Uncovering the Institutional Logics of EU Civil Protection. *Journal of the Nordic International Studies Association.* **44** (3), 288-308.

Brunner, E and Suter, M. (2008) *International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 international Critical Information Infrastructure Protection Policies*. Zurich: ETH.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2011) Vierter Gefahrenbericht. Available from: http://www.bbk.bund.de/SharedDocs/Downloads/SK/DE/Publikationen/4-Gefahrenbericht.html [Last accessed 9th December 2014].

Cabinet Office (2010) *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards.* Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf [Last accessed 28th October 2014].

Cabinet Office (2013) *A Summary of the 2013 Sector Resilience Plans*. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf [Last accessed 21st October 2014].

Cabinet Office (2014) *HMG Security Policy Framework*. Available from:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf [Last accessed 22nd October 2014].

Centre for European Policy Studies (CEPS) (2010) Protection Critical Infrastructure in the EU: CEPS Task Force Report. Available from: http://aei.pitt.edu/15445/1/Critical_Infrastructure_Protection_Final_A4.pdf [Last accessed 20th September 2014].

Centre for the Protection of National Infrastructure (n.d.) *Physical Security*. London: HMSO. Available from: www.cpni.gov.uk/advice/Physical-security/

Commission of the European Communities (2009) *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.* Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF [Last accessed 23rd October 2014].

Council of the Baltic Sea States: Civil Protection Network [online]. Available from: http://www.cbss.org/safe-secure/civil-protection-network/

Danish Emergency Management Agency, (2006) *Introduction and User Guide: DEMA's Model for Risk and Vulnerability Analysis.* Available from: http://brs.dk/eng/inspection/contingency_planning/Documents/RVA-model_user_%20guide.pdf [Last accessed 9th October 2014].

Departmento de Seguridad Nacional (2013) Available from: http://www.cnpic-es.es/Biblioteca/Legislacion/Generico/20131205_ESTRATEGIA_DE_CIBERSEGURIDAD_NACIONAL.pdf [Last accessed 16th October 2014].

Embassy of Finland, Washington D.C., (2005) Available from: http://www.finland.org/public/default.aspx?contentid=149012&nodeid=35833&contentlan=2&culture=en-US [Last Accessed 13th October 2014].

European Commission (a). Available from: http://ec.europa.eu/echo/files/civil_protection/vademecum/ee/2-ee-1.html [Last accessed 10th October 2014].

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.

Federal Bureau of Investigation ([n.d.]) *Famous Cases & Criminals: Amerithrax or Anthrax Investigation*. Available from: http://www.fbi.gov/anthrax/amerithraxlinks.htm

Federal Republic of Germany: Ministry of the Interior (2009) National Strategy for Critical Infrastructure Protection. Berlin. Available from: http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf

Federal Ministry of the Interior, (2009a) *CIP Implementation Plan of the National Plan for Information Infrastructure Protection.* Available from: http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/2009/kritis.pdf;jsessionid=EF461922E05297B4FE29A3F22943F309.2_cid287?__blob=publicationFile.

[Last accessed 21st October 2014].

Federal Ministry of the Interior, (2009b*). National Strategy for Critical Infrastructure Protection (CIP Strategy).* Available from:

http://www.bbk.bund.de/SharedDocs/Downloads/BBK/EN/CIP-Strategy.pdf;jsessionid=1F5BAD1569C334F73F6333EDB0336363.1_cid330?__blob=publicationFile [Last accessed 21st October 2014].

Finnish Government and Civil Protection Network. Available from: http://valtioneuvosto.fi/etusivu/en.jsp [Last accessed 8th October 2014].

Fischbacher-Smith, D and Fischbacher-Smith, M. (2013) *The Vulnerability of Public Spaces: Challenges for UK hospitals under the 'new' terrorist threat.* Public Management Review. **15** (3), 330-343. London: Routledge. Available from: http://www.tandfonline.com/doi/abs/10.1080/14719037.2013.769851#.VIYSkUvA7FI

Flenley, R. (2003) *Security Department Strategy 2003/06*. Canary Wharf Management Limited, unpublished.

Flammini, F., Gaglione, A., Mazzocca, N., and Pragliola, C. *Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures*. In: Critical Information Infrastructure Security, Third International Workshop, CRITIS 2008, Rome, Italy, October 13-15, 2008. Revised Papers. Springer Lecture Notes in Computer Science, **5508**, 180-189, 2009. Available from: http://wpage.unina.it/andrea.gaglione/publications.htm [last accessed 28th October 2014].

Giannopoulos, G., Filippini, R. and Schimmer, M. (2012) *Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art.* Luxembourg: European Union. Available from: http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf [Last accessed 21st October 2014].

Göbel, R., Reichenbach, G., S.S.von Neuforn and Wolff, H. (2008) *Risks and Challenges for Germany: scenarios and key questions.* Available from: http://www.zukunftsforum-oeffentliche-sicherheit.de/en/downloads/green_book_1_.pdf?1406347268 [Last downloaded 15th October 2014].

Government of the Netherlands. Available from: http://www.government.nl/issues/crisis-national-security-and-terrorism/protecting-critical-infrastructure [Last accessed 21st October 2014].

Guardian (2007) Hospital staff are stunned as doctors are questioned. *Guardian online.* 03 July 2007. Available from: http://www.theguardian.com/uk/2007/jul/03/terrorism.world2 [Accesses 01 December 2014].

Hasičský záchranný sbor České republiky. Available from: http://www.hzscr.cz/hasicien/article/implementation-of-the-council-directive-2008-114-ec-in-the-czech-republic.aspx [Last Accessed 16th October 2014].

HM Government (2011) *CONTEST: The United Kingdom's Strategy for Countering Terrorism.* Available From: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97994/contest-summary.pdf [last accessed 28th October 2014].

Lazari, A. (2014) *European Critical Infrastructure Protection*. Cham: Springer.

Malta Critical Infrastructure Protection Unit (a). Available from: http://maltacip.gov.mt//about?l=1 [Last accessed 6th October 2014].

Malta Critical Infrastructure Protection Unit (b). Available from: http://maltacip.gov.mt//links?l=1 [Last accessed 6th October 2014].

Maniati, M. (2012) *Civil Protection and European Governance: Investigating the diverging logics of the Member States and paving the way for the development of European Integration.* MA Dissertation, City University. Available from: https://www.academia.edu/3527567/Civil_Protection_and_European_Governance_Investigating_the_diverging_logics_of_the_Member_States_and_paving_the_way_for_the_development_of_European_Integration

Ministry of Economy and Energy. Available from: http://www.mi.government.bg/en/themes/critical-infrastructure-warning-information-network-ciwin-333-300.html [Last Accessed 16th October 2014].

Ministry of the Interior and Kingdom Relations (2004) *Protection of Critical Infrastructure.* Available from: http://www.nifv.nl/upload/91705_668_1223393504015-critical_infrastructure_protection_netherlands%5B1%5D.pdf [Last accessed 30th October 2014].

Ministry of the Interior and Kingdom Relations (2003) *Protection of Critical Infrastructure.* Available from: http://www.nifv.nl/upload/91705_668_1223393504015-critical_infrastructure_protection_netherlands%5B1%5D.pdf [Last accessed 7th October 2014].

National Emergency Supply Agency (a). Available from: http://www.nesa.fi/security-of-supply/ [Last accessed 8th October 2014].

National Emergency Supply Agency (b) *Objectives.* Available from: http://www.nesa.fi/security-of-supply/objectives/ [Last accessed 8th October 2014].

Newsome, B. (2014) *A Practical Introduction to Security and Risk Management.* Los Angeles: SAGE.

NHS England (2014) *NHS England Core Standards for Emergency Preparedness, Resilience and Response (EPRR).* Available from: http://www.england.nhs.uk/wp-content/uploads/2014/07/eprr-core-standards-0714.pdf
[Last accessed 28th October 2014].

Nickolov, E. (2005) *Critical Information Infrastructure Protection: analysis, Evaluation and Expectations.* Information and Security: An International Journal, 17, 105-119. Available from http://www.comw.org/tct/fulltext/05nickolov.pdf [Last accessed 16th October 2014].

United States department of State Bureau of Diplomatic Security: OSAC. Available from: https://www.osac.gov/pages/ContentReportDetails.aspx?cid=13763
[Last accessed 6th October 2014].

Ovillius,M. (2007) *A European Programme for Critical Infrastructure Protection: EPCIP.* Available from: http://www.helsinki.fi/aleksanteri/civpro/events/cip_Ovilius.pdf). [Last accessed 8th October 2014].

Pavlov, N. & Tagarov, T. (2007) *Planning Measures and Capabilities for Protection of Critical Infrastructure.* Information and Security: An International Journal, **22**, 38-48. Available from: http://pdf.aminer.org/000/230/857/capabilities_and_protection.pdf [Last Accessed 8th October 2014].

Presidency of the Council of Ministers (2013) Available from: http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf [Last accessed 9th October 2014].

Prime Minister's Office Finland (2004) *Finnish Security and Defence Policy 2004: Government report 6/2004.* Available from: http://www.defmin.fi/files/311/2574_2160_English_White_paper_2004_1_.pdf [Last accessed 21st October 2014].

Prime Minister's Office Finland (2009) *Finnish Security and Defence Policy 2009: Government report.* Available from: http://www.defmin.fi/files/311/2574_2160_English_White_paper_2004_1_.pdf [Last accessed 21st October 2014].

Prime Minister's Office Finland (2012) *Finnish Security and Defence Policy 2012: Government report.* Available from http://vnk.fi/julkaisukansio/2012/j05-suomen-turvallisuus-j06-finlands-sakerhet/PDF/VNKJ0113_LR_En.pdf [Last accessed 21st October 2014].

Public Safety Canada. Critical Infrastructure Policy. ([n.d.]) *Risk Management Guide for Critical Infrastructure Sectors.* [s.l.]: Pulic Safety Canada. Available from: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rsk-mngmnt-gd/rsk-mngmnt-gd-eng.pdf

RECIPE (2011) Good Practices Manual For CIP Policies. Brussels: European Commission.

Republic of Estonia Information System Authority. Available from: https://www.ria.ee/CIIP/ [Last accessed 9th October 2014].

Royal Institute of British Architects (2010) *RIBA guidance on designing for counter-terrorism*. London: RIBA.

Rinaldi, S.M., Peerenboom, J.P. & Kelly, T.K. (2001) *Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies,* IEEE Control Systems Magazine, pp. 11-25. Available from: http://user.it.uu.se/~bc/Art.pdf [Last accessed 30th October 2014].

Romanian Intelligence Service: *Critical Infrastructures Protection* Available from: http://www.sri.ro/upload/Brosura%20IC%20ENG.pdf

Rządowe Centrum Bespieczeństwa. Available from: http://rcb.gov.pl/eng/?page_id=210 [Last accessed 8th October 2014].

The Security and Defence Committee (2006) *The Strategy for Securing the Functions Vital to Society.* Available from: http://www.defmin.fi/files/858/06_12_12_YETTS__in_english.pdf [Last accessed 21st October 2014].

Stapelberg, R. (2008) Infrastructure Systems Interdependencies and Risk Informed Decision Making (RIDM): Impact Scenario Analysis of Infrastructure Risks Induced by Natural, Technological and Intended Hazards. *Journal of Systemics, Cybernetics and Informatics.* **6** (5), 21-27. Available from: http://www.iiisci.org/journal/CV$/sci/pdfs/R105SQ.pdf

Swedish Civil Contingencies Agency, (2014) *Action Plan for the Protection of Vital Societal Functions and Critical Infrastructure*. Available from: https://www.msb.se/RibData/Filer/pdf/27412.pdf [Last accessed 12th October 2014].

Whole Building Design Guide: A program of the National Institute of Building Sciences [online]. Available from: www.wbdg.org/design/provide_security.php [Accessed 10 December 2014].

7. Bibliography

Dolan, M. (2001) Standing Tall: New designs and materials will make future skyscrapers sturdier, safer, and smarter. *Popular Science*. December 2001. 74-79.

NHS Foundation Trust. University Hospitals Birmingham (2010) *Major Incident Response Plan.* Birmingham: NHS. Available from: http://www.uhb.nhs.uk/Downloads/pdf/MajorIncidentResponsePlan.pdf

Straw, S. (2008) *Are Hospitals Soft Targets?* [online] Security Management: Security's Webb Connection. Available from: http://www.securitymanagement.com/article/are-hospitals-soft-targets [Accessed 28 November 2014].

Georgieva, S. and Riquelme, D.M. (2013) *Slovenia: State-Owned and State-Controlled Enterprises.* ECFIN Country Focus. **10**(3)1-8. Brussels: European Commission. Available from:http://ec.europa.eu/economy_finance/publications/country_focus/2013/pdf/cf_vol10_issue3_en.pdf