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

Report No: DR/1/001

An Analysis of Critical Infrastructure Protection Measures Implemented within the European Union: Identifying which European Union Member States includes the Health Sector as part of Critical National Infrastructure and which facets of Health Infrastructure are considered Critical.

Version: 1.0

Date: 22nd Oct 14

Authors: CD, CA, and MM

Approved by: CA

Table of Contents

Glossary

The following terms have been listed by the European Commission and are available from the EC Home affairs website and other EC sites. The terms have been used as guidance when examining other data published by EU MS:

Critical Infrastructure – Physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in EU States. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services (Communication, 2004:3).

Critical Infrastructure Warning Information Network (CIWIN) – CIWIN is a protected public internet-based information and communication system, offering recognised members of the EU's critical infrastructure protection community the opportunity to exchange and discuss CIP-related information, studies and good practices across multiple sectors (CIWIN, [n.d.])

European Critical Infrastructure – European critical infrastructure (ECI) means critical infrastructure located in EU States. The disruption or destruction of which would have significant impact on at least two EU states (Council Directive, 2008).

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

European Reference Network for Critical Infrastructure Protection (ERNCIP) – providing a framework within which experimental facilities and laboratories will share knowledge and expertise in order to harmonise test protocols throughout Europe, leading to better protection of critical infrastructures against all types of threats and hazards (ERNCIP, [n.d.]).

Executive Summary

Project:

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

Work Package 1:

Threat, risk analysis and security assessment research of the state of the art regarding threats and risks to the health sector and how it is protected as part of the critical national infrastructure within Europe.

Deliverable 1:

Report on the current status of the Health Sector as part of the European National Infrastructure

Note: The scope of the report has been constrained to publically available research data in order to ensure the results are objective and reflective of the current state of affairs, so far as published data can reveal.

Preliminary Research:

In order to undertake the first task of the THREATS project, it was evident that some preliminary research was required to provide context to the research question as stated in the title of this report. The breadth of data and potential differences between European Union (EU) Member States (MS) required the research team to identify a point of reference from which to develop the investigation. The preliminary research was focussed on the European Framework for Critical Infrastructure Protection (EPCIP).

Main Research: Literature Review -

Analysis of current situation

- Analyse which European countries include the Health sector as part of their National Infrastructure.
- Analyse which European countries have identified Critical National Infrastructure assets within the Health sector.

Methodology:

An initial feasibility study was conducted to identify if data was available and accessible within the public domain. The initial study resulted in a significant number of positive results. The approach focussed on information that was immediately available for review and was not subject to disclosure sensitivity issues but it was acknowledged that other meaningful data may exist within organisations but had not been made available to the public because of administrative or disclosure issues. Limited information exists in 'hard copy' published material such as books and journals, however the availability of the material online provides greater access to material. Documents were briefly assessed and analysed to ensure they were relevant to the research.

Findings:

The initial findings contained within this report indicate a fragmented approach to CIP; some EU MS have evidenced significant progress within national boundaries whilst other MS have a much-reduced CIP signature within the public domain. THREATS acknowledge that some MS may be managing their national CIP responsibilities within a protected environment to reduce unauthorised disclosure of the sensitive facets of their plan. However not 'all of the parts of all of the sectors' can be considered critical, though the theory that some facets of all sectors is critical has been explored, especially when tested against specific scenarios.

This report provides an insight to the variation of CIP standard across all EU MS and proposes a theory that the variation is due to some critical factors: there is currently no agreed standard or unit of measure that can be applied to CIP performance management, a common language and terminology relating to CIP is yet to be agreed by all EU MS and the coordination of effort; including timelines; currently has limited effect at EU level.

The research has revealed significant differences between EU MS levels of published data relating to CNI protection. Some MS have published a national strategy document that is available from official government websites, other MS have not published a national strategy but other data exists that indicates work has been done within the field of CNI protection. In many cases EU MS relate their national strategies directly to the EC Directive (2008/114/EC) and provide very little information specific to the national perspective. In general the findings indicated that the status of CIP across the EU is disparate.

The EC has issued direction (EC, 2008) to implement CIP in each EU MS but the coordination of effort at EU level has not been effective to ensure all MS implement CIP to a required standard within an agreed timeframe.

The coordination at national level within each EU MS is poor. Some MS governments' have not taken a lead role to develop their national strategy but have relied upon private and research organisations to develop contingencies. The supporting policy directives are often a 'cut and paste' of EC policies, with very little detailed consideration for the national needs.

The literature review identified that a growing percentage of CNI was owned and managed by the private sector. According to the research 25% of EU MS rely on private organisations to manage CNI.

The research identified very limited training, exercising and testing as part of the overall effort to improve vulnerability reduction and consequence management as part of good practice, however National level exercise programmes are being conducted in other MS but are not publicly available. Some of the data collected indicated a prioritisation by some states to focus upon cyber and information security. A lack of information relating to the health sector of CNI was identified during the research process.

The team agreed that contingency plans are likely to be held at local level, though the research indicated that detailed strategy direction was lacking. The research has not identified any detailed work specific to health as a sector of CNI. The project team acknowledge that the scope of the research for this report has been constrained to publicly available data and therefore evidence that has not met the research criteria may exist. However, due to the lack of published information specific to health indicates that work is likely to be localised within individual hospitals or health authority regions.

A detailed breakdown by country can be found in Appendix A.

Introduction

1.1 In order to undertake the first task of the THREATS project, it was evident that some preliminary research was required to provide context to the research question as stated in the title of this report. The breadth of data and potential differences between European Union (EU) Member States (MS) required the research team to identify a point of reference from which to develop the investigation.

The preliminary research was focussed on the European Framework for Critical Infrastructure Protection (EPCIP). In its EPCIP communication of 12 December 2006, the Commission set out an overall policy approach and framework for Critical Infrastructure Protection (CIP) activities in the EU, this is an overall framework for activities aimed at improving the protection of critical infrastructure in Europe – across all EU States and in all relevant sectors of economic activity. Although the threats to which the programme aims to respond are not confined to terrorism, but include crime, natural disasters and other causes of accidents, its all-hazards cross-sector approach has direct relevance to the THREATS project.

The diagram (Fig.1) shows the path of the EU's request to MS and the path of the preliminary research.

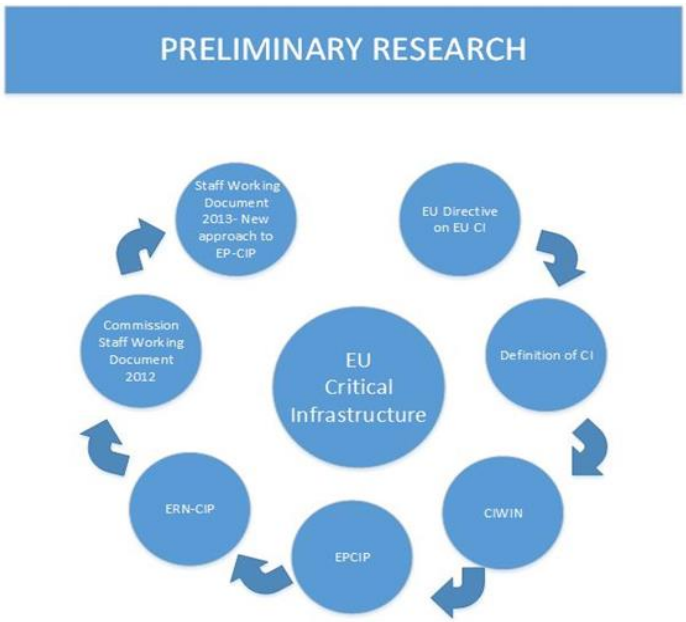

Fig.1

In April 2007 the Council adopted conclusions on EPCIP that welcomed the Commission's efforts to develop a European procedure for the identification and designation of European Critical Infrastructures (ECIs) and the assessment of the need to improve their protection. This eventually led to the adoption of Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of ECIs and their protective measures.

The scope of the Directive was limited to the energy and transport sectors. It constituted the first step in the step-by-step approach to identify and designate ECIs and assess the need to improve protection. The Directive outlined the approach that all EU MS would be required to follow, in order to identify, designate and protect ECIs in the energy and transport sectors, while indicating the ICT sector as a priority for possible future expansion of the scope.

The Commission Staff Working Document relating to the review of EPCIP, dated 22 June 2012 stated:

> 'The objective of the Directive is to identify, designate and adopt protection measures for infrastructures that are critical from a European perspective, i.e. where their disruption would have an impact on at least two Member States. The Directive specifies that Member States had to take the necessary measures to comply with the Directive by 12 January 2011 and set 12 January 2012 as the start date for the review of the Directive.
>
> Annex III to the Directive also requires all Member States to adopt a four-step process (see Fig.2) and to apply crosscutting and sectorial criteria to identify ECIs in the energy and transport sectors. In order to facilitate a cooperative approach, the Directive also requires the relevant Member States — those within which an ECI is identified and those which may be affected by its disruption — to engage in negotiations leading to the designation of ECIs (Articles 3 and 4). Once an ECI is identified, the Directive requires a specific set of actions to be taken by its owners/operators in order to develop an Operator Security Plan (OSP) documenting critical assets and security measures'.

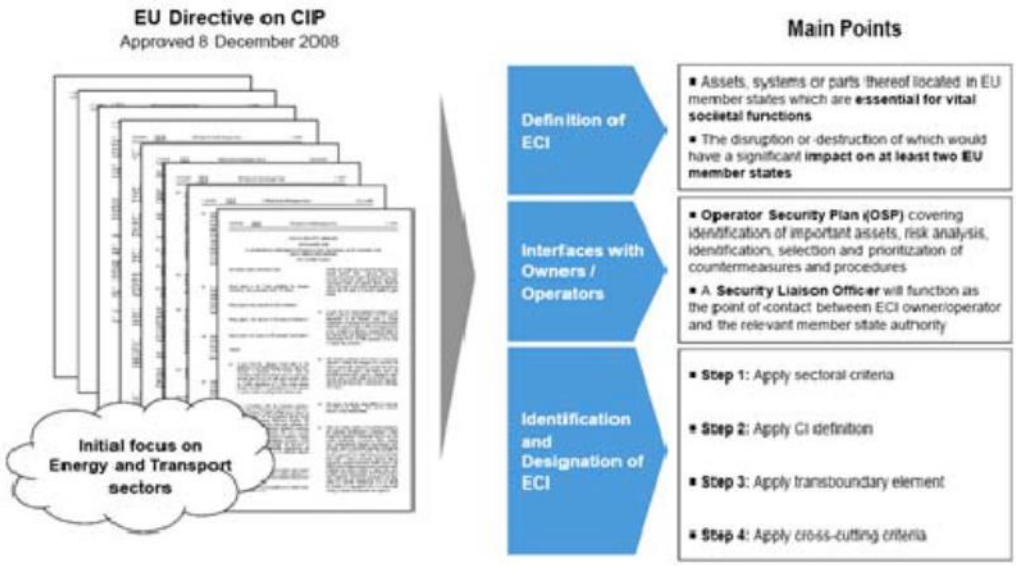

Fig. 2

The Commission Staff Working Document on the new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, dated 28 August 2013 stated:

> 'A part of our new approach is looking at the interdependencies between critical infrastructures, industry, and state actors. Threats to a single critical infrastructure can have a very significant impact on a broad range of actors in different infrastructures and more widely. Regarding risk assessment and risk management methodologies, the Commission has also funded numerous projects covering all sectors under the CIPS Programme. These include: the development of a risk assessment methodology to enhance security awareness in air traffic management23; the assessment of resilience to threats to control and data management systems of electrical transmission networks24; and an interactive risk assessment in the critical infrastructure field based on Earth Observation data and an integrated geographic information system25. The studies indicate that risk assessment methodologies for CIP follow either: 1) a sectorial approach, where each sector is treated separately with its own risk methodologies and risk ranking; or 2) a systems approach, where critical infrastructures are treated as an

interconnected network. Most work has been sectorial, but these methodologies show their limits when cross-sectorial issues need to be addressed, so a systems approach will be encouraged by the Commission from now on'.

The broadening of the implementation of the EU approach has led to the THREATS project that will concentrate on investigating the Health Sector as part of the critical infrastructure within the EU. Previous methodologies and risk assessment tools that have been used in other CI sectors will be examined and incorporated into THREATS as appropriate. The aim is to produce a revised and more practical implementation of activities under the three main work streams – prevention, preparedness and response to help build a common approach in the EU to Critical Infrastructure Protection and resilience in the Health Sector, taking full account of interdependencies.

1.1 The Infrastructure protection, from basic to critical is part of an evaluation of the vulnerability of assets and functionalities from disruptive events, which provide vital services to ensure the safety and wellbeing of society. Whether the disruptive event is manmade or natural, the societal impact of such occurrences are assessed and managed to ensure minimum levels of service are maintained. The processes, procedures and activities employed are designed to ensure a reduction in vulnerabilities, creation of resilience and the strengthening of business continuity. These functions are designed to reduce societal impact at local, regional, national and international level for all countries and organisations within the European Union member states (EU MS).

Business Continuity (BC) is now a recognised business function within most business enterprises globally. The main aim of BC is to prepare the organisation for predicted and unforeseen incidents, which could disrupt the business operation. In order to plan effectively; apply the appropriate resources in time and space; the organisation must first understand the threats that exist and the level of exposure or risk to the organisation. This is achieved by conducting a business impact analysis (BIA). The BIA underpins all subsequent preparedness planning by enabling the organisation to allocate resources and effort to the most critical areas of operations, prioritised by the level of threat, risk exposure and potential

impact to the operation in the event of disruption. It is important to understand that critical business functions are often connected in a manner that is not always immediately obvious and any disruption to a specific function could have a knock on effect to other areas of the business.

In simple terms BC should be applied to the routine management of a business to ensure there are sufficient resources to respond to a disruption, but most importantly, to recover from disruption in a manner that ensures the operation is not damaged beyond repair. This means BC is focused on preparation or preparedness and aims to build resilience into the organisation at every level. The importance of effective BC planning must not be underestimated; there now exist a wealth of data relating to BC whereby organisations failed to plan for significant disruption, which resulted in terminal failure of the business.

1.2 Ensuring an operation has resilience is not constrained to commercial business but is an appropriate function within any area of management; including government. In the United Kingdom (UK), for example, local government have a statutory responsibility, under the Civil Contingencies Act (2004), to plan for events that could disrupt the continuity of vital services and utilities. The Act is separated into two substantive parts: local arrangements for civil protection (Part 1) and emergency powers (Part 2) (Cabinet Office, 2004). The Act provides a national framework to ensure local government have identified local threats and prepared contingencies to manage a potential emergency and recover vital services at the earliest opportunity.

Contingency planning for natural and man-made disruption has never been so relevant. Hurricane Sandy in 2012 demonstrates the potential scale of disruption that can have a significant affect to even the most developed nation and the terrorist attack at the Westgate shopping mall in Kenya; in the same year that illustrates all public places are potential terrorist targets. Contingency plans must be robust and fit for purpose, and events in the UK in recent years have tested the measures contained within the Civil Contingencies Act (2004), as well as events in other EU MS testing similar established framework. But it is worth considering how quickly government, service providers and other agencies have responded to emergency

situations, reviewed their collective actions post event to identify lessons and then implemented changes which improve or enhance their future effectiveness.

1.3 The floods of 2007 in Gloucestershire illustrate the importance of collaboration between agencies to achieve a common goal and conduct a critical review after the event in order to identify lessons and learn from them. In the preceding 12-24 months before the floods Gloucestershire County Council (GCC) implemented a programme to plan for civil emergency events. Their efforts were recognised at national level and the programme was used as an example to other local governments. However, the flood event exposed a critical weakness in the contingency plan, it had been designed in isolation by GCC and had not been promulgated to other stakeholder agencies nor had it been exercised or tested at any level. However the contingency did provide GCC with an outline plan but other stakeholder agencies were unsighted to their specific roles and function within an emergency team and the collective organisation had to adjust and learn whilst responding to a serious civil emergency. The incident highlighted the complexities of large-scale emergency events and according to a report by Severn Trent Water (2007); whose operation was severely impacted by the flood; the logistical, public relations and incident management contingencies were suboptimal during the early phase of the incident.

1.4 The forest fire in Sweden during the summer of 2014 is reported to be the largest in more than 40 years (Enhance, 2014). Most EU MS are vulnerable to forest fires, especially the southern most States and forest fires can rapidly overwhelm in-country resources, requiring assistance from other EU MS. According to the Enhance project (2014) there were 16 separate calls for assistance by MS to help fight forest fires over the last three summers. Bulgaria, Montenegro, Albania, Slovenia, Bosnia and Herzegovina, Greece and Portugal have made formal requests for help for the last two summers, further demonstrating the importance of contingency planning but also illustrating the benefit of a European Commission (EC) collaborative response to similar emergencies across the European Union (EU). Forest fire events and other emergencies could easily absorb available resources and expertise contained within a single EU country and additional support might be drawn from within the EU, as illustrated during the Balkans floods in 2014.

1.5 The catastrophic flood event in Serbia and Bosnia and Herzegovina in May 2014 represents the worst ever floods to hit the Balkans (EurActiv, 2014). The event is reported to have affected more than 4 million people and the Bosnian Foreign Minister; Zlatko Lagumdžija; has reported that 'more than 100,000 houses and other buildings were no longer fit for use and that over a million people had been cut off from clean water supplies' (EurActiv, 2014).

The resources contained within the region were very quickly absorbed and both countries were overwhelmed by the impact of the flood. The event further demonstrates the value in a EU unified response. In this particular case, Serbia is a candidate country for joining the EU and qualifies for financial assistance from the EC. Although Bosnia and Herzegovina is not a member of the EU, assistance on humanitarian grounds was very quickly provided from a number of EU MS.

The EU response was activated by the EU Civil Protection Mechanism and coordinated via the Emergency Response Coordination Centre (ERCC) (EurActiv, 2014). The EU Civil Protection Mechanism was established in 2001 and includes all EU MS as well as Iceland, Norway and Macedonia and can respond at short notice to natural and man-made disasters anywhere within the EU and elsewhere (EC, 2014). The mechanism has 'monitored over 300 disasters worldwide and received more than 180 requests for assistance'; responses have included 'Hurricane Katrina in the USA (2005), the earthquake in Haiti (2010), the triple disaster in Japan (2011), and typhoon Haiyan that hit the Philippines (2013)' (EC, 2014).

1.6 The modern world has rapidly become an interconnected space whereby activity in one region; such as trade or conflict can affect activity in a different part of the world. Information technology and other technological advances have further enhanced the effect of an interconnected world or globalisation.

The theory of globalisation should be considered when seeking to identify the importance and value of a collaborative approach to Critical Infrastructure Protection (CIP) across EU MS. But it is important to understand how threats and their subsequent risks can affect isolated critical infrastructures as well as several

infrastructures, which may not necessarily be located in the same geographical area, described in the Task Force Report by the Centre for European Policy Studies:

> 'More precisely, infrastructures can either be independent, dependant, or mutually dependant. An independent infrastructure is one that in principle is isolated from the risks associated with other infrastructures. A dependant infrastructure is one that relies on another infrastructure (but not vice versa). Last, mutually dependant infrastructures depend on each other, with a successful attack to either resulting in damage to both.'
>
> (Renda, 2010:11)

The theory of an interconnected world can be illustrated further by events in Western Europe in November 2006, when a high-voltage power line was shutdown in Germany as part of a planned operation. The impact rippled across Europe resulting in power outages in France, Italy, Spain, Portugal, Austria and Netherlands, and even as far as Morocco (UCTE, 2007).

1.7 The idea of a collaborative, interoperable EU seems a more cogent prospect in light of interconnected infrastructure and the proliferation of disruption that could be generated from a single source but be experienced by multiple EU MS. Furthermore, it could be argued that it is in the interest of all EU MS to work closely and agree standard practices and methodology to protect critical infrastructure because all EU MS are vulnerable to the weakness of one MS. Renda explains:

> '…if 26 out of 27 countries have sufficiently strong policies to protect the internet backbone or challenge the spread of malware, this is not enough to guarantee the resilience of the internet network in the EU. It takes no more than one country to disrupt the whole system and expose it to threats'.
>
> (2010:7)

1.8 The type of threat and level of risk will vary from country to country across the EU; indeed some countries may not have identified a potential threat because it has not impacted them previously. The likelihood of an impact rippling across international boundaries cannot be ignored and therefore a joint approach across the EU is logical. However, a joint approach requires coordination of effort, an agreed measurable standard and a system to ensure all EU MS are fulfilling their roles and

responsibilities to the correct standard. Antecedent to any joint effort would be to agree what constitutes CNI and provide a definition that can be used as a fixed point of reference.

Despite subtle differences of opinion across the 28 EU MS, the European Council states CNI as:

> '[A] n asset, system or part thereof located in member states that is essential for the maintenance of vital societal functions, health, safety, security, economical or social well-being of people, and the disruption or destruction of which would have a significant impact on a member state as a result of the failure to maintain those functions.
>
> (European Council, 2008)

This definition will be analysed in detail in the main body of this report and correlated with definitions from MS in order to identify any disparity in the collective thinking across the EU. It is important to focus some research effort in this particular area in order to gain a deep understanding of the current state of CIP in the EU. Effort will also be applied to identifying the detail contained within the definitions, what infrastructures are considered to be critical, the THREATS project team will evidence if this is consistent across all EU MS?

1.9 Terrorist attacks on Hospitals: Risk and Emergency Assessment Tools and Systems (THREATS) is a project with a clearly defined aim and set of objectives, which can be viewed in detail at www.threatsproject.eu. The project will seek to challenge and develop models and risk assessment tools, through case study and applied to a major EU hospital infrastructure. Simulations will consider multiple attack methods, including second strike scenarios and attacks to water supply. Hospital activity will be carefully analysed to include medical and commercial activities in order to design appropriate tools and systems that are useful within all functions of a hospital. The potential results from the THREATS project will be to empower EU MS with wide and efficient capacity assessment tools to measure critical healthcare infrastructures' vulnerability to terrorist attacks. Guidelines designed to harmonise and optimise preparedness of hospitals' healthcare infrastructure will be disseminated to security authorities and operators at EU level to enable the efficient prevention of major

potential attacks and associated burdens. THREATS ultimately aim to increase the resilience of EU hospitals as a critical infrastructure by improving their protection capability and security awareness. The project will build upon the current and previous work carried out under the European Programme for Critical Infrastructure Protection. This report provides the initial assessment of the current state of CIP within the EU and will analyse the level at which health infrastructure has been included as part of the CIP planning process.

1.10 Hospitals provide the primary point of delivery of health care to the population and form a network of general and specialist disciplines to cater for the density of population. In general EU regional trauma centres are often located close to large urban areas and transport infrastructure and provide the wide range of specialist trauma and general medical services. In the smaller towns and rural areas general hospitals provide a similar function but on a smaller scale. Specialist care is referred to the regional centre as necessary. A critical failure of a regional centre could have a significant impact on the immediate population and the interdependent network of general hospitals. It is difficult at this early stage of the project to state with any scientific certainty the level or wide spread of impact of any such failure but the potential is worthy of consideration.

There are many specific and specialised challenges that arise from including hospitals as part of CNI. Major hospitals, by definition, are open 24 hours a day and provide free access to anyone seeking medical attention. To that end local security measures must be balanced with providing the appropriate level of security to protect staff, patients and resources but without impeding access to the public. Many hospital facilities rely upon ‘good will’ and the security resources are focussed upon a small number of threats e.g. combatant patients whom may be under the influence of drugs or alcohol. *Prima facie* the lack of published data relating to counter terrorist security measures at EU hospitals indicates the limited consideration applied to the potential threat, though THREATS will seek to address this theory and provide evidence to support or deny the presence of effective security measures in place at EU hospitals.

There are many influencing factors that must not be overlooked as the THREATS project progresses; they include the appetite to risk at government and health organisation level, public perception, health care worker tolerance to working within a security controlled environment and the overall public image of hospitals. Key considerations in designing security measures for hospitals include the physical protection of its buildings and assets, the security of its staff, patients, visitors, and the protection of data and information.

1.11 Although much work relating to CIP has already been done across the EU the current state of affairs is difficult to establish, particularly relating to health infrastructure. The European Council (2008) has stated an objective to develop a common standard across all EU MS that will provide individual MS with a road map to develop their national CIP policy and physical measures and will begin to reduce the vulnerability of interdependence by providing a measurable standard for MS's to protect their infrastructure. A collaborative approach supported by the EU will enable EU resources to be allocated and applied to those MS that are struggling to attain the agreed standards. The common approach also enables EU resources to have greater effect if called upon to support a national contingency because they should be interoperable and operating to a common standard. The THREATS project will work specifically in the field of health infrastructure and design common tools and practices that can support health providers in all EU MS to design and implement a sustainable and effective CIP policy.

It is important to gain an accurate understanding of health infrastructure protection across all EU MS; therefore this report will present findings that outline the current state of CIPs. The findings will provide context to the project tasks and enable research effort to be applied in the appropriate areas that will develop the collective body of knowledge. The findings contained within this report and the experience of the THREATS team indicates that differing perceptions and risk appetites exist within the EU MS, due in part to the diverse nature of each Member states infrastructure protection needs. THREATS acknowledge this variance and will develop generic guidance in such a form as to enable it to be utilised to satisfy this variance in requirement; e.g. according to the European Healthcare Federation (HOPE, [n.d.]) there are 26 hospitals in Slovenia comprising of 10 general, 10 specialised and 6 tertiary hospitals with an additional 3 private hospitals to serve a population of

2,052,496 (as at 2011) compared to France which has in total 2,698 hospitals serving a population of 65,114,688 (as at 2011). This provides a short insight to the difference in scale of health infrastructure between two EU MS and the difficulty in coordinating a huge number of hospitals over a large geographic area compared to a much smaller scale. Other differences are likely to exist and should become more apparent as THREATS progresses and although each MS will have a unique view constrained to their own national needs interdependency; although not always apparent; will play a role which highlights the need for a common standard and set of tools.

1.12 The THREATS project has been carefully designed to ensure each task develops the collective understanding of the topic in a progressive and cumulative manner. Deliverable 1 is contained within this report and has two clearly defined objectives:

a. Analyse which European countries include the health sector as part of their Critical National Infrastructure.

b. Analyse which European countries have identified Critical National Infrastructure assets within the Health sector.

The scope of the report has been constrained to publically available research data in order to ensure the results are objective and reflective of the current state of affairs, so far as published data can reveal. The report will not seek to provide new information or theories at this early stage of the project because the focus will be current publicly available research data. This approach has been influenced in anticipation of security of protectively marked material, specifically the level of security applied to material relating to CIP and the limited access and disclosure issues at this early stage of the project. Ethics and disclosure will be managed as THREATS develops.

2. Literature Review

2.1 It is important to establish a measurable definition of Critical National Infrastructure in order to understand the task of providing adequate protective measures. In order to minimise the likelihood of expending effort and resource protecting the wrong infrastructure or providing suboptimal protection to infrastructure that is likely to fail under test of a real-time event.

The research has revealed significant differences between EU MS levels of published data relating to CNI protection. Some MS have published a national strategy document that is available from official government websites; the documents provide definitions and terms of reference that state the aim and objectives of the strategy. However, other MS have not published a national strategy but other data exists that indicates work has been done within the field of CNI protection. In many cases EU MS relate their national strategies directly to the EC Directive (2008/114/EC) and provide very little information specific to the national perspective.

In terms of a national perspective the UK and Germany provide good examples of easily accessible strategy information that clearly defines CNI and the overarching plan to provide suitable and adequate resource to safeguard continuity.

The UK Government has acknowledged the importance of defining national infrastructure to provide 'clarity and consistency when considering whether infrastructure is critical' (Cabinet Office, 2010:8). The methodology adopted by UK policy makers maintains a focus at national level but also considers the impacts at local level and the effects upon the public. National infrastructure is separated into two groups: national infrastructure and critical national infrastructure. The purpose of defining which sectors are critical ensures protective efforts are proportionate to the importance of the sector. The UK policy goes further to acknowledge that some infrastructure is critical at a national level whilst other critical infrastructure is critical at a local level. The policy states the importance of this distinction as:

> 'This will enable assets, systems or networks not otherwise deemed as Critical National Infrastructure to be evaluated and included within the

> Programme if doing so would be appropriate and proportionate. However, the risk-based approach that underpins the Programme means that initial vulnerability analysis will focus on the Critical National Infrastructure.'
>
> (Cabinet Office, 2010:8)

The German Ministry of the Interior demonstrate a more inclusive approach and assert that CNI is the responsibility of 'society as a whole' that requires the support of 'government, business and industry, and the general public' (MOI, 2009). An inclusive approach requires a level of definition to ensure all parties are working to a set objective or understand their individual duties. To that end the German government define CNI as:

> 'Critical infrastructures (CI) are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences'.
>
> (Federal Republic of Germany, 2009)

The definitions across the EU relating to national and critical infrastructure are varied, though the differences are often subtle and specific to the country's needs. Renda provides a useful summary of the EC definition of the terms 'critical' and 'infrastructure':

> '… "**critical**" refers to infrastructure that provides an essential support for economic and social wellbeing, for public safety and for the functioning of key government responsibilities, such that disruption or destruction of the infrastructure would result in catastrophic and far-reaching damage. National definitions of "**infrastructure**" refer to the physical infrastructure and often also tangible assets/or to production or communications networks'. (2010:22)

2.2 Even with a published EC Directive Renda suggests the debate is ongoing and agreeing a definition is still 'a moving target' (2010:22), which becomes increasingly apparent when the definition debate is examined further. Defining critical

infrastructure is probably achievable in the short term; the EC definition goes some way to harmonising the collective thinking. Finding a consensus regarding which parts of infrastructure are critical might be a greater challenge.

The German government divides critical infrastructures into sub-groups:

> 'Critical infrastructures may, with reference to their technical, structural and functional specifics, be classified as vital (absolutely essential) technical **basic infrastructure**, on the one hand, and vital (absolutely essential) socio-economic **services infrastructure**, on the other hand'.
>
> (MOI, 2009:7)

This adds an additional layer to the 'critical' debate and that it provides an unnecessary complication by sub-dividing the critical layer of infrastructure. However due to the diversity, perception and risk appetite of the different EU MS this sub division may be necessary in determining the priority of action in reducing vulnerability and increasing protection.

The Romanian government has adopted a variation on the German approach by grouping infrastructure into three discrete groups: common infrastructures, special infrastructures and critical infrastructures. The Romanian Intelligence Service provides the following description to define each group:

> 'Common infrastructures representing a framework structure, ensuring the construction and functioning of a system; Special infrastructures playing a consistent role in the functioning of systems and processes, with a high degree of stability and security within the regional complex of economic and social life mechanisms. These types of infrastructures, subject to dysfunctions and vulnerabilities, which also exist in an insecure climate, may be considered "critical"; Critical infrastructures are, in general, vital for the stability, security, and safety of systems and processes, playing an important role in the economic, social, political, and military field. These infrastructures' criticity degree is determined by the significant consequences triggered by their disruption or destruction, including for a very short period'.
> (2009)

This definition contains a degree of ambiguity and leaves the readers to interpret the definition based upon their own understanding of CIP. In this case it seems as

though infrastructure sectors are managed as separate silos and there has been no provision made for cross-sector impacts from a single risk.

Some EU MS seem to be content with the definitions stated by the EC whilst other MS are yet to engage in the debate or state their agreement with the EC directive. Bulgaria is one such state that has very limited publicly available information and during the research phase of this report limited information was identified. However the research did discover an article relating to information security in Bulgaria that indicated an awareness of CNI. Nickolov (2005) provides a list of sectors that 'need to be functioning at least at a minimal level for the private and public sectors to be able to survive'. He comments further to suggest 'the energy supply and the communication systems can be regarded as crucial since the rest of the infrastructures depend on them in order to function properly'. Although this theory is not necessarily incorrect there is lack of detailed analysis to show the level of interdependency within all the sectors. The article was specifically about information security in Bulgaria and therefore the bias is not surprising but does little to develop the Bulgarian CIP strategy and draws policy makers to focus on two sectors that are perceived to be 'crucial'.

The UK government has adopted a different approach whereby a list of national infrastructure sectors has been compiled as follows:

a. Communications
b. Emergency Services
c. Energy
d. Financial Services
e. Food
f. Government
g. Health
h. Transport
i. Water

Each sector is considered important though 'certain critical elements of national infrastructure that if lost would lead to severe economic or social consequences or to

loss of life in the UK' (Cabinet Office, 2010:8). These critical elements form the critical national infrastructure (CNI) in the UK and are documented in the National Risk Register with the potential threats and exposure to risk (National Risk Register of Civil Emergencies, 2013). The strategy is managed as a Risk-Based approach and enables interested parties to adapt to changing circumstances and apply appropriate effort in direct relation to the most significant risk at that time. This is in contrast to the theory outlined by Nickolov (2005) whereby energy supply and communication systems were stated as the critical sectors of infrastructure. It is difficult to identify a scenario where only a single sector is impacted, which provides further weight to the theory of interdependency and the interconnected world.

2.3 Methods for identifying critical infrastructure include the subsidiarity approach. According to Recommended Elements of Critical Infrastructure Protection for Policy makers in Europe: Good Practices Manual for CIP Policies (RECIPE) (2011:15) this approach has been tried in the United States of America and elsewhere, though it has been discontinued at national level. The second method is the top down approach whereby the critical infrastructure sectors are defined at strategic level and specific elements of the CNI sector are listed as critical. In simple terms the energy sector; for example; may have many important elements that are represented as national infrastructure but only a few elements of the sector are actually critical; such as electricity generation or distribution of gas, oil and electricity. This approach is reflective of the UK and German strategy and enables each sector to be analysed in detail against a set of threat and risk criteria. This improves efficiency and application of protective measures.

2.4 In 2006 the French government recognised the need to improve coordination and physical protection measures to critical infrastructures and published a decree for the 'Safety of Vital Importance of Activities' (SAIV). SAIV (2006) recognises the 'operator based approach' to identifying CNI and is utilised throughout the French CIP programme and is underpinned by a 'strong "mandated" legal basis for cooperation' and a system dating back to the 'cold war' with strong 'traditional connections with professional and industrial associations' that creates a system whereby vital operators are identified instead of the vital service. This enables the French government to make a provision to ensure the threats are identified and risks managed by the operator of the site/service.

The benefits of this approach include the use of the 'knowledge worker' or group of people with real expert knowledge who are also in a position to enable the bespoke solutions for their service/sector. However, the system relies upon close liaison between agencies and organisations to ensure emerging threats are relayed to all parties and best practices are shared across public and private organisations.

RECIPE (2011:17) provides detail to assist policy makers and practitioners to identify critical infrastructure and outlines a methodology that can be applied to all sectors: identify sector specific criteria, assess criticality, assess dependency issues and apply crosscutting criteria. The critical elements of CNI protection are managed appropriately by the EC and MS respectively; therefore the detailed criteria are not available for deeper analysis.

2.5 In this short review of the current situation the different approaches to CIP across the EU are clear and the prospect of a unified approach within the EU remains distant. The research has identified similarities within national CIP strategy and extensive work by the EC to coordinate a common approach but commonality between MS is still lacking. The Centre for European Policy Studies (CEPS) task force (2010:15) illustrate the lack of cooperation between nations when dealing with critical information infrastructure protection (C(I)IP and highlight on the absence of a unified or coordinated emergency response to potential threats.

2.6 In order to develop an EU CIP strategy that is flexible, adaptive and fit for purpose in all MS a common approach, including language, is required. The Polish Rządowe Centrum Bezpieczeństwa (Government Centre for Security) have a publicly available website that provides links to various security related strategy documents, including CNI but the specific strategy documents are only available in Polish. Arguably the impetus for a European CNI strategy comes from the EC and therefore the Polish national documents, available in the national language, represents a less inclusive approach.

It is likely that the Polish language issue is an oversight though other MS

governments have also published in their own language. EU MS must remain cognisant that there are currently 28 different member states within the EU and therefore a common operating language is prudent. The EC already utilises English as the common language based on the wide use of English throughout Europe and the world in terms of civil protection and disaster management internationally.

The use of a common language is not a new concept and has been used in the commercial sector for generations. The use of language must remain the prerogative of the MS but progress must be made with the EU in mind.

2.7 The commercial sector is now a key player in the field of CIP and approximately 85% of CNI are owned by the private sector (CEPS, 2010:14). This means that government alone cannot manage CIP and the implementation of protection systems must be conducted in a manner that does not impede the commercial business from making a profit or remaining competitive.

Public-Private Partnerships (PPP) have traditionally been contractual agreements between the public and private sector but the growth of CNI within the private sector has created the demand for a closer relationship between the two sectors. In simple terms ‘with the current majority of CI in private hands and the responsibility for civil protection and emergency preparedness in public hands, PPPs are essential for meeting contemporary threats’ (RECIPE, 2011:39). The Crisis and Risk Network (2009:8) makes it very clear that PPPs are ‘much more than a delegation of public tasks to private players’, the benefits can be seen where specialist expertise, capability and capacity is developed to support a priority function. The RECIPE manual uses the building of the Channel Tunnel as a case in point where mutual cooperation was developed between private and public organisations, the risk was owned and managed by the private sector which meant it was in their interest to ensure the risk management system was robust enough to respond to threats/risks without impacting the project or consuming the potential profit margin.

The private sector responsibility and participation in the CNI protection programme is present in the health sector. There are examples of hospital buildings that are constructed by private companies and leased to the health authority under a system where the health provider is simply the tenant and the building provider fulfills the role of landlord and facility manager.

2.8 Specific details relating to hospital infrastructure has not been identified during the research phase of this report and will probably require additional field research to generate data. However the research has identified that health is a sector common to all CNI strategy documents reviewed. The Romanian Intelligence Service provides some useful though limited detail relating to their health sector; as listed within the Romanian CNI: 'health and hospital care; drugs, serums, vaccines and pharmaceutical products; Bio-laboratories and bio-agents' (2009:23).

More research is required to identify data relating to the detailed protective systems for health infrastructure across the EU but the information contained within this report provides a convincing indication that the hospital infrastructure; the networks of medical and hospital capability within regions, nations and perhaps as wide as the EU; are interconnected or interdependent in ways that have previously been underestimated. In order to frame this theory the question could be asked: 'if a coordinated terrorist attack was executed against a regional trauma centre and outlying general hospitals what would the impact be to the health sector within that region, nation and across the EU?'

2.9 The likelihood of a terrorist attack against a hospital or health facility is difficult to comprehend in the developed world. The Geneva Conventions (1949) provides protection under international law to non-combatants, infrastructure and humanitarian organisations and their activities. In 1977 the Additional Protocol II was invoked which provided additional protection: 'Article 9 – Protection of Medical and Religious Personnel, Article 10 – General Protection of Medical Duties and Article 11 – Protection of Medical Units and Transport'.

Unfortunately the Geneva Conventions (1949) and Additional Protocol II (1977) are only as effective as international monitoring and enforcement of international law. Furthermore, the rule of national and international law is not recognised by terrorist organisations, which highlights a paradox relating to the Provisional Irish Republican Army (PIRA). PIRA attempted to claim prisoner of war status throughout the campaign in Northern Ireland, specifically during the H Block hunger strikes at the Maze Prison, but successfully targeted Musgrave Park Hospital in 1991 (Ganor and Wernli, 2013:28) in contravention to the Geneva Conventions (1949).

2.10 The literature provides a rich picture of the extent to which hospitals have been targeted during various conflicts and civil unrest throughout the world. Ganor and Wernli (2013:1) assert 'approximately 100 terrorist attacks have been perpetrated at hospitals worldwide, in 43 countries on every continent, killing approximately 775 people and wounding 1,217 others'. This data demonstrates the vulnerability of hospitals, highlighting them as potential soft targets. The goodwill of humans and legal precedence such as the Geneva Conventions or international law do not provide sufficient assurance to ensure hospitals remain a safe haven.

2.11 The case studies provided by Ganor and Wernli (2013) are compelling but it should be noted that each incident occurred in a conflict zone. Other evidence suggests that hospitals are not just vulnerable to terrorist attack but also other types of organised violence. Brown (2012) suggests hospitals are 'turning more and more into places of immigrant violence'. His comments come in the wake of an incident at Odense University hospital, Copenhagen when a 'group of about 70 men, some armed with "cudgels", invaded the Odense University emergency ward' in response to a previous incident between rival groups which resulted in one man receiving a gunshot wound. His subsequent treatment at the hospital initiated the mob attack. Brown reports that police were already present at the hospital and had to discharge their firearms as a warning and disperse the mob (2012).

But further research has shown that the Copenhagen incident is not an isolated event. Israeli (2008:204) describes the rise of violent incidents in French hospitals from 145 attacks in 2004 to more than 200 in 2006. Although the attacks discussed

by Israeli are often a single person perpetrating an attack against a single health worker, the perpetrators are from the same religious background/ethnic group, which presents a worrying trend. Furthermore this data demonstrates a lack or regard for the sanctity of hospitals over pious conviction or ideology by a section of society.

This theory is relevant to the research and will be useful when THREATS progresses to analyse the threats to hospitals.

3. Methodology

3.1 Before presenting the results of the research that has been conducted to support this report it is important to understand the research approach and how data has been collected, analysed and presented. Although the field of CIP is not new, some problems relating to available data were anticipated and others were encountered along the way. This chapter will explain the contingencies and solutions that were implemented to facilitate the research. The field of CIP has become more transparent as better engagement between public and private agencies has developed and EU guidance and direction has been issued, but certain areas of CIP remain protected and undisclosed for security reasons.

3.2 An initial feasibility study was conducted to identify if data was available and accessible within the public domain. The study was simplistic and entailed an Internet search of EU MS using various public search engines and a variety of CIP terminology. The initial trawl resulted in a significant number of positive results and the research team were confident that a thorough search of publicly available data would harvest valuable results.

3.3 The aim of the first research task was to collect information that could be analysed in order to establish the current status of CIP across all EU MS. Working within the time frame of the overall project and the restrictive nature of data protection within CNI security protocols that the scope of the research has been drawn from publicly available data. This approach would focus on information that was immediately available for review and was not subject to disclosure sensitivity issues. However, it was acknowledged that other meaningful data may exist within organisations but had not been made available to the public because of administrative or disclosure issues.

Limited information exists in ‘hard copy’ published material such as books and journals. Although many government documents are available in print form, there is a cost and lead-in time implication to obtaining physical copies. However the availability of the material online provides greater access to material. The results were collated, analysed and used to redefine a further search. In addition, EU MS

government websites were visited to identify relevant information. A simple sampling analysis method was utilised whereby documents were briefly assessed by the research team and their content analysed to ensure they were relevant to the research.

The first trawl harvested a large amount of data and it was important to follow a strategy for selecting relevant data and dismissing data that was of no use. The tertiary data provided further references to secondary data. Information was available in government white paper documents, including EC level strategy documents. Other information was available in reports, journals, newspaper articles and books. Although much of the data provided a valuable source of secondary data it also provided references to other relevant works.

3.4 In order to focus the efforts of the research team on the most relevant information a strategic approach was taken to harvesting data, focussing on publicly available information in English. This methodology was adopted to avoid becoming overwhelmed with data of limited value. The model defined by Saunders, Lewis and Thornhill (2009:60) illustrates a review spiral that goes through distinct phases in repetition and enables the research parameters to be filtered and redefined throughout the process. This model was adopted and applied to the review of literature for this study, a process that continued throughout the creation of this report until the closing stages (King and Wincup, 2008:19).

3.5 The importance of validity, accuracy and relevance have been considered throughout the research phase and a constant referral to the research question has been applied to ensure the research approach has maintained focus in the correct area. The problem of other data in existence that has not been made publicly available and the potential findings of this report being inaccurate or not providing a full ‘picture’ of the current state of CIP within the EU were discussed. However, it must be remembered that this report represents the initial examination of the situation within the EU and the project will be progressive and accumulative. It is likely that the project team will engage governments and partner agencies in due course and other data will become apparent. It is anticipated that as further research and evidence is obtained that the report will become more dynamic.

4. Findings

4.1 In general the findings indicated that the status of CIP across the EU is disparate. The EC has issued direction (EC, 2008) to implement CIP in each EU MS but the coordination of effort at EU level has not been effective to ensure all MS implement CIP to a required standard within an agreed timeframe. Furthermore, the coordination at national level within each EU MS is suboptimal and was apparent during the research for this report. Some MS governments' have not taken a lead role to develop their national strategy but have relied upon private and research organisations to develop contingencies. Moreover, the supporting policy directives are often a 'cut and paste' of EC policies, with very little detailed consideration for the national needs.

4.2 A table of findings, listed by MS can be found at Annex A to this report. The findings indicate that only 60% of EU MS government websites contain any direct reference to CIP within the narrative and only 21% of EU MS governments provide a link to a national strategy or policy document. These findings are surprising when considering the importance of CIP at a national and EU level. This research has only analysed publicly available data collected from a series of internet trawls and has not taken into account any data that is available upon request from the MS. This is due to the overall timetable of the THREATS project. Furthermore, the research has not been able to consider unpublished data nor has it analysed closed communication networks or lines of communication between government and CNI operators; which is not disclosed due to national security issues.

4.3 The literature review identified the utility of PPPs and stated that a growing percentage of CNI was owned and managed by the private sector (see para 2.7). The management of CNI still requires a strategic level management plan to ensure coordination between regions and suppliers but this research has identified 25% of EU MS being reliant upon the private sector to manage and develop the national CIP strategy. The management of CIP by the private sector seems a logical way to proceed and ensures the subject matter experts within a specific sector are closely involved with ensuring the national infrastructure is maintained and developed in a manner that ensures an optimal service. However, in some cases the evidence

indicates that the government have a 'light touch'; assessed by the lack of CIPs strategy/policy directive contained on the official government website; and are not closely involved with the management of CNI at a national level and cutting across to the EU to ensure the national strategy and CIP activity are in harmony with other neighbouring states and the EU.

4.4 Language barriers and problems relating to definitions and research terminology were anticipated and discussed within the methodology. However, despite contingencies and extensive searches two MS provided very limited results that indicate a lack of CIP at national level. It is possible that CIP activity already exits within those states but a coordinated national programme and a published strategy have yet to be identified.

The research has provided an interesting observation that many academic or research organisations are now engaged within the CIP field providing theoretical support to policy makers and operators. In many cases, research organisation names and titles give the impression that they are the national lead or centre of excellence for all things CIP. It will be interesting to develop this observation further to identify the value added by academia.

Analysis of available data has identified use of common terms and practices but is limited to those MS with a more developed strategy. Overall, the use of common language, terms and practices across the 28 MS seems to be limited and there are many cases where terms and definitions provide the same meaning but are written with subtle differences, as illustrated by the literature review.

4.5 The research identified very limited training, exercising and testing as part of the overall effort to improve vulnerability reduction and consequence management as part of good practice. But good examples of training, exercising and testing can be taken from the Civil Protection Network (CIVPRO), which was established in 2006 by the EUROBALTIC II Project for Civil Protection, part of the Civil Protection for Baltic Sea states. CIVPRO manage an on-going exercise programme that provides practical training for emergency responders to civil emergencies. The research team are aware of national level exercise programmes that are being conducted in other

MS but are not publicly available. To that end, it is likely that other comprehensive training, exercising and testing is being conducted in other MS and may become more visible to THREATS as the project develops.

4.6 Some of the data collected indicated a prioritisation by some states to focus upon cyber and information security, otherwise referred to as critical information infrastructure protection (CIIP). Although CIIP is a critical element at a national and EU level, risk and threat assessment methodology must avoid any bias towards a particular sector and ensure a holistic approach to societal risk. The literature review identified information that provides a cogent argument that each sector of national infrastructure is important though only elements of each sector are critical. This needs to be read in context to specific threats and potential crisis scenarios to understand that it is difficult to separate sectors when considering which is more important.

4.7 A lack of information relating to the health sector of CNI was identified during the research process. The team agreed that contingency plans are likely to be held at local level, though the research indicated that detailed strategy direction was lacking, which in turn is a potential sign that coordination between health authorities within a MS and overall coordination at EU is likely to be uncoordinated. Once again, the picture is based on a ‘snap shot’ research of publicly available data and the reality might include a well-coordinated and common approach at national and EU level.

5. Conclusions and Recommendations

5.1 This research has illustrated that although CIP activity is underway in many of the EU MS, and the EC have provided strategic direction, the overall collective approach remains uncoordinated and not effective to bring all states up to a common standard. The EU must identify a measurable standard that is fit for purpose in measuring effectiveness of CIP within all MS. A common standard is vital if the EC intend to establish an effective EU level CIP policy and programme because 'what gets measured get done' as asserted by many business organisations to mean something must have a criteria by which the performance can be measured and managed. Without a measurable standard it will be difficult to identify progress and difficult to bring all MS to the same level of compliance. The risks associated with interdependencies have already been discussed and the problems associated with one group undertaking CIP to a high level only to be undermined by a country that have been less diligent.

5.2 A common standard and measure of performance is feasible. There are numerous organisations; such as the International Standards Organisation (ISO); which accredit various industries to conduct their activity in an appropriate manner and to an agreed standard. Accreditation to standards such as ISOs provides assurance to stakeholders and the public that the operation is being conducted responsibly, with due care and a level of accountability exists within the organisation.

5.3 The research has shown that CIP activity exists but the level of coordination at EU level is currently lacking. There is collective effort in some regions, such a CIVPRO in the Baltic States, but the collective approach needs to be implemented to greater effect within some MS and at EU level. The research organisations currently engaged with CIP need to optimise their collective learning and share information to ensure the research benefits the EU as a whole. Some EU MS that have less resource and finance will undoubtedly benefit from the collective effort; the inclusion of the less developed countries to the collective effort will ensure they pose less of a risk in terms of interdependencies.

5.4 The research has not identified any detailed work specific to health as a sector of CNI. The project team acknowledge that the scope of the research for this report has been constrained to publicly available data and therefore evidence that has not met the research criteria may exist. However, due to the lack of published information specific to health indicates that work is likely to be localised within individual hospitals or health authority regions. Further investigations are required to confirm this theory but the THREATS team anticipate the need for more investment and attention by governments and health authorities.

The THREATS project is timely and will very likely add value to work that has already been done within the EU and work that will continue to develop the collective knowledge. Close engagement with health sector stakeholders will be vital; as the project develops to ensure the research remains valid and reflects the reality within the sector. Furthermore, the systems and tools that are intended to result from the overall project must be user friendly and fit for purpose and a closer collaboration between the THREATS team and the end user will ensure the final outcome is valid and implemented as part of routine activity.

6. References

[Anon.] [n.d.] *Hope exchange programme 2015: Hospitals in the Member States of the European Union* [online]. HHE. Available from: http://www.hope.be/03activities/quality_eu-hospitals...

[Anon.] (2014) *EU Committed to helping Serbia, Bosnia and Herzegovina* [online]. EurActiv. Available from: http://www.euractiv.com/sections/global-europe/eu-committed-helping-flooded-serbia-bosnia-and-herzegovina-302236

Brown, S. (2012) Hospital Terror In Denmark. *Front Page Magazine.* 24 August, p 1-3. Available from: http://www.frontpagemag.com/2012/stephenbrown/hospital-terror-in-denmark

Cabinet Office (2013) Preparation and planning for emergencies: responsibilities of responder agencies and others. HMSO: London. Available online at www.gov.uk

Cabinet Office (2010) Strategic Framework and Policy Statement: on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. London: HMSO. Available online at www.gov.uk

Critical Infrastructure Warning Information Network ([n.d.]) *CIWIN* [online]. Available from: https://**ciwin**.europa.eu/

Crisis and Risk Network (2009) Focal Report 2: Critical Infrastructure Protection. Zurich: ETH. Available from: www.css.ethz.ch/publications/pdfs/**Focal**-**Report-2**-CIP.pdf.

Enhance Project (2014) *When the EU encounters forest fires...*[online]. Available from: http://enhanceproject.eu/news/articles/73

European Commission (2001) *EU Civil Protection Mechanism.* Brussels: European Commission. Available from: http://ec.europa.eu/echo

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

European Council (2005) *The European Union Counter-Terrorism Strategy.* Brussels: European Council. Available from: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33275_en.htm

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

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

European Commission ([n.d.]) *ERNCIP Project Platform* [online]. Brussels: European Commission. Available from: https://**erncip**-project.jrc.ec.europa.eu/

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

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

Israeli, R. (2008) *The Spread of Islamikaze Terrorism In Europe: The Third Islamic Invasion.* Middlesex: Vallentine Mitchell

King, R.D. and Wincup, E. (2008) *Doing Research on Crime and Justice.* Oxford: Oxford University Press.

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

Renda, A. (2010) Protecting Critical Infrastructure in the EU: CEPS Task Force Report. Brussels: Centre for European Policy Studies

Romanian Intelligence Service (2009) Critical Infrastructures Protection. Bucharest: SRI. Available from: www.sri.ro/upload/Brosura%20IC%20ENG.pdf

SAIV (2006) Sectors of Activity of Vital Importance. France: 2006. Cited in RECIPE (2011) *Good Practices Manual For CIP Policies.* Brussels: European Commission.

Saunders, M., Lewis, P. and Thornhill, A. (2009) *Research Methods for Business Students.* 5th ed. Harlow: Pearson Education.

Union for the Co-ordination of Transmission of Electricity (2007) *System Disturbance on 4 November 2006: Final Report.* Brussels: Union for the Co-ordination of Transmission of Electricity. Available from: https://www.entsoe.eu/fileadmin/user_upload/_library/publications/ce/otherreports/Final-Report-20070130.pdf

7. Bibliography

Monti,M.(2010) A New Strategy For The Single Market: Report to the President of the European Commission. Brussels: European Commission. Available from: www.ec.europa.eu/bepa/pdf/**monti_report**_final_10_05_2010_en.pdf

Rennie, D. (2006) Muslims Challenged by Gynaecologists. *The Daily Telegraph.* 23 October 2006. Available from: http://www.telegraph.co.uk/health/healthnews/3344291/Muslims-challenged-by-gynaecologists.html

Annex A – Research Findings – Listed by EU MS

Ser	EU MS	Published CIP Policy – Y/N	Health included as CNI and listed in policy?	Policy Reference/ link	Bibliography – other relevant data
01	Austria	Y No reference on government website but inference to CIP within OIIP document.	Y OIIP provide CIP information in Austria and reference to RECIPE manual.	https://www.bka.gv.at/site/3539/default.aspx	http://www.oiip.ac.at/en/institut/institution-outline.html https://www.tno.nl/content.cfm?context=thema&content=inno_publicatie&laag1=893&laag2=910&laag3=1&item_id=836&Taal=2
02	Belgium	Y No reference on government website but inference to CIP within CEPS task force document.	Y	http://aei.pitt.edu/15445/1/Critical_Infrastructure_Protection_Final_A4.pdf	http://www.irsd.be/website/media/Files/Focus%20Paper/FP15.pdf
03	Bulgaria	Y Focus is on energy and cyber infrastructure.	?	http://www.mi.government.bg/en/themes/critical-infrastructure-warning-information-network-ciwin-333-300.html	http://www.comw.org/tct/fulltext/05nickolov.pdf

04	Croatia	N No reference on government website and no other relevant data identified.	N	www.mvep.hr/en/	
05	Cyprus	Y No reference on government website but Cyprus safety Platform identified.	?	http://cyprussafetyplatform.blogspot.it/2012/08/22nd-february-2012-1st-workshop-of.html www.**cyprus**.gov.cy/.../gwp.getCategory?...**Government**%20**Websites**...	http://www.kios.ucy.ac.cy/critis2014/ https://www.ciprnet.eu/consortium.html http://www.euc.ac.cy/easyconsole.cfm/id/788/course_id/2205
06	Czech Republic	Y Reference to CIP and links to EC directive contained at the Ministry of Interior website	N	http://www.hzscr.cz/hasicien/article/crisis-management-in-the-czech-republic.aspx	http://www.sersc.org/journals/IJDRBC/vol3/5.pdf
07	Denmark	Y	? No reference to health infrastructure	http://brs.dk/eng/inspection/contingency_planning/Documents/RVA-model_user_%20guide.pdf	http://brs.dk/eng/aboutus/international_coorporation/Pages/international_co_operation.aspx

08	Estonia	Y Reference to CIP not on government website but on Information System Authority website with bias to CIIP	? No reference to health infrastructure	https://valitsus.ee/en	https://www.ria.ee/CIIP/
09	Finland	Y Reference to CIP not on government website but on Civil Protection Network website	? No reference to health infrastructure	http://www.helsinki.fi/aleksanteri/civpro/thdata/cip.htm http://www.valtioneuvosto.fi/etusivu/en.jsp	
10	France	Y	? No reference to health infrastructure	http://www.gouvernement.fr/english	http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf http://www.cert.ssi.gouv.fr/ www.agence-nationale-recherche.fr/.../franco-german-coordinated-call-f...

11	Germany	Y National CIP strategy document available at Ministry of the Interior website	Y Reference to public health contained in strategy document.	https://www.bsi.bund.de/EN/Topics/Criticalinfrastructures/criticalinfrastructures_node.html	
12	Greece	Y? Reference to a CIP workshop (Project ARGOS) at Ministry of Public Order and Citizen Protection website, but no evidence of national strategy	N	www.kemea.gr/index.php/en	
13	Hungary	Y No strategy document on government website but detailed CIP presentation available from Ministry of Interior	Y Health listed as CNI sector in MOI presentation	www.kormany.hu/ www.katasztrofavedelem.hu/letoltes/iparbiztonsag/lrl/CIP_EN.pdf	http://www.cert-hungary.hu/en http://www.webcastlive.es/4enise/archivos/P11/P11_Ferenc_Suba.pdf
14	Ireland	Y There are various documents; that make reference to	? Emergency/crisis management document identified which incorporated health response, but no	http://www.gov.ie	http://www.dcenr.gov.ie/NR/rdonlyres/7900740B-E0BC-4ED9-966C-7366DD04A08D/0/Trans

		CIP; listed on the government website but research didn't identify a single overarching national strategy document	reference to CIP.		missionandOtherEnergyInfrastructure.pdf http://www.epa.ie/researchandeducation/research/fundingopportunities/europeanfunding/h2020sc5focusareas/disaster-resiliencesafeguardingandsecuringsocietyincludingadap/#.U-nKEXwcTIU
15	Italy	Y There are various documents; that make reference to CIP; listed on the Ministry for Civil Protection website but research didn't identify a single overarching national strategy document. Italy contributes to CIVPRO (see Finland).	Y Reference made to health as a CNI sector in the Project TENACE report	http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf	http://www.protezionecivile.gov.it/jcms/en/homepage.wp http://www.infrastrutturecritiche.it/aiic/index.php?option=com_content&view=article&id=219&Itemid=125 http://www.isticom.it/documenti/news/pub_003_eng.pdf http://www.dis.uniroma1.it/~tenace/download/deliver

					able/Report_tenace.pdf
16	Latvia	Y Cabinet Regulation no.496 issued but no detail of strategy identified.	? No evidence of CIP strategy inclusive of health identified.	http://www.google.it/url?url=http://www.vvc.gov.lv/export/sites/default/docs/LRTA/MK_Noteikumi/Cab._Reg._No._496_-_Identification_of_Critical_Infrastructuresx_Including_European_Critical_Infrastructures...doc&rct=j&frm=1&q=&esrc=s&sa=U&ei=IO7pU8KAJ46BPaKzgZgM&ved=0CCwQFjAD&sig2=GcXYAc4JAasrPxD4rHZ_2g&usg=AFQjCNGuTq17RS5HkM-ZE4M7dXYse6lZpA	www.mk.gov.lv/en/
17	Lithuania	Y Reference to CIP not on government website but on CIVPRO website.	? No reference to health infrastructure.	www.lrv.lt/	http://www.helsinki.fi/aleksanteri/civpro/publications/WP6.pdf
18	Luxembourg	N No reference to CIP identified on government website.	N No documented evidence found.	https://www.gouvernement.lu/	http://www.112.public.lu/organisation/administration/organisation/protection_civile/index.html
19	Malta	Y	Y	http://ciipmalta.gov.mt/about	http://ciipmalta.gov.mt/ho

		No strategy document identified but clear referencing to CIP on government website.	No strategy document identified but health listed as CNI sector on government website.	?l=1	me?l=1 http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=11808&l=1
20	Netherlands	Y Reference to CIP contained on government website.	Y Health listed as CNI sector on government website but no details of strategy.	http://www.government.nl/issues/crisis-national-security-and-terrorism/protecting-critical-infrastructure	http://www.alejandrobarros.com/media/users/1/50369/files/4363/2_NetherlandsCIdefpaper_2003.pdf http://www.nifv.nl/upload/91705_668_1223393504015-critical_infrastructure_protection_netherlands%5B1%5D.pdf
21	Poland	Y Reference to CIP and regulatory support to CIP contained on government website. Poland contributes to CIVPRO (see Finland)	Y Health listed as CNI sector on government website but no details of strategy.	http://rcb.gov.pl/eng/?page_id=210	
22	Portugal	N	N	www.**portugal**.gov.pt/en.asp	http://www.portugal.gov.pt/en/the-ministries/ministry-

		No reference to CIP identified on government main website nor Ministry for Home Affairs website.		x	of-home-affairs.aspx
23	Romania	Y Reference to CIP contained at Ministry of Internal Affairs website and sign posting to - Coordinating Centre for Critical Infrastructure Protection	Y? Researcher didn't identify specific strategy document that listed health as CNI sector.	http://www.mai.gov.ro/engleza/index07.htm?searWords=critical%20infrastructure%20protection	http://www.arpic.org/index.php/about-us http://www.sri.ro/upload/Brosura%20IC%20ENG.pdf http://www.aes.bioflux.com.ro/docs/2013.148-157.pdf
24	Slovakia	Y? Research couldn't identify a strategy document but did identify Ministry of Interior – Civil Protection and Crisis Management website	? Strategy not identified.	www.vlada.gov.sk/**government**-of-the-**slovak**-republic/	http://www.minv.sk/?ochrana-kritickej-infrastruktury http://www.tfzr.rs/jemc/files/Vol3No1/V3N12013-01.pdf

25	Slovenia	Y Reference to CIP contained on government website and listed in English but links to strategy documents in Slovenia language	Y? Researcher could not confirm due to language barrier.	http://www.mo.gov.si/en/areas_of_work/critical_infrastructure_protection/	http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/pdf/ministrstvo/RSNV2010_slo_en.pdf
26	Spain	Y Reference to CIP on the Ministry for Interior website but links to documents are in Spanish.	Y? No detailed health strategy identified due to language barrier.	http://www.cnpic-es.es/en/Legislacion_Aplicable/Generico/index.html	http://www.belt.es/legislacion/vigente/sp_pcivil/spublica/pdf/080311-Proyecto-Decreto-PIC.pdf https://www.jornadaspscic.isdefe.es/descarga/II%20Technical%20Conference%20Final%20Report.pdf
27	Sweden	Y Swedish Civil Contingencies Agency (MSB) commissioned by the government to manage CIP.	Y Listed as CNI in MSB strategy document.	https://www.msb.se/RibData/Filer/pdf/27412.pdf	https://www.msb.se/en/

		Sweden contributes to CIVPRO (see Finland)			
28	United Kingdom	Y Policy statement contained on government website.	Y No detailed strategy provided but health listed as CNI sector.	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf	http://www.cpni.gov.uk/about/cni/ https://www.gov.uk/government/publications/national-risk-register-for-civil-emergencies-2013-edition

The Organisation for Economic Co-operation and Development is an international economic organisation of 34 countries founded in 1961 to stimulate economic progress and world trade. It is a forum of countries committed to democracy and the market economy, providing a platform to compare policy experiences, seek answers to common problems, identify good practices and coordinate domestic and international policies of its members.

Austria – OIIP (Austrian Institute for International Affairs) is an independent, non-profit think tank that focuses on globalization, European integration, comprehensive security, and the comparative study of international affairs.

Belgium – CEPS (Centre for European Policy Studies) is a policy think tank in Brussels, providing research and activities on economic and international policy matters.

Cyprus – Cyprus Safety Platform is a consortium of government departments and private organisations that have come together to discuss, develop and manage various national concerns, including national infrastructure.

Denmark – DEMA (Danish Emergency Management Agency) is part of the Danish Ministry of Defence and is responsible for a multitude of tasks at national level, including CIP.

Estonia – Information System Authority responsible for coordinating the development and administration of the national information system, to help the state provide the best possible services to citizens. Estonia contributes to CIVPRO (see Finland).

Finland – The CIVPRO Civil Protection Network was established in 2006 by the EUROBALTIC II Project for Civil Protection, which is part of the EUROBALTIC Programme for Civil Protection initiated by the Council of the Baltic Sea States.

The CIVPRO Network aims to conduct studies addressing research questions in civil protection, risk management and emergency preparedness. CIVPRO consists of a variety of partners and its activities cover all of the Baltic Sea Region. It is coordinated by Aleksanteri Institute, Finnish Centre for Russian and Eastern European Studies, of the University of Helsinki.

The Organisation for Economic Co-operation and Development (OECD) is an international economic organisation of 34 countries founded in 1961 to stimulate economic progress and world trade. It is a forum of countries committed to democracy and the market economy, providing a platform to compare policy experiences, seek answers to common problems, identify good practices and coordinate domestic and international policies of its members.