CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Kadri Kaska and Lorena Trinberg

Regulating Cross-Border Dependencies of Critical Information Infrastructure

Tallinn 2015

www.ccdcoe.org
publications@ccdcoe.org

Table of Contents

Figures and Tables

Abbreviations

ACSS	Austrian Cyber Security Strategy
ANSSI	French Network and Information Security Agency
APCIP	Master Plan for the Protection of Critical Infrastructure (Austria)
ASS	Austrian Security Strategy
BMI	German Federal Ministry of the Interior
BSI	German Federal Office for Information Security
BVT	Federal Agency for State Protection and Counter Terrorism (Austria)
C(I)I	critical (information) infrastructure
C(I)IP	critical (information) infrastructure protection
C.N.A.I.P.I.C.	Italian National Anti-Crime Computer Centre for Critical Infrastructure Protection
CERT	Computer Emergency Response Team
CERT-SI	Security and Industry CERT (Spain)
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CNPIC	National Centre for the Protection of Critical Infrastructures (Spain)
DoS	Denial of Service
ECI	European Critical Infrastructure
EPCIP	European Program for Critical Infrastructure Protection
EU	European Union
ICT	information and communication technology
INCIBE	National Institute of Cyber Security (Spain)
MOD	Ministry of Defence
MOFA	Ministry of Foreign Affairs
MOI	Ministry of Interior
NCSS	National Cyber Security Strategy
NCTV	National Coordinator for Counterterrorism and Security (the Netherlands)
NISP	Italian Nucleus Inter-Ministerial Unit for Situation and Planning
NSA	National Security Authority
RIA	Estonian Information System Authority
SOVI	Critical Infrastructure Strategic Consultative Body (the Netherlands)
US/U.S.	United States

Introduction

One of the least explored areas of cyber vulnerabilities concerns cross-border dependencies of critical information infrastructure (CII).[1] The provision of vital services such as banking or telecommunications is increasingly reliant on CII which may be located in another country or have a critical dependency on information systems outside of a country's jurisdiction. This trend is expected to continue alongside globalisation and technologically-driven business practices such as the adoption of cloud computing services.

Cross-border dependencies create additional vulnerabilities and a potential source of instability even for countries that have addressed these issues domestically. Risks include cascade effects that can arise from the dependencies as well as choices that might be made by a sovereign actor not taking into account dependencies in other countries.

Discernible examples of legal and regulatory remedies to mitigate the risks arising from CII located outside national territory are virtually non-existent; the same applies to the results of a national survey conducted as a part of this research, as well as to observations from its literature review. There are rare national strategy documents that emphasise the importance of the topic, and a few academic texts to the same effect, but an established, commonly accepted, discernible approach to cross-border CII dependencies is currently lacking.

Against the prevailing lack of research and measures directly addressing the topic of cross-border CII dependencies, this study has two main objectives:

a) Identify the existing state of knowledge about critical infrastructure dependencies on information infrastructure beyond national territory as reflected in academic and security research; and
b) Identify the state of awareness about the issue in a selection of NATO nations and determine any existing nationally employed strategic, legal and regulatory tools to remedy risks that arise from vulnerabilities due to cross-border dependencies of CII.

We approached these objectives in four stages: first, we conducted an open source review of existing research dealing with cross-border aspects of critical information infrastructure, critical infrastructure (inter)dependencies upon information infrastructure, and the various combinations thereof. In parallel, we studied national legal instruments, national cyber security strategies, and national policy documents which have regard to critical infrastructure protection and cyber security, as well as soft law instruments by international organisations.[2] The nations included in the study were selected on the criteria of advanced or long-time experience with critical information infrastructure protection (CIIP), recent legislative attention to the issue, or particular geographic setting presuming the necessity of attention to cross-border dependencies.

Building on the initial literature review, we developed a survey for distribution among national CII experts and authorities responsible for the coordination of critical (information) infrastructure protection among NATO Allies and partner nations[3], with whom we established contact prior to circulating the survey. The survey

[1] Where beneficial for clarity, the full phrases of 'critical information infrastructure' and 'critical infrastructure' are used throughout the document in parallel with their corresponding abbreviations, 'CII' and 'CI'.
[2] This being an introductory and conceptual study, we did not analyse individual national risk assessments which may include cross-border elements in some of the threat scenarios. It may well be that a particular remedy has been introduced upon individual or sectoral CII operators that the research did not reveal and that the national experts contributing to the study either were not aware of or refrained from pointing out.
[3] With a particular focus on the NATO CCD COE sponsoring nations, but not limited to them. The NATO CCD COE Sponsoring Nations, at the time of conducting the survey, were Estonia, Czech Republic, France, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, and the United States. Turkey as a nation in the officially process of joining the Centre was included in the survey.

enquired about three aspects: critical (information) infrastructure and CI concept and designation; responsibilities of infrastructure operators and coordinating bodies; and specific cross-border aspects, including national cross-border dependency risk perception and existing national remedies to mitigate these risks. The survey was carried out during October 2014. Experts from twelve nations participated in the survey.[4]

The responses of the participating experts were combined with open source information obtained from the literature review and compiled into country overviews, covering CII approaches and cross-border aspects of each respondent country. Finally, each draft country overview was verified with the relevant national expert, whose comments were integrated into the final version of the overview. However, it should be noted that while the authors gratefully acknowledge the support of the experts, the overviews were prepared by the authors of this study and should not be considered as representing the official opinions of the corresponding countries.

The study is structured as follows. We first offer a summary of the survey responses together with the main findings of the research, covering both findings from the survey as well as those from the literature review.

The bulk of the study, Part I, offers a country-by-country delineation of national legal and strategy approaches to cross-border dependencies on CII. In each country overview, we first describe the national concept of critical infrastructure and critical information infrastructure, including the basis of CII designation and nationally recognised critical sectors. Secondly, we outline the responsibilities of actors involved, both those of the national coordinating bodies and of CI operators. The cross-border aspects are then pointed out, describing in particular the remedies which address cross-border dependencies. As noted above, Part I relies on input received from national experts in the course of the survey as well as on independent research carried out in the course of the initial literature review.

Part II of the study offers an annotated bibliography of existing research related to critical infrastructure dependencies on information infrastructure beyond the borders of the national territory. The two primary themes that the literature review looks at are cross-border dependency risk perception and existing measures (including legal, regulatory and policy) for addressing cross-border dependencies.

The bibliography includes academic research and publications by security research institutions, but also research invited by regional organisations such as the EU, or by national authorities. For this task, we reviewed selected academic journals from academic publishers[5], along with online academic legal research services,[6] and internet search engines.[7] In the results, we omitted most general articles which addressed only sectoral (inter)dependencies but not cross-border or cross-jurisdictional aspects in particular. While the main focus of the research was on work published in 2010 or later, a number of substantial resources were published before that date and fairly little ground-breaking work seems to have been published since then.

Each entry includes a full reference to the publication followed by a list of keywords and a synopsis of the publication; cross-border aspects are specifically highlighted in the synopsis where this seemed useful to understanding the relevance of the publication to cross-border dependencies. Where relevant, recommendations offered in the publications are included. The results are presented by type in chronological order. The literature review is followed by a thematic keyword index.

[4] Namely, Austria, Belgium, Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, the Netherlands, Spain, and Turkey.
[5] Including Elsevier, Springer, Inderscience; including academic journals such as International Journal of Critical Infrastructures; International Journal of Critical Infrastructure Protection; International Journal of Emergency Management.
[6] HeinOnline.
[7] scholar.google.com, books.google.com, www.google.com.

We do not claim that the list is a complete collection of all writings relevant to the topic. As will be demonstrated throughout the following sections, the amount of existing research, as well as legal and policy instruments targeting the cross-border CII dependencies issue directly is marginal, and therefore, we needed to expand the scope of the research to identify information that might be relevant or helpful to the target audience in tackling the issue.

The study concludes with an annex offering contact information for the national bodies responsible for CI and CII coordination in the nations covered in the study.

The study is primarily intended to assist national policy developers and regulatory bodies dealing with critical information infrastructure coordination. Both the survey and the literature review primarily looked into legal, policy and strategic issues of cross-border CII dependency, and did not consider research which discussed purely technical and operational-level solutions. This being an introductory and conceptual study, individual national risk assessments which may include cross-border elements in some of the threat scenarios were not analysed. It may well be that a particular remedy has been introduced by individual or sectoral CII operators that the research did not reveal and that the national experts contributing to the study either were not aware of or refrained from pointing out.

The authors would like to express their gratitude to Lea Hriciková and Colin Ian Sweet for their valuable support and contribution to this study.

Findings of the study

National approaches to critical (information) infrastructure

Terms and definitions

National remedies to address vulnerabilities in critical infrastructure are affected by and often dependent on the national setting, including the country-specific threat picture, market and infrastructure characteristics, organisational tradition and culture, and language. Even though this study is mainly Europe-focused due to the range of nations included in the study, and the approach to critical infrastructure protection (CIP) is to some extent harmonised throughout Europe on the basis of the European Critical Infrastructure directive,[8] it is useful to have basic appreciation for the national variation of key concepts. Hence, the following subsection will briefly summarise the variations in terminology and definitions used nationally. Individual national definitions are reflected in Part I.

Of the twelve nations involved in this study, the majority of the national cyber security strategies as well as legal and policy documents operate with the terms 'critical infrastructure' and 'critical information infrastructure'. A few peculiarities exist – e.g. rather than 'critical infrastructure', France prefers the notion 'operators of critical importance' (*Opérateur d'importance vitale*), and in Estonia, the central notion is 'vital services', but on comparison of national definitions, it can largely be gathered that all nations included in the study understand 'critical infrastructure' (regardless of the particular terminology used) as 'an asset, system or part thereof […] which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact […] as a result of the failure to maintain those functions'.[9]

While critical infrastructure is largely uniformly defined across all nations participating in the survey, definitions for 'critical information infrastructure' are less common. Six nations in the survey define critical information infrastructure in national law. In three cases, the term coincides with critical infrastructure; three countries provide a specific legal definition stipulated by means of a specific legal act on cyber security (Czech Republic and Latvia) or by ministerial decree (Italy). The remainder provide no definitions, although they might use the term itself. It is not uncommon to address critical (information) infrastructure protection by means other than legislation, either binding or non-binding (e.g. Austria, the Netherlands).

Critical information infrastructure is typically addressed either as part of a critical sector or service, or as a distinct critical sector or service itself. However, the two options are not necessarily considered mutually exclusive; a few respondents noted that CII can both constitute a distinct critical sector and be a part of or support another sector in parallel, and the national approaches detailed in Part I of the study indicate the same.

[8] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L [2008] 345/75). The majority of the nations covered in the study are Member States of the European Union.

[9] ibid, Article 2(a). Again, note that eleven of the twelve survey respondents are EU Member States, so the high degree of similarity of national definitions for CI can be explained by the inclusion of the definition in the Directive.

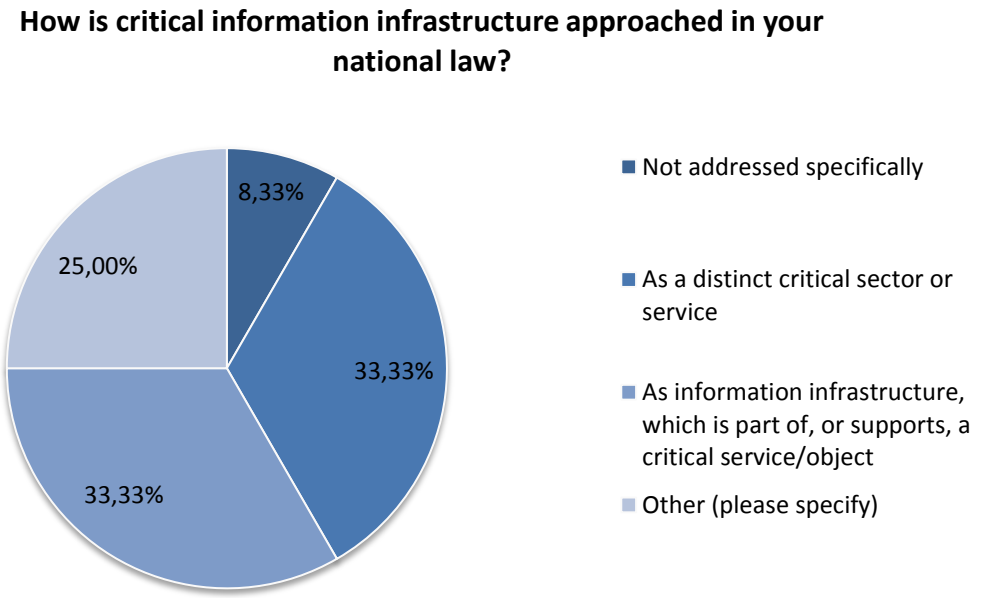

Figure 1. National law approach to critical information infrastructure

The number of sectors recognised as critical differs by nation, ranging from five (Turkey) to thirteen (Austria). Not all nations go by a sectoral approach (e.g. Latvia and Estonia) and intersectoral boundaries also differ from nation to nation. However, with regard to national consideration of sectors as critical, those commonly mentioned (by more than a half of the respondents) include IT and communications; transport; energy; finance; food; water management; health and medical services; and public security and public order.

National coordinating bodies for critical information infrastructure

The national coordination and supervisory tasks with regard to CIIP are commonly held by a national cyber security centre (or equivalent)[10] or the national or government CERT.[11] Other options include the national security authority (NSA), national telecommunications regulatory authority, and an inter-ministerial unit subordinated to the President of the Council of Ministers (Czech Republic, Turkey, and Italy, respectively).

With regard to the relationship of these national CIIP bodies to the overall national coordinator for the protection of critical infrastructure, approaches again vary by nation. In seven of the nations surveyed, CIP coordinating function is contained within a different body (Austria, Czech Republic, Germany, Estonia, Hungary, Latvia, and Turkey). In a further three nations, the coordinating and supervisory entity for CIIP is linked or subordinated to the CIP coordinator (Spain, France, and the Netherlands), and in Belgium and Italy, both functions are held by the same entity.

In roughly half of the nations surveyed, the coordinating body for the protection of CII during routine everyday operation is also the coordinator for crisis situations.

[10] Estonia, Belgium (for the National Cyber Security Centre, who further coordinates with the National Crisis Centre), France, Germany, the Netherlands, and Spain.
[11] Austria, Hungary, and Latvia.

Further details can be found in Table 1 below.[12]

COUNTRY	National coordinating body for CIP	Coordinating body for CIIP	
		During routine everyday operation	During crisis situations
Austria	**Federal Chancellery Ministry of the Interior**	**Austrian Government Computer Emergency Response Team (GovCERT)**[13]	Under development[14]
Belgium	**National Crisis Centre**		**National Cyber Security Centre** (under development) in cooperation with the **National Crisis Centre**
Czech Republic	**Ministry of the Interior** (General Directorate of Fire Rescue Service of the Czech Republic)	**National Security Authority (NSA)**	
Estonia	**Ministry of the Interior** (Rescue and Crisis Management Policy Department)	**Estonian Information System Authority (RIA)** (Risk Control and Advisory Department, CIIP Unit)	
France	**General Secretariat for Defence and National Security** (under the authority of Prime Minister)	**French Network and Information Security Agency (ANSSI)**	
Germany	**German Federal Ministry of the Interior (BMI)**	**German Federal Office for Information Security (BSI)**	**German Federal Ministry of the Interior (BMI)**
Hungary	**Ministry of Interior** National Directorate General for Disaster Management	**Government CERT**; **CIP CERT** (for the designated CIs); other sectoral CERTs	**Ministry of Interior** National Directorate General for Disaster Management
Italy	**Nucleus Inter-Ministerial Unit for Situation and Planning (NISP)**		Governance: **Nucleus Inter-Ministerial Unit for Situation and Planning (NISP)/ Nucleus Unit for Cybersecurity (NSC)** Police: **National Anti-Crime Computer Centre for Critical Infrastructure Protection (C.N.A.I.P.I.C.)**[15] of the Ministry of Interior Police (Police Service, Post and Communications)

[12] Contact information for CIIP coordinators is available in the Annex.
[13] According to the ACSS, an operational structure of Federal Chancellery, MOD, MOI and MOFA is under development and will be the responsible body.
[14] The Austrian Cyber Security Strategy is implemented with the main focus on national operational structures. The Cyber Security Steering Group on Government-level has been established and coordinates the implementation.
[15] The C.N.A.I.P.I.C. is committed exclusively to the prevention and suppression of cybercrimes, of common matrix, organised or terrorist, who would target the critical nature of information infrastructures and of national importance.

COUNTRY	National coordinating body for CIP	Coordinating body for CIIP	
		During routine everyday operation	During crisis situations
Latvia	**Commission of Intermediary Institutions for State Security**	**Information Technology Security Incident Response Institution** (national CERT): incident support prevention **Constitution Protection Bureau**: recommendations for eliminating deficiencies	
The Netherlands	**Minister of Security and Justice** (delegated to **National Coordinator for Security and Counterterrorism**)	**National Coordinator for Security and Counterterrorism (NCTV)**; direct activities delegated to **Department for Cyber Security, National Cyber Security Centre**	
Spain	**National Centre for the Protection of Critical Infrastructures (CNPIC)**	**National Centre for the Protection of Critical Infrastructures (CNPIC)** through **CERT-SI** (an organ of **National Institute of Cyber Security (INCIBE)**)	
Turkey	**Ministry of Transportation, Maritime and Telecommunications**	**Information and Communication Technologies Authority**	

Table 1. National coordinating bodies for CIP and CIIP

Legal responsibilities for critical information infrastructure

The direct legal responsibility for the security and functioning of CII is held by the critical infrastructure operators, who have to plan and apply security measures, manage risks in the critical infrastructure in their operation, and ensure the functioning of installations, networks, systems, and physical or ICT assets. Whether these obligations apply to operators automatically or require their nomination as a designated CI operator (e.g. Turkey) depends on the national approach and is further specified in Part I.

Some nations, such as Latvia, attach obligations to the infrastructure owner or legal possessor (although the latter will typically coincide with the operator); the Czech Republic has a fairly detailed outline of obligations for the administrators of CI information and communication systems. Latvia requires the owner or legal possessor of CII to appoint a person responsible for security of the particular critical infrastructure, who then ensures, in cooperation with the national CERT, risk assessment and CI management for the information systems. Likewise, in Austria, the responsibilities are formally held by a nominated Chief Information Officer.

However, national C(I)IP bodies may have corresponding obligations to assist the CI operators, provide guidelines, etc. As an example, in Latvia, the Constitution Protection Bureau and the national CERT cooperate with the person responsible for the security of the critical infrastructure to ensure both the assessment and management of its current risks. In some nations, such as Germany and Italy, certain critical sectors further have sectoral regulators with certain tasks and responsibilities defined by legal acts.

The responsibilities of the operator and other relevant players are specified in various legal acts. Some countries have a longer list of legal acts which resemble a widespread carpet of obligations (e.g. Germany), other countries have a very condensed list of legal acts (e.g. Turkey, Spain, Estonia). Notably, Austria has not adopted any legal acts to this point and operates according to its Cyber Security Strategy (ACSS) and the Governmental Report on the Austrian Security Strategy (ASS).

The four main legal obligations of the infrastructure owners are notifying and reporting, monitoring, implementing security measures, and maintaining security documentation. These apply in the majority of the countries surveyed. Almost as common is the obligation to submit to specific security measures or government

guidelines in the case of incidents. Other examples given referred to the obligation to implement specific measures set out by the NSA (Czech Republic); Italy noted that basically all actions and measures necessary to ensure the protection of CI are included in the relevant legal acts as legal obligations. Estonia has defined a full list of obligations in secondary legislation.[16]

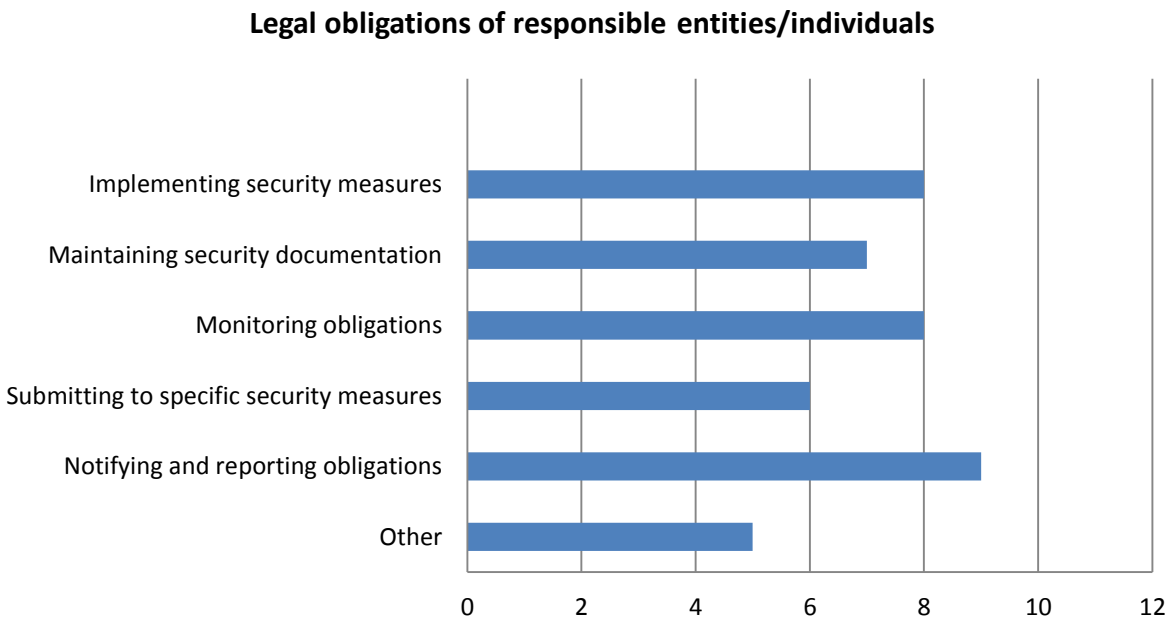

Figure 2. Legal obligations of entities/individuals responsible for the security and functioning of CII.

Cross-border dependencies

Identifying cross-border dependency

Service suppliers, especially transnational ones, are often unaware of the fact that they spatially define the external limits of a country's national security. An organisation operating data communications networks or fixed or mobile telephone networks across several countries, or a commercial bank operating payment and cash services in multiple national markets are driven by business continuity and efficiency considerations, but may accept the risk of a service failure caused by *force majeure* or may not consider the impact of a particular business choice to service provision in another country. Traditional remedies relied upon by the national authority to ensure the functioning of information infrastructure which conditions the operation of a critical service are less useful for infrastructure which is located beyond national boundaries due to the national regulator's authority being territorially limited. Mitigating distinctive risks related to such transnational service models firstly requires awareness, by both the relevant national regulators and the service operator, of the existence of cross-border dependencies, as well as their nature and extent.

[16] Vabariigi Valitsuse 14.03.2013 määrus nr 43 "Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmed" (RT I, 20.03.2013, 7) (Security Measures for Vital Service Information Systems and Related Information Assets; English translation available at <https://www.ria.ee/public/KIIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf >, accessed 03 December 2014).

The word *dependency* is defined as '[t]he condition of being dependent; the relation of a thing to that by which it is conditioned; contingent logical or causal connection';[17] *dependent* in turn means '[c]ontingent on or determined by, requiring someone or something for […] support, unable to do without.'[18] In the context of critical infrastructure, dependency is consequently understood as the 'one-directional reliance of an asset, system, network, or collection thereof – within or across sectors – on an input, interaction, or other requirement from other sources in order to function properly.'[19] The addition of a cross-border dimension to this paradigm by means of an extraterritorially located essential 'asset, system, or part thereof' not merely adds a further element of complexity to the system, but also increases the diversity of actors required to manage it.

Dependency can be manifest in various forms. From the existing concepts of infrastructure interdependencies (see, for example, items 1 and 14 in Part II of this study), various types of infrastructure dependency can be constructed. These include, among other, physical dependency (which is defined as a requirement, often engineering reliance between components), informational dependency (an informational or control requirement between components), and policy/procedural dependency, which exists due to policy or procedure that relates a state or event change in one infrastructure sector component to a subsequent effect on the other component.[20] While this study did not inquire about the particular type of dependency between the critical infrastructure and information infrastructure supporting it (partly due to the apparent lack of a common approach and methodology to distinguish between them and partly due to the perceived lack of practical output for the purposes of this study), the individual characteristics of a dependency of a critical infrastructure would have to be sought in each case and it would have to be borne in mind that a solution developed for addressing a certain type of dependency may not be universally adoptable for other dependencies merely because both share a cross-border element.

To understand the current views about cross-border CII dependencies, the survey inquired about the respondents' perception of sectors or services that show a particularly relevant dependence on cross-border information infrastructure. The responses highlight certain sectors where the perception of dependency on cross-border information infrastructure appears particularly high. On a scale of 'none' to 'critical', ICT and telecommunications, finance, and energy were perceived as showing a dependence on cross-border information infrastructure to a degree that was considered between substantial and critical.[21] With the exception of the healthcare sector, all of the remaining critical sectors were considered at least somewhat dependent of cross-border CII, with transportation and media nearing substantial dependency on average.

Figure 3 presents the weighted average perception of sectoral dependency.[22]

[17] Oxford English Dictionary, 'dependency', <http://www.oed.com/view/Entry/50244?redirectedFrom=dependency#eid>, accessed 2 December 2014.
[18] Oxford Dictionaries, 'dependent, <http://www.oxforddictionaries.com/definition/english/dependent> accessed 2 December 2014.
[19] U.S. Department of Homeland Security, 'National Infrastructure Protection Plan' (2009). <http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf> accessed 02 December 2014, 109.
[20] ibid.
[21] 0 (none), 1 (minimal), 2 (substantial), and 3 (critical).
[22] Responses marked N/A (not applicable) as well as those abstaining from responding to the question were excluded from the calculation of the weighted average.

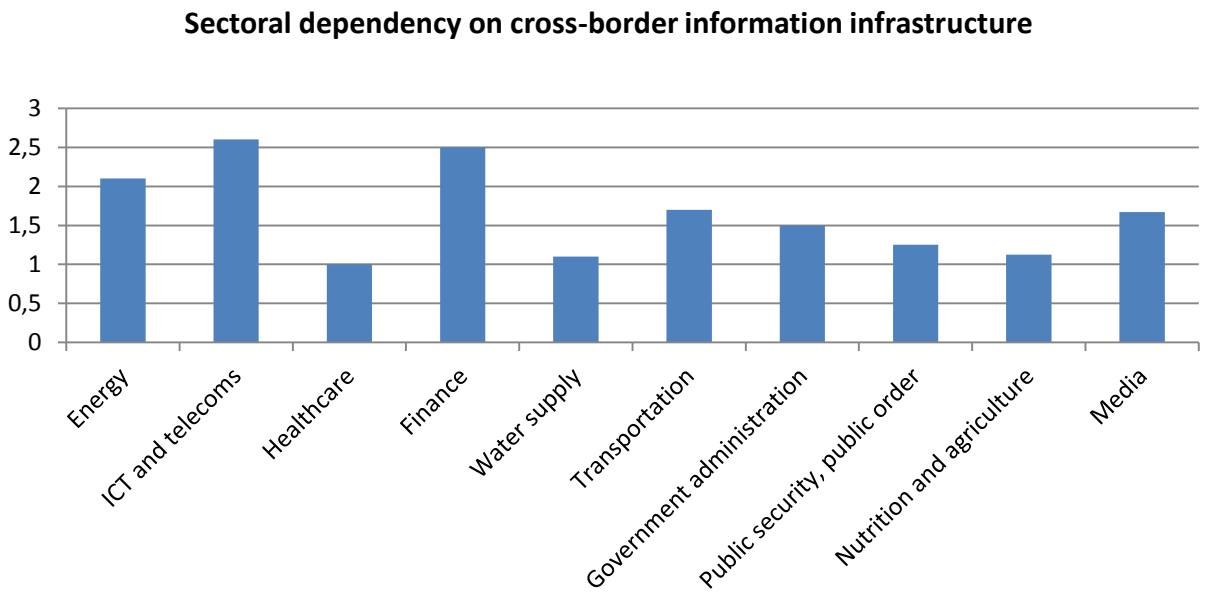

Figure 3. Overall perception of sectoral dependency on cross-border information infrastructure.

Across some of the sectors, there are rather significant differences in dependency perception by different respondents. For example, in the healthcare sector, two respondents viewed the sector as not dependent on cross-border CII to any extent while a further two considered it to be substantially dependent, and responses regarding the water supply and media sector ranged from none to critical.

Those considered critically dependent by most respondents were information systems and telecommunications, and the financial sector; for the energy sector, opinions were almost equally divided between 'critical' and 'substantial'. Traffic and transportation as well as the media sector were also most frequently considered as substantially reliant on cross-border CII; the remainder of the sectors were mainly considered as demonstrating only a minimal dependency on cross-border CII.

In none of the sectors did the dominant opinion point to no cross-border dependency. Four sectors were considered by all respondents without exception to demonstrate at least some level of dependency: information systems and telecommunications, finances, energy supply, and government and administration. For the first of those two, none considered the dependency to be less than substantial.

Two further critical sectors were pointed out as dependent on cross-border information infrastructure: domestic and international trade (one respondent considered it to be critically dependent), and manufacturing/industrial production (two respondents considered it to be minimally to substantially dependent).

Table 2 presents individual national assessments with regard to sectoral dependency on cross-border CII.

	None	Minimal	Substantial	Critical	N/A	Responses	Weighted Average
	0	1	2	3			
Energy supply	0 (0.00%)	1 (9.09%)	**5 (45.45%)**	4 (36.36%)	1 (9.09%)	11	2,1
Information systems and telecommunications	0 (0.00%)	0 (0.00%)	4 (36.36%)	**6 (54.55%)**	1 (9.09%)	11	2,6
Healthcare	2 (18.18%)	**5 (45.45%)**	2 (18.18%)	0 (0.00%)	2 (18.18%)	11	1
Finances	0 (0.00%)	0 (0.00%)	4 (36.36%)	**5 (45.45%)**	2 (18.18%)	11	2,5
Water supply	2 (18.18%)	**6 (54.55%)**	1 (9.09%)	1 (9.09%)	1 (9.09%)	11	1,1
Traffic and transportation	1 (9.09%)	2 (18.18%)	**6 (54.55%)**	1 (9.09%)	1 (9.09%)	11	1,7
Government and administration	0 (0.00%)	**5 (45.45%)**	2 (18.18%)	1 (9.09%)	3 (27.27%)	11	1,5
Public security and public order	1 (9.09%)	**4 (36.36%)**	3 (27.27%)	0 (0.00%)	3 (27.27%)	11	1,25
Nutrition/agriculture	1 (9.09%)	**6 (54.55%)**	0 (0.00%)	1 (9.09%)	3 (27.27%)	11	1,125
Media	1 (9.09%)	**3 (27.27%)**	**3 (27.27%)**	2 (18.18%)	2 (18.18%)	11	1,67
							1.65 / 3

Table 2. Individual perception of sectoral dependency on cross-border information infrastructure.

Risks of cross-border critical information infrastructure dependency

With regard to noteworthy risks related to cross-border critical information infrastructure dependency, the responses highlighted the following:

- **Technological risks**, including natural and man-made hazards – operating errors, failure of communication systems (undersea cables, satellites); non-updated systems and the use of outdated technology, but also the lack of technical expertise and know-how in case of an incident. Some respondents pointed to specific threats and risks, such as availability risks in case of a denial of service attack (DoS) or the risk of disruption of regional network exchange nodes and the electrical grid. In the energy supply context in particular, geographic risk factors were highlighted.
- **Legal and procedural risks**. This includes differences in legislation and policy, which complicate dealing with the matter on an international level, but also the lack of equivalent security standards, including on the EU level. One respondent pointed out, as a potential concern, the availability of the so-called 'bulletproof hosting'[23] services that are not prosecuted. Risks of not using an all-hazards approach to critical infrastructure protection were seen as a broad problem.

[23] '"Bulletproof hosting" refers to hosting services that give their customers great freedom as to the type of content they may upload. Some of these services are not in compliance with national laws and have been used by spammers. Many but not all of the bullet-proof hosting services are outside of the country of the content provider.' Johannes M. Bauer, Michel J. G. van Eeten, Tithi Chattopadhyay, Yuehua Wu, 'ITU Study on the Financial Aspects of Network Security: Malware and

- **Financial** aspects were noted, in particular inadequate funding of security systems.
- Surprisingly often, **social or cultural problems** were identified – such as differences in threat perception, the lack of trust, lack of information sharing in the context of both preventive and reactive activities. Different security cultures across borders are a further factor that complicates cross-border CII activities.
- Eventually, the rising complexity of society was seen as an **inherent factor** impacting the choice of measures to address cross-border CII dependency. One respondent called attention to the activities of state and non-state actors, including potential military operations – while a generic CI risk in itself, it may entail specific significance for cross-border CII due to creating a linkage between the potential security threat scenarios of several nations.

One respondent pointed to the risks being dependent on specific circumstances, which renders generalisation difficult and impractical; Austria referred to the risk matrix contained in the national cyber security strategy.[24] A further national expert refrained from responding, referring to information security restrictions.

Overall, the responses indicated a difficulty of meaningfully generalising risks that are specifically determined by the cross-border factor. Risks relevant to CI which is dependent on information systems outside of the country's territory are in character largely comparable to the risks faced by nationally contained CI; on the other hand, any specifics are more typically sectoral or conditioned by the setup of certain infrastructure (e.g. electric supply networks). In this case, risks that occur due to cross-border dependency can be determined in the course of an all-hazards risk assessment against a particular critical infrastructure, but such assessment does not necessarily yield usefully adoptable solutions for another infrastructure or sector.

Mitigating cross-border risks

In general, there are very few distinguishable measures in national law that directly deal with cross-border dependencies: only three respondents (Spain, Estonia and Hungary) noted specific legal obligations to assess and mitigate cross-border dependencies on critical information infrastructure. In Spain, CI operators must detect and assess cross-border dependencies in the main security plans they have to develop, while CII administrators are required to identify the relationship between ICT and the essential service provided by the CI operator, which must then be represented also in the operator and facilities security plans. In Estonia, the providers of the vital services are required by law to ensure the continuous operation of the vital service also in a manner and by means not dependent on information systems located in foreign countries; vital service providers are obliged to perform risk analysis of continuous operations that also consider IT risks. National-level risk analyses mandated by the national cyber crisis coordination body (Estonian Information System Authority) include cross-border dependency aspects. In Hungary, there are obligations specified by legal regulation for the state and local government levels, including restrictions regarding data storage and management on territories outside of the European Union Member States or, in certain cases, outside of Hungary.

However, in addition to the clear-cut legal requirements for cross-border dependencies, the significance of other measures for CIIP should not be overlooked. Germany has specified legal obligations related to the national implementation of the EU Council Directive 2008/114/EC (European Critical Infrastructures

Spam' (ITU 2008), <www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf> accessed 12 Dec 2014.

[24] Annex I of the Austrian Cyber Security Strategy. Austrian Federal Chancellery, 'Austrian Cyber Security Strategy' (2013). <https://www.bka.gv.at/DocView.axd?CobId=50999> accessed 06 November 2011.

directive),[25] and the Netherlands includes an incident reporting obligation for CII in a draft act (Security Breach Notification) currently in the parliamentary process. Both have relevance for cross-border risk mitigation.

The remaining national experts indicated no specific legal obligations related to CI cross-border dependency on information infrastructure, while some did point to the existence of general obligations for CI operators or CII administrations that also apply to cross-border aspects.

Nearly all respondents found the CIP objectives and measures laid out in their national cyber security strategies to be relevant and applicable to cross-border dependencies, highlighting in particular the following:

- international collaboration and cooperation;
- engaging in bi- and multilateral dialogue and cooperation;
- enforcing international rules of conduct, standards and norms; and
- promoting information sharing.

Estonia was the only nation which directly addressed cross-border dependencies in the national cyber security strategy, requiring that interdependencies between vital services, including cross-border dependencies, be constantly mapped and managed. Detailed measures are not publicly available.[26]

In short, all examined countries have introduced some sort of remedies in order to address CI dependencies; there is little specifically on the dependencies of CII and the depth of the remedies taken varies significantly. However, a common consensus regarding the necessity for international cooperation in the context of CIIP should support further development in this area.

Literature review

The same overall observation made about the survey also holds for the review of the existing academic and semi-academic research relating to cross-border dependencies of critical information infrastructure: the topic has not been directly and systematically addressed in the literature, and beyond recognising overall vulnerability caused by sectoral dependencies, little has been written about cross-border mitigation of such vulnerabilities in particular.

Considering the objective of this study, the research question posed for the literature review sought four essential, cumulative elements: critical infrastructure, information systems ensuring the functioning of critical infrastructure, dependencies, and a cross-border component. The main challenge for mapping out the existing state of knowledge was that seldom are all these elements addressed in the aggregate. While publications discussing, for example, sectoral (inter)dependencies of critical infrastructure, potential cross-border impact of threats to information infrastructure, or critical infrastructure dependency on information systems, are plentiful, there is little among them that add substantive value to the discussion of cross-border dependencies of critical infrastructure on information infrastructure. Furthermore, not only is specific attention rare, it also tends to be occasional and random rather than systematic and methodical.

Cross-sector (inter)dependency itself is widely acknowledged as a source of vulnerability, although the claims of 'mutual functional linkage of almost all critical infrastructure sectors'[27] are not always substantiated – as

[25] Directive 2008/114/EC (n 8).
[26] Estonian Ministry of Economic Affairs and Communications, *Cyber Security Strategy 2014-2017* (2014) s 1.3 <https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf>, accessed 04 December 2014.

observed by Luiijf, Nieuwenhuijs, and Klaver in a study modelling real-life incident data, it is mainly the energy and telecommunication sectors that 'drive' cascade effects of critical infrastructure failure, while other sectors rather tend to be the 'victim' of dependencies which hardly cause a spill over of failure to any other sector.[28]

The scope and amount of existing research useful for the research task at hand is further limited by the fact that existing research on cross-border CII dependencies often looks at cross-border information infrastructure in a loose and abstract manner, speaking about internet infrastructure or interconnected telecommunications networks in general, without specifying the role that the specific information infrastructure has for supplying a particular critical service. Consequently, solutions offered tend to remain limited to two highly abstract types of recommendations: 'enhancing awareness' and 'furthering international cooperation'.

Likewise, most of the current discussions about cross-border critical (information) infrastructure protection appears limited to potential spill over of effects of a critical infrastructure incident beyond the originating country's national borders, revolving around notions such as cross-border incident, cross-border impact, or cross-border damage.

The research activities performed in the course of this study indicate two central conceptual issues which need to be considered for future research about practices regarding cross-border dependencies. First, in many cases, cross-border dependencies are not dealt with in isolation from the overall CI risk picture, but rather contained within 'all-hazards' risk assessment and management. Similar observations were also made from the survey (see Part I of the study); and many sources, including the OECD recommendations (items 17 and 19 in Part II), advise an 'all-hazards' approach to CI risks.

Therefore, the lack of overall mitigation measures or legal obligations with regard to cross-border CII dependencies in national legal and policy frameworks does not necessarily imply a lack of attention to the topic, it merely implies that an all-hazards risk assessment is better suited for tailored measures to address specific identified risks in complex or in connection to other identified risks and threats, being aware of interdependencies as well as the cumulative and mutual impact of measures. The fact that studies and activities regarding cross-border CII dependencies appear more frequently on a sector-specific or service-specific basis such as telecommunications or energy seems to support this understanding.

Moreover, many nations do not address critical *information* infrastructure distinctly from critical infrastructure but rather as a part of thereof, under a single conceptual framework (see Figure 1). Such a line is also followed in policy recommendations (see, for example, item 14 of Part II); however, for that reason it is also difficult to determine whether a nation does not have a CII approach at all, or whether it includes CII in its overall CIP approach.

Finally, the national perception of threats as critical certainly plays a role in determining both the policy and research attention given to a particular aspect of national critical infrastructure protection. As national concerns differ, some countries such as the US or Spain, are more concerned about terrorist attacks against critical infrastructure, whereas small, highly interconnected countries like Estonia or the Netherlands place more importance on their reliance on extraterritorial information systems. National analysis is therefore not unreasonably based on presumed threat patterns, and measures are consequently defined in order to address the particular type of threat. It cannot therefore be excluded that some countries do not currently consider cross-border CII dependency as a problem deserving separate and focused measures.

---

[27] M Seidl, L Šimák, 'Protection of Critical Infrastructure' (2012) 1(14) Logistics and Transport <http://www.logistics-and-transport.eu/index.php/main/article/viewFile/204/197> accessed 10 December 2014.

[28] H.A.M. Luiijf, A.H. Nieuwenhuijs, and M.H.A. Klaver, *Critical Infrastructure Dependencies 1-0-1* (2008), <http://publications.tno.nl/publication/102547/FOpThI/luiijf-2008-critical.pdf>, accessed 8 September 2014.

Consequently, with regard to suggestions for further study in this topic, the relevance of existing national all-hazards risk assessments to the problem of cross-border CII dependencies should be reviewed. Since this will likely be a painstaking technical task which may not yield much useful output across sectors or services, rather than a systematic overall study, such research may be more reasonably be carried out by nation or by sector, service or system, with the objective of seeking best practices, both for the national risk assessment process and for particular remedies introduced. For improving overall awareness about the current state of knowledge and activity about cross-border dependencies, and for stimulating internal national assessment on cross-border dependencies, the study at hand should nonetheless be useful.

PART I:
National approaches and existing remedies

AUSTRIA

1.1. Concept and designation

The Austrian conception of CI is closely related to Directive 2008/114/EC. The legal definition can be found in the Master Plan for the Protection of Critical Infrastructure (APCIP)[29] of 2008:

> 'Critical infrastructures are those infrastructures or parts thereof which are essential for the maintenance of vital societal functions. Their disruption or destruction has a significant impact on health, safety and security or the economic and social well-being of the Austrian people or the effective functioning of the state.'

According to the APCIP, the vital sectors are maintained under the guidance of Directive 2008/114/EC and cover 13 sectors: energy; ICT; water; food; health; finance; transport; chemical Industry; research; constitutional Institutions; social system; distribution system; search and rescue.

There is no legal definition for the term CII, nor does the Austrian Cyber Security Strategy, which was adopted by the Council of Ministers in March 2013, attempt to define it. However, CII is considered a distinct critical sector or service, which adheres to an operator-based approach. Some 26 companies of strategic importance were identified within the statistical section 'Information and Communication'.[30] The operator-based approach avoids setting specific criteria for the identification of critical infrastructure assets, instead opting to rely on the companies themselves to report on the CII that they control.

1.2. Responsibilities

The implementation of the European as well as the APCIP is overseen by two entities: the Federal Chancellery and the Ministry of Interior. The latter, particularly through the subordinate Federal Agency for State Protection and Counter Terrorism (BVT),[31] is responsible for security matters. The nominated Chief Information Officers (CIOs) and sometimes CERTs are the corresponding individuals and entities which have direct responsibilities, but there is a notable absence of legally enacted responsibilities in the area of CII. Similarly, no legal obligations have been set out yet.

The Austrian Government Computer Emergency Response Team (GovCERT Austria)[32] is currently responsible for ensuring the uninterrupted and secure performance of day-to-day IT systems and networks, servicing Austria's public administration and critical information infrastructure. Founded in 2008, GovCERT Austria is run by the Federal Chancellery in cooperation with CERT.at to prevent and handle security-relevant incidents relating to Austria's use of information and communication technologies. According to the Austrian Cyber

[29] Austrian Federal Government Cabinet of Ministers, *Master Plan for the Protection of Critical Infrastructure* (2008), <http://www.kiras.at/uploads/media/MRV_APCIP_Beilage_Masterplan_FINAL.pdf>, (in German only), accessed 05 November 2014.
[30] The selection of companies was carried out along the Austrian Federal Economic Chamber's statistical classification of NACE, *Austria ÖNACE* (2008), <https://www.wko.at/Content.Node/Interessenvertretung/ZahlenDatenFakten/Oenace_2008_2014.html>, accessed 05 November 2014.
[31] Austrian Federal Agency for State Protection and Counter Terrorism <http://www.bmi.gv.at/cms/bmi_verfassungsschutz/>, [in German], accessed 06 November 2014.
[32] The Austrian Government Computer Emergency Response Team <www.govcert.gv.at>, accessed 06 November 2014.

Security Strategy (ACSS),[33] an operational structure involving the Federal Chancellery, Ministry of Defence (MOD), Ministry of Interior (MOI) and Ministry of Foreign Affairs (MOFA), is under development and will include the creation of a central coordinating authority, acting as a platform for developing an intervallic and incident-related Cyber Security Picture, as well as discuss potential operational measures. In addition, the Cyber Security Steering Group at governmental level was established and is responsible for monitoring and supporting the collaborative implementation of the ACSS and for coordinating all measures relating to cyber security at a political-strategic level.

1.3. Cross-border aspects

According to the assessment of the Austrian expert, there are four sectors which show a critical dependence on cross-border information infrastructure. These sectors are 1) information systems and telecommunications; 2) the financial sector; 3) the energy sector; and 4) the industrial production sector. Three sectors out of the ten given choices were associated with a substantial dependency on cross-border information infrastructure. Additionally, the domestic and international trade sector was named as one of those showing a substantial dependency on trans-border information infrastructure.

When it comes to listing potential risks arising from locating CII outside national borders, Annex 1 of the ACSS[34] has to be emphasised. Annex 1 provides a Cyber Risk Matrix (2011) showing the probability of occurrence of certain risks ranging from technical to legal, including operating errors and massive attacks by state and non-state actors. Manipulation of transportation IT systems (air, train, road), a lack of security awareness and standards, and a lack of focus on regulations for IT security are taken into consideration as well as those risks emerging from the absence of a systematic technology impact assessment among a number of other threats.

It is the owners and operators of information and communication technology (ICT) that are primarily responsible for protecting their systems. Therefore, referring to the national expert, there is a call for obliging CI operators to report severe cyber incidents. Also, existing arrangements for the protection of CI – namely, the APCIP – and the Governmental Crisis and Civil Protection Management should be reviewed on an ongoing basis. This way the responsible bodies will continue to adapt to new cyber challenges, modifying their activities as required.

No particular measures for cross-border dependencies are foreseen in the Austria; however, the national expert considered the ACSS objectives related to global networking and international cooperation, both at the European and global levels, as involving the assessment and mitigation of cross-border dependencies of CII. Austria focuses in particular on exchanging information, formulating international strategies, developing voluntary schemes and legally binding regulations, prosecuting criminal cases, holding transnational exercises and conducting cooperation projects. Where appropriate, bilateral or international agreements will play a role and be taken into account.[35]

[33] Austrian Federal Chancellery, *Austrian Cyber Security Strategy* (ACSS) (2013) p 10, <https://www.bka.gv.at/DocView.axd?CobId=50999>, accessed 06 November 2014. The ACSS is based on the Governmental report on the *Austrian Security Strategy* (ASS) (2013), <https://www.bka.gv.at/DocView.axd?CobId=52251>, accessed 06 November 2014.
[34] ibid, p 18.
[35] ibid, p 16.

BELGIUM

2.1. Concept and designation

The Belgian Act on Security and Protection of Critical Infrastructure[36] offers the following definition of 'CI' (the term 'CII' is not specified, but suits the criteria included in the CI description):

> 'The term CI refers to an 'installation or a system or part thereof which is of federal interest and is essential for the maintenance of vital societal functions, health, safety, security and for the economic or social well-being of citizens, and whose interruption of operations or destruction would have a significant impact due to the failure of these functions'. [37]

The act distinguishes between 'critical national infrastructure' and 'European critical infrastructure', basing the distinction on the extent of the impact, that is whether an instance of interruption or destruction of critical infrastructure is contained within Belgium or causes a significant impact in at least two European Union countries.

The above definition, which corresponds with the one provided by Directive 2008/114/EC, also applies to sectors involved with electronic communication and is valid for the IT aspects of other CI sectors such as energy, transport and finance. CII in Belgium is being approached as a distinct sector, while it is also seen as a part of CI.

Critical sectors addressed under the Act include the transport sector (road, rail, waterways), the energy sector (electricity, oil, gas, production and transmission), the financial sector, and the electronic communications sector.

The process of identifying the particular CI objects within each sector is fixed to the Act. According to Article 5 § 1, the 'sectoral authority' is designated to identify the national and European critical infrastructure object. Taking a closer look at Article 3,1° a)-d) this 'sectoral authority' is specified as:

> 'Concerning the transportation, the energy or finance sector it is the corresponding Minister or, in case of delegating the task, the sectoral authority can also be one of the administrative staff members of the Minister.'

The same applies for the electronic communication sector, although there is a slight difference due to an additional option: Article 3,3° (d) assigns the identification of a critical infrastructure object alternatively to a member of the Belgian Institute for Postal Services and Telecommunication.[38]

---

[36] *Loi du 1er juillet 2011, Loi relative à la sécurité et la protection des infrastructures critiques* (2011), <http://www.ejustice.just.fgov.be/mopdf/2011/07/15_2.pdf#Page6>, [in French], accessed 02 July 2014. The Act is the implementation of EU Directive 2008/114/EC. In contrast to the EU directive, the Act does not only apply for the transportation and energy sector, but also for the finance and communication sector. See further at <http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2011070108&table_name=loi>

[37] Definition in original text: 'Une infrastructure critique est une 'installation ou un système ou partie de celui-ci, d'intérêt fédéral, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'interruption du fonctionnement ou la destruction aurait une incidence significative du fait de la défaillance de ces fonction.'; ibid art 3.

[38] Belgian Institute for Postal Services and Telecommunications <http://www.bipt.be/en>, accessed 23 September 2014.

2.2. Responsibilities

National coordinating bodies and their responsibilities

The operator is responsible for risk analysis in preparation of the security measures in its security plan. This plan is to be inspected by the inspection services of the sectoral authority. Two types of criteria are used for identifying and designating CI: intersectoral criteria, which are valid for all critical sectors, and sectoral criteria specific to a particular sector. The sectoral authority creates the sectoral criteria according to the distinctive characteristics of the sector in question following consultation with the Directorate-General of the Crisis Centre (DGCC)[39] of the Federal Public Service Interior and, when indicated, after consultation with the regions concerned.[40]

The intersectoral criteria are already set out in Article 6,§3 and are predicated on the following aspects:

1. Human loss, namely the potential number of dead or injured people;
2. Economic impact, namely the extent of economic loss or the degradation of products and services and their impact on the environmental surrounding; and
3. The effect on the population, namely their trust, the physical suffering and the disruption of daily routine and essential services

Having identified potential national critical infrastructures, the sectorial authority provides a list to the Directorate-General of the Crisis Centre and when indicated to the concerned region, where the CI designation is upheld upon their approval. [41]

In the event that a cross-border critical infrastructure is identified, the national point of contact for the protection of critical European infrastructure within the Directorate-General Crisis Centre is obliged to initiate bilateral or multilateral discussions with the affected EU member states in cooperation with the sectoral authority and, when indicated, with the regions concerned.

When an agreement is reached on existing critical European infrastructures located on Belgian territory, the sectoral authority proceeds to apply the designation to the agreed infrastructure and notifies the operator about the decision and its accompanying motives.[42] At this point, the operator bears direct legal responsibility for the CII under Section 3, Article 12ff of the Act. The National Crisis Centre and the Directorate-General of the Crisis Centre[43] is the national coordinating body for the protection of CI across public and private entities.

Within one year of the notification of the designation of an object as critical infrastructure, the General Directorate prompts the coordinating organ for the analysis of threats (OCAM)[44] to provide a threat analysis of the CI and of any sub-sectors of which it forms a part. This analysis consists of an evaluation which must assess how the concerned threats to the CI are likely to manifest, and if they have already been detected, how those threats may develop and which measures might be necessary to take.[45]

---

[39] The Director- General of the Crisis Centre is in charge of the special protection of goods and people and of the national coordination of the public order in Belgium; term meaning in original text art 3,1°: '*direction générale Centre de Crise du Service public federal Intérieur, chargée de la protection spéciale des biens et des personnes et de la coordination nationale en matière d'ordre public';* <http://centredecrise.be/fr>, accessed 23 September 2014

[40] Loi relative à la sécurité et la protection des infrastructures critiques (n 36), art 6 s 1er.

[41] ibid Art 7 s 1, accessed 02 July 2014.

[42] Loi relative à la sécurité et la protection des infrastructures critiques (n 36) art 7 s 2 and art 8.

[43] Belgian National Crisis Centre <http://crisiscentrum.be/nl>, accessed 06 November 2014.

[44] Original term 'O*rgane de Coordination pour l'Analyse de la Menace',* <http://crisiscentrum.be/fr/content/evaluation-de-la-menace-0>, accessed 24 September 2014;

[45] Loi relative à la sécurité et la protection des infrastructures critiques (n 36) art 10.

Responsibilities of the operator

The operator of critical infrastructure holds a set of responsibilities, including implementing security measures, maintaining security documentation, monitoring obligations and notifying and reporting obligations.

Establishment of a point of security contact:[46] These set of responsibilities are described in Section 3, Article 12ff of the Act on Security and Protection of Critical Infrastructure. It designates a point of security contact from where data will be passed on to the sectorial authority within a time frame of six months, starting from the day of the notification of the designation of the object as a critical infrastructure and every six months thereafter.

This security contact point shall be available at any time, serving as contact point for the sectoral authority, the Directorate-General of the Crisis Centre, the mayor and the police regarding all types of questions related to the security and protection of a critical infrastructure. When such a contact point already exists as stipulated by standing national or international provisions for a sector or subsector, the operator shall forward its information to the relevant sectoral authority.

Elaboration of an operator's security plan:[47] The operator shall further elaborate an operator's security plan which aims to prevent, mitigate, and neutralise risks to the functional interruption or destruction of the critical infrastructure by taking material and internal organisational measures. This security plan must be set up within a year of the notification of the designation of the object as a critical infrastructure. Within the same timeframe the operator shall implement the internal measures envisaged by the operator's security plan.

The operator is also responsible for organising exercises, updating the operator's security plan depending on the lessons learned from those exercises or any modifications arising from the exercises' risk analysis.

The frequency of exercises and necessary updates of the operator's security plan though is determined by the King. It is also the King who determines the modalities of participation of the police services in the course of operator-organised exercises.

The Royal Decree[48] of 27 May 2014, incorporating the electronic communications sector within Article 13 of the Act of 1 July 2011 specifies not only the content of security measures but also the information which must be included in the operator's security plan. Article 2 of the decree provides a brief list of the minimum elements to be included in the security plan:

1) A generic description of the critical infrastructure;
2) A risk analysis;
3) Internal and permanent security measures;
4) Internal gradual security measures;
5) Description of exercises; and
6) Specified details to the internal gradual security measures (as set in Article 6 of the decree).

[46] ibid Art 12.
[47] ibid Art 13.
[48] Royal Decree of 27th May 2014, 'Arrêté royal exécution dans le secteur des communications électroniques de l'article 13 de la loi du 1er juillet 2011 relative á la sécurité et la protection des infrastructures critiques', C-2014/11429, MB 11.08.2014, <http://www.bipt.be/en/operators/telecommunication/legislation/national-framework/royal-decree-of-27-may-2014-implementing-in-the-electronic-communications-sector-article-13-of-the-act-of-1-july-2011-on-the-security-and-protection-of-critical-infrastructures>, accessed 25 September 2014.

In addition to those legal provisions or regulations which impose in certain sectors and subsectors the responsibility to inform certain determined services, Article 14 of the Act requires that the operator immediately notify the Centre for Information and Communication.[49]

2.3. Cross-border aspects

The research did not reveal many activities concerning the cross-border aspect. No legal obligations pertaining to CI operators, CII administrators, or the cyber crisis management coordinating body to assess or mitigate dependencies on CII have resulted from their location or potential location outside national borders. However, the Cyber Security Strategy foresees bilateral cooperation as a matter of the utmost importance in general, and even without explicitly pointing it out, this fact is most likely to apply to the cross-border dependencies of CII.

CZECH REPUBLIC

3.1. Concept and designation

Critical infrastructures are addressed in Act No. 240/2000 Coll. on Crisis Management (the Crisis Management Act), as amended by Act No. 320/2002 Coll. and Act No. 430/2010 Coll. [50]

The Crisis Act (§ 2m) lists nine sectors that are considered critical for the Czech Republic. These include energy, water management, the food industry and agriculture; health services; transport, communication and information systems the financial market and currency; emergency services; and public administration. 'Cross-cutting' and sectoral criteria, defined on the basis of the Act, are used to determine the 'critical infrastructure elements' within each of these sectors.[51]

The Act on Cyber Security and Change of Related Acts (Act No. 181/2014 Coll., came into force on 01 January 2015)[52] defines critical information infrastructure (§ 2b) thus:

> 'Critical information infrastructure means an element or system of elements of the critical infrastructure in the sector of communication and information systems within the field of cyber security.'

Notably, critical information infrastructure by this definition only includes 'elements of the critical infrastructure in the sector of communication and information systems'.[53] 'Electronic communication network[s] providing direct international interconnection to public communication networks or providing direct

[49] All relevant legal acts can be accessed at <http://crisiscentrum.be/nl/inhoud/kritieke-infrastructuur-0> [in French], accessed 06 November 2014.
[50] Crisis Management Act no 240/2000 Coll., <http://www.hzscr.cz/hasicien/file/crisis-management-act-n-240-2000-coll-pdf.aspx>; Critical infrastructure is defined in s 2 (g) as 'the element of critical infrastructure or the system of elements of critical infrastructure, disruption of which would have a significant impact on the State security, on ensuring the basic living needs of the population, on health of people and State economy'.
[51] Crisis Management Act no 240/2000 Coll., s 4 (d), <http://www.hzscr.cz/hasicien/file/crisis-management-act-n-240-2000-coll-pdf.aspx>.
[52] Act on Cyber Security and Change of Related Acts (Act on Cyber Security) no 181/2014 Coll., <http://www.govcert.cz/download/nodeid-577/ > or at <http://www.govcert.cz/download/nodeid-591/> [in English].
[53] Information and communication systems handling classified information are beyond the scope of the Act (n 52).

connection to critical information infrastructure' are considered 'important networks' (§ 2 g). The set of obligations upon operators in each category are different.[54]

3.2. Responsibilities

National coordinating bodies

Cyber security management and supervisory tasks with regard to critical information infrastructure are divided between the national CERT and the NSA. The national CERT handles information sharing on at national and international level. It keeps records of contact information for administrators of 'important networks' (including those electronic communication networks that provide direct connection to critical information infrastructure), handles notifications about cyber security incidents, evaluates cyber security incidents, and carries out vulnerability analyses. In addition, the CERT provides coordination and assistance to administrators of 'important networks' and acts as a point of contact. The CERT coordinates its activities with the NSA and is authorised to share incident information with the NSA (§ 17).

The NSA, and the governmental CERT as its structural unit in particular (§ 20), have tasks primarily with regard to the administrators of critical information infrastructure information and communications systems.[55] The NSA administers information supplied by the administrators, evaluates events and incidents, and provides administrators with support. The governmental CERT also 'provides cooperation' during cyber security events and incidents. It is also the Czech contact point for cyber security authorities outside the Czech Republic and is responsible for information exchange for incidents.

The NSA is authorised to require corrective action from operators under its supervision in case of 'deficiencies' or in the event of immediate danger by a cyber security incident (§ 24). Under § 13, the NSA is further entitled to issue decisions on reactive measures to solve a cyber security incident or to secure information systems or networks and electronic communication services from a cyber security incident.

On the basis of incident analysis and with the purpose of improving the security of information systems or services or electronic communication networks, the NSA may also issue protective measures of a general nature, which under steady state are mandatory for the administrators of critical information infrastructure information and communication systems (§ 14-15), but during the 'state of cyber emergency' (defined in § 21 of the Act) or general state of emergency, also apply to administrators of important networks and important information systems.

Responsibilities of the operator

§3 of the Act on Cyber Security determines 'liable persons' (public authorities and natural and legal persons) who bear responsibilities for cyber security nationally. With regard to critical infrastructure, these include:

- Public authorities or natural and legal persons administrating an important network;
- Administrators of critical information infrastructure information systems; and
- Administrators of critical information infrastructure communication systems.

[54] Moreover, a category of 'important information systems' is defined in the Act, which is not critical information infrastructure, but may 'endanger or noticeably limit the performance of public administration in case of information security breach'; see Act on Cyber Security (n 52) s 2 (d).
[55] As well as administrators of important information systems, which are not considered part of CI.

Administrators of information systems and communication systems of critical information infrastructure are obliged to implement security measures and to keep records of security measures in security documentation (§ 4(2)). Such security measures include both organisational[56] and technical measures.[57] The content and extent of the security measures, as well as requirements for security documentation, are to be defined by forthcoming secondary legislation.[58] Critical information infrastructure providers are obliged to follow these requirements in their selection of information and communications system providers.

Legal obligations also pertain to:

- Detecting cyber security events (potential breaches) and incidents (actual breaches) in their networks and systems (§ 7);
- Reporting cyber security incidents in their networks and systems to the NSA (§ 8 (3)) (in addition to informing duties defined in other legal acts, such as the informing duty of operators of electronic communications networks);
- Submitting to specific 'reactive and protective measures' (§ 11-15) necessary for protecting networks and systems from cyber threats or incidents, or necessary for resolving an incident; and
- Notifying the NSA of their contact details and any subsequent changes thereof (§ 16 and 29).

For administrators of 'important networks', only three of these obligations apply: they are required to report cyber security incidents in their networks and systems to the national CERT (§ 8 (2)), they must subject to 'reactive measures' in the event of a state of cyber emergency or state of emergency (§ 11 (3) a)), and they are required to notify their contact details to the national CERT.

3.3. Cross-border aspects

Cross-border dependency aspects are not specifically addressed in the Act on Cyber Security; neither are they considered in the Crisis Act. The authority of the NSA to impose reactive, protective and corrective measures, as outlined above, applies in a general manner.

In accordance with § 20j of the Cyber Security Act, the governmental CERT, as part of the NSA, performs vulnerability analysis in the field of cyber security. In doing so, it may receive and analyse data from cyber security authorities abroad, as well as provide 'incidents record data' to cyber security authorities abroad to the extent necessary to ensure the protection of cyberspace (section 4 of § 9).

[56] Including information security management system, risk management, security policy, organisational security, security requirements on suppliers setting, assets management, human resources security, critical information infrastructure or important information system operation and communication management, access of persons to critical information infrastructure or to important information system management, acquisitions, development and maintenance of critical information infrastructure and important information systems, cyber security events and cyber security incidents management, business continuity management, and critical information infrastructure and important information systems control and audit.

[57] Including physical security, communication networks integrity protection tools, users' identity verification tools, access authorisation management tools, counter malicious code protection tolls, critical information infrastructure and important information systems, their users and administrators activities recording tools, cyber security events detection tools, collection and evaluation of cyber security events tools, application security, cryptographic devices, tools for ensuring the levels of information availability, and industrial and management systems security.

[58] National Security Authority of the Czech Republic, *Draft Regulation on Important Information Systems* (2014), <http://www.govcert.cz/download/nodeid-1227/> with explanatory report at <http://www.govcert.cz/download/nodeid-1257/>; and *Draft Regulation on Cyber Security* (2014), <http://www.govcert.cz/download/nodeid-1216/> with explanatory report at <http://www.govcert.cz/download/nodeid-1304/>.

ESTONIA

4.1. Concept and designation

The Estonian approach to critical infrastructure protection builds upon the concept of 'vital services', which are listed (but not defined) in the Emergency Act[59] (§ 34). The list includes 43 vital services in the notional categories (or sectors) of justice system; public security and public order; government and public administration; utilities, transport, and communications; medical services; environmental services; food and drinking water safety; and financial services. 'Information systems used for the provision of the vital service and the related information assets' – in essence, CII – are an object of specific legal and regulatory measures on the basis of § 40 of the Act.[60]

4.2. Responsibilities

National coordinating bodies

The Emergency Act appoints nine government ministries and public bodies with responsibilities in managing the continuous operation[61] of the vital services, with the Ministry of Interior bearing the overall national coordinator role. The obligations of the agencies are outlined in § 35; these include coordination of vital service operation, advising vital service providers, supervision over ensuring the continuous operation of vital services; and regular reporting to the national coordinator (Ministry of Interior). The Act authorises the responsible ministries to issue secondary legislation for two purposes: establishing the description of the vital service, and establishing continuous operation requirements for the vital services.

The supervisory body for compliance with vital service electronic security requirements is the Estonian Information System Authority.[62] The latter has the mandate of a law enforcement authority as defined in the Law Enforcement Act[63] and may, in case of a failure of the vital service provider to comply with the requirements described above, issue precepts or impose fines of up to €20,000 (Chapter 6 of the Emergency Act).

Finally, the Information System Authority is responsible for developing an emergency risk assessment to address the risk of a vital service-relevant cyber incident, and for preparing the national emergency plan for large scale cyber incidents.[64] The scope of both documents, however, is wider than incidents affecting vital services. The relevant emergency risk assessment is to be presented to the Ministry of Interior as the national

[59] Hädaolukorra seadus (RT I 2009, 39, 262), passed 15.06.2009. [Emergency Act; English translation available <https://www.riigiteataja.ee/en/eli/517122014005/consolide> accessed 19 December 2014].
[60] Vabariigi Valitsuse 14.03.2013 määrus nr 43 "Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmed" (RT I, 20.03.2013, 7) (Security Measures for Vital Service Information Systems and Related Information Assets; English translation available at <https://www.ria.ee/public/KIIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf >, accessed 03 December 2014). In the regulation, adopted on the basis of the Emergency Act 2009 § 40, *an information system used for the provision of the vital service* is defined as an information system that affects the operation of an activity whose interruption would severely jeopardise the capacity of an institution or enterprise to provide vital services and hinder the achievement of the goals set out by the institution or enterprise upon providing the service; see § 2 (1)-(2).
[61] Understood as the 'capability of consistent functioning and the ability to restore consistent functioning after an interruption'.
[62] Emergency Act (n 59) § 47 (2) 2).
[63] Korrakaitseseadus (RT I, 12.07.2014, 84), passed 23.02.2011. [Law Enforcement Act; English translation available <https://www.riigiteataja.ee/en/eli/522082014007/consolide> accessed 19 December 2014].
[64] Emergency Act (n 59) §§ 6 and 7.

coordinator for vital services, and it is to be updated periodically,[65] and it is to be taken into account in the preparation of development plans of relevant authorities.[66] In case of a major cyber incident that requires the activation of the emergency response plan, the Information System also leads incident response activities.[67]

Responsibilities of the operator

The providers of a vital service, as well as their duties, are defined in § 37 of the Emergency Act. Providers can be both state or local government authorities or legal persons, depending on their actual supply of any of the vital services listed in § 34. In certain cases, a natural person may also be regarded a vital service provider. Providers of vital services have the following obligations:

- Preparing a continuous operation risk assessment;
- Preparing a continuous operation plan for the particular service offered;
- Notifying events which significantly disturb the continuous operation of the vital service, or an impending risk of such incident; and
- Subjecting themselves to the supervision of competent authorities over the continuous operation of the vital service.

Guidelines for implementing these obligations are defined in secondary legislation. Moreover, other obligations may be defined by law or by secondary legislation.

In particular, under § 40 of the Emergency Act, providers of vital services are obliged to ensure 'the constant application of security measures' with regard to the 'information systems used for the provision of the vital service and the related information assets'. Such security measures are established by Government regulation (Regulation No. 43 of the Government of the Republic of 14 March 2013)[68] and include (§§ 3-5):

- Incorporating, in the risk assessment of continuous operation referred to in § 37, an assessment of the extent that information systems affect the operation of the critical activity;
- Creating and implementing an information security management system that takes into account the principal activities and risks of that particular vital service provider; and
- Appointing a contact person who will be responsible for notifying the Estonian Information System Authority of any security incidents with significant impact and reporting about incident resolution.

4.3. Cross-border aspects

With regard to vital service information systems which are located in a foreign country, the provider of the vital service is required to ensure the continuous operation of the vital service also in a manner and by means not dependent on information systems located in foreign countries.[69]

The continuous operation risk assessments and continuous operation plans required under §§ 37 and 40 of the Emergency Act are to include an assessment of cross-border dependency on information systems as well as the measures foreseen to prevent and respond to disruption.

[65] Types of emergency for which a risk assessment and emergency response plan is to be prepared are defined by a Government order (Vabariigi Valitsuse 25.04.2013 korraldus nr 208 'Nende hädaolukordade nimekiri, mille kohta koostatakse riskianalüüs ja lahendamise plaan, ning hädaolukorra riskianalüüsi ja hädaolukorra lahendamise plaani koostamiseks pädevate täidesaatva riigivõimu asutuste määramine' (RT III, 30.04.2013, 16) [in Estonian]).
[66] Emergency Act (n 59) § 6.
[67] Estonian Information System Authority <https://www.ria.ee/en/>, accessed 02 December 2014.
[68] Security Measures for Vital Service Information Systems (n 60).
[69] Emergency Act (n 59), § 40.

The revised Estonian Cyber Security Strategy adopted in September 2014 specifically addresses vital service cross-border dependencies on information infrastructure. Subsection 1.2. of the Strategy defines the objective to ensure that information relating to dependencies on critical services provided from outside the Republic of Estonia is kept up to date, the extent of their impact on the functioning of services is promptly evaluated, and associated risks are systematically reduced.[70] Detailed activities with regard to achieving this objective are outlined in the Implementation Plan to the Strategy.

The Estonian Information System Authority monitors compliance with this requirement both in a reactive (by assessing the continuous operation plans submitted by vital service providers) as well as a proactive manner (by inquiry to specific vital service providers).

FRANCE

5.1. Concept and designation

Under the fluid French approach, designations of critical infrastructure are broadly contextualised, rather than delineated in specific facilities or sectors. Article R. 1332-2 of the French Defence Code specifies:

> 'An industry of critical importance...consists of activities contributing to a common objective, which:
>
> 1. Relate to the production and the distribution of indispensable goods and services needed:
>   a. to satisfy the basic needs of human life;
>   b. to exercise state authority;
>   c. to operate the economy;
>   d. to maintain defence capabilities;
>   e. to provide for the security of the nation;
>
>   when these activities are difficult to substitute or replace;
> 2. Or can pose a serious danger to the public.' [71]

In the French Cyber Security Strategy, Operators of Critical Importance (OIV: *Opérateur d'importance vitale*), are defined as operators of critical infrastructure, either as public or private operator(s) referred to under L.1332-1 and L.1332-2 of the French Defence Code, who 'exercise activities cited in Article R. 1332-2 and included in a critical sector' and which 'manages or uses for this activity one or more organisations or works, one or more facilities, whose damage, unavailability or destruction due to malicious action, sabotage or terrorism would directly or indirectly seriously compromise the military or economic capabilities, the security or the survival ability of the nation or seriously threaten the lives of its population.'[72] Additionally, obligations pertaining to operators of critical infrastructure may be extended to managers of specified institutions under Article L.511-1 of the Environmental Code or managers of a nuclear installation under Article L.593-1 of the

[70] Estonian Ministry of Economic Affairs and Communications, *Cyber Security Strategy 2014-2017* (2014) <https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf> accessed 02 December 2014.

[71] French Defense Code, art L. 1332-2, original legal text available at <http://www.legifrance.gouv.fr/affichCode.do;jsessionid=FE83165666A431AE6F030DBDB97612DE.tpdjo17v_2?idSectionTA=LEGISCTA000028342597&cidTexte=LEGITEXT000006071307&dateTexte=20141113>, accessed 03 July 2014.

[72] Agence Nationale de la Sécurité des Systèmes d'Information, *Information Systems Defence and Security: France's Strategy* (2011), p 22 *Glossary*, <http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf>, accessed 03 July 2014.

Environmental Code 'when the destruction or damage to certain facilities of these institutions may pose a serious threat to the population.'[73]

The Prime Minister's Order of 2 June 2006 'Establishing on the List of the Sectors of Critical Infrastructure and Designating Coordinating Ministers of these Sectors'[74] lists 12 vital sectors in its annex – typically dealing with state issues, the protection of citizens as well as concerning the economic and social life of the nation: state civil activities, law enforcement activities, military activities of the state, food, electronic communication – including broadcasting and information, energy, space and research, finance, water management, industry, health, transportation.

France does not have a specific definition for Critical Information Infrastructure, but under 'Chapter IV: Provisions on the Protection of Critical Infrastructure against the Cyber Threat' of 'Act No. 2013-1168 of 18 December 2013 on Military Programming for the years 2014 to 2019 and Various Provisions Concerning Defence and National Security' (hereafter 'the Military Programming Act') substantial updates to the French Defence Code have specified information systems operators as distinct 'operators of critical infrastructure' under the determinant Acts, Articles R. 1332-1 and R. 1332-2.[75]

5.2. Responsibilities

Under the authority of the Prime Minister of France, the General Secretariat for Defence and National Security (GSDNS) is responsible as the central coordinating body for critical infrastructure protection, including critical information infrastructure protection.[76] Since July 2009, The National Security Agency Information Systems (ANSSI) has served as the national authority for the security of information systems, provisioning assistance to the GSDNS, creating and implementing measures to protect information systems proposed by the Prime Minister as well as under the strategic guidance of the GSDNS' Strategy Committee for the Security of Information Systems. ANSSI's core mission is to monitor, prevent, detect and react to cyber attacks as the central cyber defence mechanism for the government of France's classified networks. As regards CII, ANSSI aims to 'prevent threats by supporting the development of trusted products and services' and 'to provide reliable advice and support to governmental entities and operators of critical Infrastructure,' as well as serve as a pool of expertise for technical assistance to both the public and private sector.[77] Under Article 5 of Decree No. 2009-834 of 7 July 2009 Establishing a National Service Called 'National Security Agency Information

[73] French Defense Code, art L. 1332-2, original legal text available at <http://www.legifrance.gouv.fr/affichCode.do;jsessionid=FE83165666A431AE6F030DBDB97612DE.tpdjo17v_2?idSectionTA=LEGISCTA000028342597&cidTexte=LEGITEXT000006071307&dateTexte=20141113>, accessed 03 July 2014.

[74] Prime Minister's Order on Establishing on the List of the Sectors of Critical Infrastructure and Designating Coordinating Ministers of these Sectors, 2 June 2006, original text available at <http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20060604&numTexte=1&pageDebut=08502&pageFin=08502>, accessed 14 November 2014.

[75] Act No 2013-1168 on Military Programming for the years 2014 to 2019 and Various Provisions Concerning Defence and National Security, 18 December 2013, original text available at <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte&categorieLien=id>, accessed 14 November 2014.

[76] French General Secretariat for Defence and National Security <http://www.sgdsn.gouv.fr/site_rubrique70.html>, accessed 27 November 2014.

[77] French National Security Agency Information Systems (ANSSI), *Missions,* <http://www.ssi.gouv.fr/fr/anssi/missions/>, accessed 14 November 2014.

Systems, ANSSI specifically supports the security of information systems of vital installations under the remit of the coordinating ministers of the sectors of critical infrastructure.[78]

Operators of information systems when designated as operators of critical infrastructure are required by the updated provisions of French Defence Code outlined by Article 22 of the Military Programming Act to meet the obligations listed therein.[79] Consequently, operators of critical information systems are legally obligated to comply with 'sets of safety rules necessary for the protection of those information systems' outlined by the Prime Minister; to implement intrusion detection systems operated by service providers acting under the authority of ANSSI or the Prime Minister; and to submit their information systems to either ANSSI or a service appointed by the Prime Minister to verify the level of security and compliance with the Prime Minister's safety rules.

Additionally, Article 22 of the Military Programming Act mandates that in response 'to major crises threatening or affecting the security of information systems of critical infrastructure, the Prime Minister may decide on measures that operators […] must implement.'[80] All requisite legal, organisational, and technical obligations are implemented at the expense of the operator of information systems designated as an operator of critical infrastructure.

5.3. Cross-border aspects

France, both in its 2013 White Paper on Defence and National Security and Cyber Security Strategy, acknowledges that cross-border dependencies on networking and information systems, particularly the internet, demand the state collaborate closely with equipment manufacturers and operators of critical infrastructure 'to guarantee and improve the security of these critical systems.'[81] France's surveyed national expert identified 'Information Systems and Telecommunications' cross-border dependencies as 'critical,' while 'energy supply,' 'finance,' and 'traffic and transportation,' were all rated as holding 'substantial' dependencies. The remaining sectors were estimated as of minimal cross-border dependency.

The Prime Minister coordinates and sets policy for the protection of information systems, including those provisions specifically aimed at coordinating international collaboration and mitigating cross-border dependencies. ANSSI's Sub-Directorate for External Relations and Coordination (*Sous-direction Relations Extérieures et Coordination*) is responsible for coordinating intergovernmental and private sector relations and for representing the French Government on the international stage.

Notably, the Prime Minister is responsible for setting the conditions of technical responses to a cyber attack which is aimed at destroying the national information systems but which can have a wider impact on the

[78] Government Decree No 2009-834 Establishing a National Service Called *'National Security Agency Information Systems*', 7 July 2009, original legal text at <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212>, accessed 27 November 2014.
[79] Act No 2013-1168 on Military Programming for the years 2014 to 2019 and Various Provisions Concerning Defence and National Security, 18 December 2013, art 22, original text available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte&categorieLien=id, accessed 14 November 2014.
[80] ibid.
[81] Agence Nationale de la Sécurité des Systèmes d'Information, *Information systems Defense and Security: France's strategy* (2011), p 7, <http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf>, accessed 27 November 2014.

economy or security. The measures can also include 'neutralising (the attack's) effects by accessing the information systems that are at the origin of the attack.'[82]

GERMANY

6.1. Concept and designation

The Cyber Security Strategy for Germany provides the following definition for the basic term CI:

> 'Critical infrastructures are organizations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences.' [83]

A legal definition of the term CI or CII could not be detected, but in 2014 Germany produced a draft of a new IT-security Act[84] which includes a similar definition in Article 1, declaring assets, constructions or parts of the following sectors as CI: energy, ICT, transport and traffic, health, water, nutrition as well as the finance and insurance sectors.

The Federal Office for Information Security (BSI) presents the following definition of CII: 'The term Critical Information Infrastructure refers to the information and communication technology sector (ICT) as well as to the ICT-based infrastructures of other sectors.'[85]

Germany places emphasis on the fact that CII is a central component of almost all CI and of growing importance. Therefore, the German Cyber Security Strategy stresses that the protection of CII is their main priority of cyber security.[86] At the Federal level, the following areas (and subsectors) have been identified as critical:

Energy (electricity, gas, oil), information technology and telecommunications (telecommunications and information technology), transport, health (logistics, air-, maritime-, inland waterways-, rail & road-transport), water (public water supply and public sewage disposal), food (food industry and food trade), finance and

[82] Act No 2013-1168 on Military Programming for the years 2014 to 2019 and Various Provisions Concerning Defence and National Security, 18 December 2013, ch IV art 21, original legal text available at <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte&categorieLien=id>, accessed 14 November 2014.

[83] German Federal Ministry of the Interior (MOI), *Cyber Security Strategy for Germany* (2011), p 15, <http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile>, [in German; English translation available at <http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile> accessed 9 January 2015]; see also, *Nationale Strategie zum Schutz Kritischer Infrastrukturen (Kritis-Strategie)* (2009), p 3, <http://www.bmi.bund.de/cae/servlet/contentblob/598730/publicationFile/34416/kritis.pdf>, accessed 30 June 2014. A similar definition is provided by the German Federal Office for Information Security: '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';* see *recommendations for Critical Information Infrastructure Protection',* <https://www.bsi.bund.de/EN/Topics/Criticalinfrastructures/criticalinfrastructures_node.html>, accessed 30 June 2014.

[84] German Federal Ministry of the Interior, *News report: Federal Minister of the Interior at the IT Summit* (2014), <http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/EN/2014/10/it-summit.html>; see IT-Security Act Draft, <http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf?__blob=publicationFile>, [in German], accessed 07 November 2014.

[85] Author's translation from original version available at <https://www.bsi.bund.de/DE/Themen/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html>, accessed 07 November 2014.

[86] Cyber Security Strategy for Germany (n 83) p 6.

insurance industry (banks, stock exchanges, insurance companies, financial service providers), state and administration (government and public administration, parliament, judicial bodies, emergency rescue services including civil protection) as well as media and culture (broadcasting – like television and radio-, print and electronic media, cultural property, structures of symbolic meaning).[87]

Germany recently presented the draft of its new IT Security Act[88] – the result of the German Cyber strategy 2011. The Act had not passed the legislative process at the time of this research, but seems likely be approved. The draft is intended to secure critical infrastructure of sectors relating to energy, information and telecommunication, transport, health, water, and food, as well as the finance and insurance sector in a pioneering way.

One of the striking features of the draft is that it establishes an 'every-two-year-obligation' for companies to provide evidence that they have done everything possible to defend their systems and mitigate risk for systems supporting CI. It establishes a 'technical inspection authority,' to audit companies operating in the sensitive field of CI.

6.2. Responsibilities

The Ministry of the Interior, in its draft of the IT Security Act, obliges operators of CI to notify a still undetermined contact point at the BSI in the event of a security incident. Operators and companies providing and controlling the software used by critical infrastructures which have already suffered serious incidents often do not want to reveal these violations because they fear a loss of reputation. Once the Act has passed there will be an obligation to report cyber incidents to the BSI. With the help of the new IT-Security Act, more information on the number and depth of cyber incidents will be widely available. It is yet not clear whether companies will take this obligation seriously as there remains no clear method of monitoring fulfilment. In minor cases though, this can be done anonymously**,** which might increase the likelihood of timely and accurate incident reporting. It is then up to the BSI to assess incoming data to generate an attack pattern in order to warn exposed companies of active and upcoming cyber threats. In addition, the latest version of the draft (which was approved by the Federal Government but still has complete the legislative process) also imposes an obligation on providers to warn their customers if they notice that the user's connection is being misapplied – for instance as part of a botnet.[89] It also enables the BSI to run security tests of publicly available IT products and systems in order to evaluate them, and to publish their assessments.[90]

[87] ibid, p 15; specifically for the subsectors, see <http://www.kritis.bund.de/SubSites/Kritis/EN/introduction/sectors/sectors_node.html>, accessed 01. October 2014.

[88] Draft of German Law on the Security Enhancement of IT systems (IT-Security law) 18 August 2014, <http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf?__blob=publicationFile> accessed 21 August 2014.

[89] Art. 5 no 3.c) 4.b) of the draft of the IT-Act: <http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf?__blob=publicationFile>; <http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/12/bundeskabinett-beschlie%C3%9Ft-it-sicherheitsgesetz.html>, accessed 08 January 2014.

[90] Art. 1 no 6. Of the draft of the IT-Act: <http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf?__blob=publicationFile>; <http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/12/bundeskabinett-beschlie%C3%9Ft-it-sicherheitsgesetz.html>, accessed 08. January 2014.

Given the widening scope of its mandate, the BSI[91] will create 133 new positions with costs of €8.8 million and an annual budget of €5 million.[92]

Existing legislation which imposes special duties for operators can be also be found in 'federal Länder-made laws'.

Legal obligations usually cover the following aspects: implementing security measures, maintaining security documentation, monitoring obligations, submitting to specific security measures or government guidelines in the case of incidents as well as notifying and reporting obligations.

The BSI serves as the coordinating body for the protection of CII during routine everyday operation while the Ministry of Interior (BMI) assumes responsibility for the protection of CII during crisis situations.

6.3. Cross-border aspects

Referring to the German survey answers, one sector (finances) was marked with a critical dependency on cross-border information infrastructure, while additional five sectors were regarded with a substantial degree of dependency (energy, ICT, traffic and transportation, government and administration, and media). The risks involved were seen from different legal, social, and technical angles and include problematic aspects of differing legislation, failure of communication systems, the rising complexity of society, differing security cultures, and the risk of not using an 'all hazards' approach.

The National Strategy for Critical Infrastructure Protection (CIP Strategy)[93] is one of the documents pointing out the cross-border aspect in its chapter on international cooperation, emphasising at the same time its importance in the field of information and communications technologies as well as energy and transport infrastructure. Germany clearly states its support for all efforts and measures identifying and minimising vulnerabilities to critical infrastructure, particularly trans-border infrastructure. Accordingly, Germany focuses on the exchange of information and best practices as well as for the coordination of measures to protect trans-border critical infrastructures.

The German Cyber Security Strategy addresses the problem of cross-border dependencies on critical information infrastructure in a brief and generic way in its section entitled 'framework conditions'. The section acknowledges that 'incidents in other countries' information infrastructures may also indirectly affect Germany'[94]. In consequence, the strategy points out the relevance of enforcing international rules of conduct, standards and norms, but also that a mix of domestic and foreign policy is needed to solve the complexity of

[91] German Federal Ministry of the Interior, *Bundesinnenministerium legt Entwurf für IT-Sicherheitsgesetz vor* (2014), <http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/08/einleitung-ressortabstimmung-it-sicherheitsgesetz.html>; for more information see <http://www.welt.de/politik/deutschland/article131352043/Die-Angst-der-Regierung-vor-dem-grossen-Blackout.html> and <http://www.welt.de/print/welt_kompakt/article131357115/Bund-plant-TUeV-fuer-IT-Sicherheit.html> and <http://www.lahrer-zeitung.de/inhalt.internet-neues-it-sicherheitsgesetz-soll-vor-cyberattacken-schuetzen.cad9850d-47b8-401b-a8bf-377992fa6ab0.html>, accessed 19 August 2014.

[92] Also the Federal Criminal Agency (BKA) will get additional 79 new positions, costs covered with approximately 5,4 million euros, and additional 630.000 euros for tangible means; additional but fewer positions and expenses are planned for other governmental entities that work on the prevention of cyber-attacks, such as the Federal Office for the Protection of the Constitution (BfV); see German IT-Security Law Draft, 18 August 2014, p 7, <http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf?__blob=publicationFile> and <http://www.faz.net/aktuell/politik/inland/de-maiziere-ueber-die-digitale-agenda-deutschland-wird-it-vorreiter-13103217.html>, accessed 19 August 2014.

[93] German Federal Ministry of the Interior, *National Strategy for Critical Infrastructure Protection* (2009), p 18, <http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf>, accessed 02 October 2014.

[94] Cyber Security Strategy for Germany (n 83) p 4.

the trans-border problem. Enhancing the framework conditions for drawing up common minimum standards (a code of conduct) with allies and partners is considered to be key to improving cybersecurity.

National strategy objectives with regard to CIIP

Initially the National Plan for Information Infrastructure Protection (NPSI),[95] issued in 2005, represented the Government's principal strategy for the protection of ICT and ICT-dependent assets. The three main strategic and security tasks mentioned are:

1) Adequate prevention of the information infrastructure in Germany;
2) Effective reaction whenever an IT-incident occurs; and
3) Sustainability through strengthening German IT-security by setting up international standards.

Two implementation plans, most importantly 'KRITIS', evolved in 2007 shortly after the NPSI was set up. In 2009 the National Strategy for Critical Infrastructure Protection (CIP Strategy)[96] followed, specifically pointing out the risks and threats for Critical Information Infrastructure. Eventually the 2011 Cyber Security Strategy for Germany was enacted as the continuation of the NPSI, among other things, now representing the enhancement of framework conditions in the cyber security sector.[97] The BSI is responsible for the supervision of the strategy.[98]

The German strategic objectives and measures against current threats outlined by the 2011 Cyber Security Strategy mentions as foremost among other strategic areas[99] the 'protection of critical information infrastructures'.[100] The positioning leads to the conclusion that this area is the fundamental priority of cyber security. Subsequently, closer coordination between the public and the private sector based on intensified information sharing has been seen as critical and helped foster Implementation Plan KRITIS ('UP KRITIS'), where a number of different task forces were set up which deal with intra-sectoral and cross-sectoral work.[101] Representatives from the economic as well as the administrative sides, had already been formed, but the core aim of the UP KRITIS is to secure the regular functionality of critical infrastructure in Germany.

The involvement of the 'National Cyber Security Council'[102] is of great value. Among other tasks, the Council helps examine whether additional sectors are to be included in the cooperation network, whether the

---

[95] German Federal Ministry of the Interior, *National Plan for Information Infrastructure Protection* (2005), <http://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf>, accessed 02 October 2014.

[96] German Federal Ministry of the Interior, *National Strategy for Critical Infrastructure Protection* (2009), <http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf>, accessed 02 October 2014.

[97] German Federal Office for Information Security, *Schutz Kritischer Infrastrukturen* <https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Content_Cyber-Sicherheit/Strategie/kritis/kritis.html;jsessionid=2983CDCEAA93577F138A1C9B21B6E09C.2_cid359> accessed 01 October 2014.

[98] German Federal Office for Information Security <http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html>, accessed 01 October 2014.

[99] The other strategic areas concern: 2. Secure IT systems in Germany, 3. Strengthening IT security in the public administration, 4. National Cyber Response Center, 5. National Cyber Security Council, 6. Effective crime control also in cyberspace, 7. Effective coordinated action to ensure cyber security in Europe and worldwide, 8. Use or reliable and trustworthy information technology.

[100] Cyber Security Strategy for Germany (n 83), p 6 (f).

[101] German Federal Office for Information Security, *CIP Implementation Plan* (2007), <https://www.bsi.bund.de/EN/Topics/Criticalinfrastructures/ImplementationPlan/implementationplan.html>, accessed 02 October 2014.

[102] The National Cyber Security Council plays an important role within the chosen strategic objectives and measures and is therefore described in a separate strategic area of the Cyber Strategy; see Cyber Security Strategy for Germany (n 83) p 9.

introduction of new technologies is necessary and advisable, whether protective mandatory measures have to be implemented, and whether additional powers are required in case of specific threats. Eventually it is planned to examine the necessity of introducing harmonising rules aimed at maintaining critical infrastructures during IT crises.

HUNGARY

7.1. Concept and designation

Hungary follows the critical infrastructure concept set out in the EU Directive: critical infrastructure is an asset, system or part of thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, the disruption or destruction of which would have a significant impact as a result of the failure to maintain those functions. The relevant basic provisions are defined in Act CLXVI of 2012 on the identification, designation and protection of vital systems. Ten sectors are considered as vital: these are energy, transport, water, ICT, financial, agriculture, industry, public health, government, and public security and defence management.

Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies[103] defines 'vital information system elements' as 'electronic information facilities, tools or services of vital system elements designated by law as European vital system elements or national vital system elements, whose failure or destruction would make the vital system elements designated by law as European vital system elements or national vital system elements, or any parts thereof, unavailable or severely reduce their operability' (Section 1(33)). While the Act primarily applies to the 'electronic information systems' of central and local government agencies[104], Section 2(2)c) of the Act extends its application to '[electronic information] system elements designated by law as European vital system elements or national vital system elements.'

7.2. Responsibilities

The tasks of the national coordinating and supervisory body for the protection of critical infrastructure in Hungary lie with the National Directorate General for Disaster Management (of the Ministry of Interior), who possesses a wide range of competences, including regulatory and supervisory authority in the areas of industrial safety, fire safety and civil protection.[105] With regard to critical information infrastructure protection, responsibilities are held by the CIP CERT operated by the National Directorate General for Disaster

[103] Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies. <http://www.nbf.hu/anyagok/Act%20L%20of%202013%20on%20the%20Electronic%20Information%20Security%20of%20Central%20and%20Local%20Government%20Agencies.docx> accessed 07 November 2014.

[104] Section 2 of Act L (ibid). These include central state administration bodies (minus the Government and its committees), Offices of the President of the Republic, Parliament, and the Constitutional Court, as well as the National Office for the Judiciary and courts, prosecution services, the Office of the Commissioner for Fundamental Rights, the State Audit Office, and the National Bank of Hungary. Moreover, the Act also covers the Budapest and county government offices, offices of the representative bodies of local and nationality governments and the administrative associations of the authorities, and the Hungarian Defence Forces. According to the Act's explanatory memorandum, the Government and Government Committees remain outside the personal scope of the act since they perform their tasks as bodies without an independent organisational structure and independent electronic information systems. Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies. Justification for the Act on the Electronic Information Security of Central and Local Government Agencies. <http://www.nbf.hu/anyagok/Act%20L%20of%202013%20on%20the%20Electronic%20Information%20Security%20of%20Central%20and%20Local%20Government%20Agencies.docx> accessed 07 November 2014.

[105] Zsolt Boszormenyi, Mark Szente. 2015. 'National Directorate General For Disaster Management (NDGDM)'. *Katasztrofavedelem.Hu*. Accessed January 5 2015. http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_intro&lang=eng.

Management, and the government CERT within the Special Service for National Security. Furthermore, specialised CERTs such as those of the Ministry of Defence and the media and telecommunications regulator hold certain specific tasks.[106]

Act L of 2013 defines roles and responsibilities with regard to 'electronic information system security' of government agencies, but also 'vital information infrastructure' or 'vital information systems'. The Act established a new authority, the Cyber Defence Management Authority, within the 'organisational framework of the Ministry led by the minister in charge of information technology', with independent responsibilities and official powers to 'take, order and monitor any measure for the protection of a particular electronic information system to manage threats to the relevant electronic information system' (Sections 14 and 16). Such broad authorisation includes the right to check the relevant organisations' compliance with statutory security requirements and procedural rules, but also to engage the National Security Authority – either upon the request of the [Authority] or upon the request of the affected organisation – to conduct vulnerability assessments and provide action plans for the elimination of vulnerabilities (Section 18).

Concerning vital information infrastructure in particular, the primary tool foreseen in Act L is domestic and international CIIP exercises , and various bodies including the Authority, the National Security Authority, the Government Incident Management Centre and the National University of Public Service have a mandate to organise, contribute and participate (Sections 18 to 23).

In crisis situations, the Ministry of Interior coordinates the protection of critical information infrastructure. This would also be the case in major cyber incidents.

According to the national expert, Hungarian national law does not specify direct legal responsibilities of entities or individuals for the security and functioning of critical information infrastructure.

7.3. Cross-border aspects

Legal obligations to assess and mitigate cross-border dependencies on critical information infrastructure appear to be defined by a governmental legal regulation (for the state and local government levels); the national cyber security strategy further foresees measures that are deemed relevant for cross-border dependencies, in particular relating to identification process in ICT sector, increasing the number of CERTs, participation in international exercises, and distribution of good practices.

A noteworthy restriction to data storage and management is contained in Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies. To mitigate risks arising from cloud computing and service outsourcing to entities beyond national reach, the Act limits data asset management outside of Hungarian territory: in accordance with Section 3(2), electronic information systems which are designated by law as European vital system elements or national vital system elements may only be operated in the territory of the Member States of the European Union. Furthermore, if the operator is not registered in Hungary, a representative must be appointed to act in the territory of Hungary, who will be responsible for compliance with the provisions of the Act (Section 4).

Data managed by governmental bodies[107] may in any case only be managed in electronic information systems operated in the territory of Hungary, unless 'limited-purpose electronic information systems used for diplomatic information purposes' are used (Section 3(1) and (2)).

[106] Krasznay Csaba, Török Szilárd, Hungary's Cyber Defense Readiness from the Perspective of International Recommendations, IX. Évfolyam 1. szám - 2014. március <http://hadmernok.hu/141_20_krasznaycs.pdf> accessed 07 November 2014.

ITALY

8.1. Concept and designation

The Italian concept of CI is closely based on Directive 2008/114/EC. Legislative Decree 11 April 2011, n. 61[108] represents the implementation of the EU Directive, while Art. 2 of the Decree contains a number of definitions including one for CI, which is anchored to the same wording used in the EU Directive:

> 'Critical Infrastructure: Infrastructure, located in a Member State of the European Union, which is essential for the maintenance of vital societal functions, health, safety and economic and social welfare of the population, and the disruption or the destruction of which would have a significant impact in the state, due to inability to maintain those functions.'

Those CI which have been designated by the Italian government can be found in the Decree of the Minister of the Interior on the Identification of CII of national interest.[109] According to Article 1 of the decree, computerised information infrastructure should be considered of national interest as well as those systems and information services which support the institutional functions of:

a) Ministries, agencies and institutions that they supervise, operating in the fields of international relations, security, justice, defence, finance, communications, transport, energy, environment, health;
b) The Bank of Italy and independent authorities;
c) State-owned companies, regions and municipalities appealing metropolitan areas of no less than 500,000 people, operating in the fields of communications, transport, energy, health and water conservation; and
d) Any other institution, administration, organisation, person, public or private, whose activities, for reasons of law enforcement and public security are recognised of national interest by the Minister of the Interior, or on proposal of the prefects- the provincial authorities of public safety.

8.2. Responsibilities

The National Organisation for Crisis Management, also known as the title of the final version of the Decree of the President of the Council of Ministers of 5th May 2010 set up two bodies. Firstly, it created the Political Strategic Committee (CoPS) as the political authority for crisis management and secondly, the Nucleus Inter Ministerial Unit for Situation and Planning (NISP) as the central coordinating authority for the Italian Government both in times of stability and crisis.[110] CoPS is chaired by the President of the Council of Ministers and otherwise comprised of the ministers of foreign affairs, the interior, defence, the economy and finance.[111]

---

[107] See the list of such governmental bodies in n 104. The prohibition does not apply to the Hungarian Defence Forces and foreign missions due to their inherent functions which require their ability to work with their information systems and data abroad.

[108] Legislative Decree no 61, 11 April 2011, <http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2011-05-04&atto.codiceRedazionale=011G0101&elenco30giorni=false>, [in Italian]; for a short summary see <http://terna2011.message-asp.com/en/electricity-system/italy%E2%80%99s-regulatory-framework>, accessed 04 December 2014.

[109] Decreto del Ministro dell'Interno (Decree of the Ministry of Internal Affair), 9 January 2008, <http://archivio.cnipa.gov.it/HTML/RN_ICT_cron/si_20080109%20Decreto%20Ministero%20interno.pdf>, (Italian only), accessed 14 November 2014.

[110] Decree of the President of the Council of Ministers of 5 May 2010 final (National Organization for Crisis Management), <http://www.gazzettaufficiale.it/gunewsletter/dettaglio.jsp?service=1&datagu=2010-06-17&task=dettaglio&numgu=139&redaz=10A07594&tmstp=1276847998921>, [in Italian], accessed 04 December 2014.

[111] ibid, Art 4.

NISP, in its support of CoPS, is chaired by the Secretary of State, and staffed with two representatives each from ministries including MOFA, MOI and MOD as well as from agencies and other administrative bodies as Agency Information and Internal Security (AISI) and the Department of Fire, Rescue and Public Civil Defence.[112]

CoPS primary function is to serve as an advisory body and avenue of governance for the President of the Council of Ministers, which, relating to crisis management, 'evaluates the elements of the situation, examines and defines measures to be approved by the Council of Ministers, and also, when necessary, authorises, on a temporary basis, the adoption of countermeasures in respect of the general guidelines of the government, treaties and international agreements.'[113]

NISP, giving agency to the measures proposed by CoPS, is tasked with crisis prevention and emergency preparedness, supporting inter-ministerial coordination, harmonising common procedures and capabilities (information sharing, intelligence gathering, inter-ministerial and operational planning, international collaboration), as well as developing crisis exercises with domestic and international partners.[114] In the event of a crisis, NISP maintains a coordinating role, but also acts to examine the situation, identify and propose measures to be taken by CoPS and the President of the Council of Ministers, as well as formulating the national position and collaborative efforts vis-à-vis international actors. Notably, in the execution of its crisis preparation and response mandate, and particularly in regard to CI and civil defence planning, NISP relies heavily on the approval and support from the Ministry of the Interior and its Inter-Ministerial Technical Commission for Civil Defence (CITDC).[115]

The Ministries of the Interior, Defence, the Department of Civil Protection of the PCM, the Ministry of Economic Development (energy sector), and the Ministry of Infrastructure and Transport (Transport Sector), are responsible for all actions to secure nationally located CI/CII in their respective sectors, as well as informing NISP of these actions or proposed actions.[116] Individual installations of CI fall under the supervision of a 'Prefect of Territorial Jurisdiction,[117]' a local authority that serves as the responsible entity for infrastructure protection at the local level. Additionally, each relevant authority must nominate a liaison officer to serve as a point of contact with the property manager of each individual installation of critical infrastructure, as well as the local 'Prefect.'

Operators are required[118] within 30 days of receiving the designation as an installation of European Critical Infrastructure to submit the name of a liaison officer for safety, to the 'Prefect,' to the property owners, and to the relevant authority of the designated infrastructure. The authority, through its liaison officers, works with the operators and owners of a designated critical infrastructure to conduct a risk analysis that will either serve to create or update an Operator Safety Plan that meets the minimum standards outlined by the EU's directives on CI. After the creation or update of the Safety Plan, completed within one year of an installation's designation, the relevant parties must review the Safety Plan once every five years.

[112] ibid, Art 5.
[113] ibid, Art 4.
[114] ibid, Art 6.
[115] ibid, Art 6 para 4 I; and Legislative Decree no 61, Implementation of Directive 2008/114/EC of 11 April 2011 on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, art 4 para 5-6 <http://www.governo.it/Governo/Provvedimenti/testo_int.asp?d=63162;> accessed 24 November 2014.
[116] ibid, art 11 para 1.
[117] ibid, art 11 para 2.
[118] ibid, art 12 para 1-8.

The national Computer Emergency Response Team (CERT-N) under the Ministry of Economic Development, which coordinates CERT-N with NISP, is responsible for cybersecurity of domestic CII as the 'national capability to survey and react to potential threats and actual attacks.'[119]

Operators of public communication services and networks accessible to the public, as well as operators of critical infrastructure who rely on computer and telecommunication systems are legally obliged by Legislative Decree N. 259/2003 (the Electronic Communication Code):[120] to notify the Cybersecurity Unit of the Prime Minister's Military Advisor's Office of significant violations of their computer systems and networks; to adopt the best practices and measures for cyber security; to provide information and access to information security authorities when required by Law N. 124/2007;[121] and to collaborate with cyber crisis management authorities.[122]

8.3. Cross-border aspects

Concerning the assessment of dependencies on cross-border infrastructure as enquired after by this NATO CCD COE survey, the Italian expert's response was interesting. Three sectors, namely energy supply, information systems and telecommunications, and finances, were classified with a cross-border dependency on information infrastructure of a 'substantial level,' whereas the remaining seven sectors were assessed with having only a 'minimal dependency.' No additional sectors were mentioned with a cross-border dependency of remarkable value.

Beside those obligations listed above and arising from the Legislative Decree, 11 April 2011, n. 61, no additional or specific obligations could be detected for any other actors pertaining cross-border dependencies mitigation or assessment.

Insofar as this area still remains to be dealt with by bilateral and multilateral agreements, NISP serves as the Italian point of contact for EU members and the EU Commission in regard to the Protection of European Critical Infrastructure. NISP also disseminates best practices and guidelines drafted by the EU to the relevant authorities, 'Prefects,' owners, and operations of European Critical Infrastructure.

LATVIA

9.1. Concept and designation

Critical infrastructure in Latvia in general is designated on the basis on the National Security Law, which defines critical infrastructure as 'objects, systems or parts of systems located on the territory of Republic of Latvia, which are important for implementation of functions vital to society and for provision of health protection, security, economic and social welfare, and destruction or malfunction of which would significantly affect the functions of the State.' While this definition also includes critical information infrastructure, a specific act on

[119] Presidency of the Council of Ministers of the Government of Italy, *National Strategic Framework for Cyberspace Security* (December 2013, Rome), p 23, <http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf>, accessed 25 November 2014.
[120] Legislative Decree no 259, Electronic Communications Code, 18 December 2013, (OJ 214 of 09.15.2003 - Suppl. Ordinario n. 150), art 16-bis, para 2, letter b), <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-08-01;259>, accessed 25 November 2014.
[121] Law no 124, 'Information System for the Security of the Republic and New Secret Discipline', 3.08.2007, (author's translation); <http://www.camera.it/parlam/leggi/07124l.htm, accessed 25 November 2014.
[122] Decree of the President of the Council of Ministers, Directive Laying down Guidelines for the National Defence and Cyber Security, 24 January 2013, (OJ Series General n.66 of 19/03/2013), art 11 para 1.

cyber security – the Law on the Security of Information Technologies[123] – further addresses 'critical infrastructure of information technologies'.

The Latvian approach to CI does not rely on specified critical sectors; rather, any infrastructure found to meet the criteria of criticality can be designated as critical infrastructure. The decision to designate a particular infrastructure – including IT infrastructure – as critical is taken by the government cabinet in accordance with the National Security Law.

9.2. Responsibilities

National coordinating bodies

The Commission of Intermediary Institutions for State Security is responsible for coordinating the protection of critical infrastructure in Latvia. The Commission is an advisory collegial institution, chaired by the Ministry of Internal Affairs and consisting of representatives from government ministries;[124] public agencies such as the Police, State Fire and Rescue Service; Armed Forces; security agencies such as the Constitution Protection Bureau; CERT Latvia; and the National Bank.[125] The Commission evaluates ministerial input[126] regarding the designation of critical infrastructures and proposes the results to the Cabinet for approval;[127] it also prepares legislative proposals to the Cabinet for improving critical infrastructure security, including competency allocation and planning activities.[128]

For critical information infrastructure (or the 'critical infrastructure of information technologies'), the role of coordinating security measures is shared between the state security service, the Constitution Protection Bureau,[129] and the national CERT – the Information Technology Security Incident Response Institution of the Republic of Latvia –, operating under the Ministry of Defence.[130] The activities of both agencies in the area of CII are governed by Information Technology Security Law and a Cabinet regulation that further specifies the planning and implementation of security measures.[131]

The Constitution Protection Bureau cooperates with the CERT and CI owners and legal possessors in ensuring the assessment and management of the current risks of the critical IT infrastructure. The Bureau informs the owners of the critical infrastructure of the designation of their systems as CI and approves the appointment of the person responsible for the security of the particular CI. It has a right to examine personnel related to ensuring the operation of the CI; request the national CERT to conduct inspections of CI to determine the vulnerability and security risks of the relevant critical infrastructure; and give recommendations to CI owners for the elimination of the detected deficiencies. It may also issue recommendations to state administrative

[123] Law on the Security of Information Technologies (2010); English text available at <http://www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_the_Security_of_Information_Technologies.doc>.
[124] Defence; Foreign Affairs; Economics; Finance; Interior; Transport; Justice; Health; and Environmental Protection and Regional Development.
[125] Cabinet Regulation No. 496, 'Procedures for the Identification of Critical Infrastructures, Including European Critical Infrastructures and Planning and Implementation of Security Measures', 1 June 2010, s 6.
[126] Beyond the relevant ministries, proposals to designate an infrastructure as CI can also be made by the Security Police, the Constitution Protection Bureau or the Military Intelligence and Security Service.
[127] Cabinet Regulation No 496, s 18.
[128] ibid s 35.
[129] The Constitution Protection Bureau <www.sab.gov.lv> .
[130] Information Technology Security Incident Response Institution of the Republic of Latvia <https://www.cert.lv/?lang=en>, for further information see <https://www.cert.lv/section/show/12>.
[131] Cabinet Regulation No 100, 'Procedures for the Planning and Implementation of Security Measures for the Critical Infrastructure of Information Technologies', adopted 1 February 2011, <http://likumi.lv//ta/id/225776>; English translation at <http://www.vvc.gov.lv/export/sites/default/docs/LRTA/MK_Noteikumi/Cab._Reg._No._100_-_Planning_and_Implementation_of_Security_Measures.doc>.

institutions who supervise the CI owners. The Bureau, together with the Latvian CERT, also periodically informs the National Information Technologies Security Council regarding current threats to critical infrastructure.[132]

The Information Technologies Security Incidents Response Institution (CERT.LV) provides support for and coordinates CII incident prevention, inter alia by cooperating with the Constitution Protection Bureau and CI owners in risk assessment and risk management. With regard to the implementation of security measures for critical infrastructure, the primary measure foreseen by the regulation is security inspection. Based on such inspections, the CERT may issue recommendations to the CII operator.[133]

Responsibilities of the operator

Direct legal responsibility for the security and functioning of critical information infrastructure lies with the owner or legal possessor of the critical infrastructure. The CI owner is required to define security measures based on identified risks, document these measures, and present the documents to the Constitution Protection Bureau on the latter's request. It has a legal obligation to ensure the security of the CI in such a way that the identified risks are managed.[134]

The CI owner shall appoint a person responsible for the security of the critical infrastructure, who will stand for planning security measures for the critical infrastructure, and, in cooperation with the Constitution Protection Bureau and the Latvian CERT, ensure the assessment and management of the current risks of the critical infrastructure.[135]

Further sectoral security measures may apply to CII operators in the financial and capital markets, as well as for state information systems.

9.3. Cross-border aspects

No particular legal measures are defined to address cross-border CII dependencies. Such issues can potentially be brought to the attention of the Commission of Intermediary Institutions for State Security by the responsible ministries, services or security agencies in accordance with the mechanisms defined in National Security Law. The Commission may then perform the necessary communications with the European Commission and European Union Member States.

As noted in the survey, measures taken nationally to assess and mitigate cross-border dependencies on critical information infrastructure primarily comprise bilateral agreements and cooperation.

THE NETHERLANDS

10.1. Concept and designation

Dutch national law does not address critical infrastructure in particular, neither does it provide a legal definition of critical infrastructure or criteria for defining critical infrastructure. The Netherlands takes a policy

[132] Cabinet Regulation No 100, ch II and III.
[133] ibid.
[134] ibid, s 8-10.
[135] ibid, s 7.

approach to critical infrastructure protection based largely on public-private cooperation between responsible government ministries and other bodies, and private sector critical infrastructure operators.[136]

The country's approach to threats against the vital interests of society is outlined in the National Safety and Security Strategy,[137] which addresses all national security-relevant threats in a single framework.[138] The implementation method of the Strategy is further detailed in the Guidelines for the National Security Implementation Method, published by the Ministry of Security and Justice.[139] The core of the method is the annual National Risk Assessment, which involves threat identification, and impact and likelihood assessment. This is used to define risk prevention, preparation and response measures. The annual assessments have analysed a number of critical information infrastructure threat and vulnerability scenarios including energy security and ICT breakdowns.

Critical infrastructure in the Netherlands is divided into twelve critical sectors containing 31 essential products and services provided by both the private sector and public bodies. The sectors are energy; telecommunications and ICT; drinking water; food; health; the financial sector; surface water management; public order and safety; legal order; public administration; transport; and the chemical and nuclear industries.[140]

A description of each critical sector is maintained by the Critical Infrastructure Strategic Consultative Body (*Strategisch Overleg Vitale Infrastructuur*, SOVI), who also directs the mapping of vulnerabilities and inter-dependencies of critical infrastructure.[141]

A legislative process currently appears to be underway to define the criteria for critical infrastructure as well as redefine the current national critical infrastructure.

10.2. Responsibilities

National coordinating bodies

Critical infrastructure protection in general falls within the governance of the Netherlands Ministry of Security and Justice.[142] The entity directly responsible for coordinating critical infrastructure protection in the Netherlands is the National Coordinator for Security and Counterterrorism,[143] who cooperates with several ministries in the Netherlands which are each responsible for the critical infrastructure in their domain.

[136] Booz & Company (Italia) Srl, Stock-Taking of Existing Critical Infrastructure Protection Activities (European Commission 2009).
[137] Ministerie van Veiligheid en Justitie, *Strategie Nationale Veiligheid* (2007), <https://www.nctv.nl/Images/strategie-nationale-veiligheid-2007_tcm126-495325.pdf>, accessed 12 November 2014. An overview of the national safety and security method in English is available in the Ministry's publication *Working With Scenarios, Risk Assessment And Capabilities In The National Safety And Security Strategy of the Netherlands* (2009), <http://www.preventionweb.net/files/26422_guidancemethodologynationalsafetyan.pdf>, accessed 12 November 2014.
[138] Government of the Netherlands, *National Security*, <http://www.government.nl/issues/crisis-national-security-and-terrorism/national-security> , accessed 12 November 2014.; E Pruyt and D Wijnmalen, 'National Risk Assessment In The Netherlands: A Multi-Criteria Decision Analysis Approach (ed), *Multiple Criteria Decision Making for Sustainable Energy and Transportation Systems. Proceedings of the 19th International Conference on Multiple Criteria Decision Making, Auckland, New Zealand, 7th - 12th January 2008* (Springer 2010).
[139] *Working with Scenarios* (n 137).
[140] Government of the Netherlands, *Protecting Critical Infrastructure*, <http://www.government.nl/issues/crisis-national-security-and-terrorism/protecting-critical-infrastructure>, accessed 12 November 2014.
[141] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, *5 Vragen Over Het Strategisch Overleg Vitale Infrastructuur (SOVI)* (2010), <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/brochures/2009/06/23/5-vragen-over-het-strategisch-overleg-vitale-infrastructuur-sovi/5vragenoversovi-1.pdf>, accessed 12 November 2014.
[142] Protecting Critical Infrastructure (n 140).
[143] National Coordinator for Security and Counterterrorism <https://english.nctv.nl/>, accessed 02 December 2014.

Coordination for critical information infrastructure protection lies with the National Cyber Security Centre within the Department for Cyber Security of the Ministry of Security and Justice.

The National Coordinator for Counterterrorism and Security (NCTV) is also responsible for the coordination of national crisis and disaster preparedness and response, including cyber security.[144] In cyber crisis situations, that is when cyber incidents have a disruptive effect on society, the National Cyber Security Centre, and the ICT Response Board activated within the National Cyber Security Centre in particular, will have an 'upgraded' mandate to coordinate incident response and provide advice.[145]

The Netherlands national cyber security strategy (NCSS 2) emphasises the government's supervisory role 'which may include determining regulations and standards for the vital sectors', doing so in consultation with the vital sectors. The strategy points out the intent to widen the scope of existing sectoral regulatory authorities to include cyber security.[146]

Responsibilities of the operator

As the Dutch CIP system is based on public-private partnership and responsibility within each critical sector, there is no overarching legal act to define the responsibilities of CI operators or CII administrators in ensuring the security and functioning of CII, but some sectoral legal acts do exist. With regard to the critical sector of telecommunications and ICT, the Telecommunications Act[147] defines the responsibilities of public electronic communications networks and publicly available electronic communications services regarding the security and integrity of the networks and services provided by them.

In accordance with Article 11a.1, electronic communications network and service providers[148] should 'take appropriate technical and organisational measures to control risks to the security and integrity of their networks and services'. The Ministry of Economic Affairs may also impose obligations for technical or organisational measures with respect to the security and integrity of these networks and services, as well as subject a network operator or service provider to a security audit at the latters' expense.

Network and service providers are obliged to notify the Ministry of Economic Affairs of significant security breaches and loss of integrity in their networks and services; they must also provide, on request, information necessary to assess the security and integrity of their networks and services. The Minister may decide to disclose information about the breach to the public or require the service provider to do so if disclosure of such information is in the public interest (Article 11a.2).

In accordance with Article 15.2, the Minister of Economic Affairs and the Netherlands Authority for Consumers and Markets are authorised to impose administrative penalties to enforce operator and service provider

[144] Central Government, *Crises en rampen voorkomen* (2014), <http://www.rijksoverheid.nl/onderwerpen/veiligheid-en-terrorismebestrijding/crises-en-rampen-voorkomen>, accessed 8 October 2014.
[145] National Cyber Security Centre (NCSC), *Coordination During Crisis,* <https://www.ncsc.nl/english/services/crisis-management-reinforcement/coordination-during-crisis.html>, accessed 13 November 2014; NCSC, *ICT Response Board*, <https://www.ncsc.nl/english/services/crisis-management-reinforcement/ict-response-board.html>, accessed 13 November 2014.; E van den Heuvel and GK Baltink, 'Coordination and Cooperation in Cyber Network Defense: The Dutch Efforts to Prevent and Respond', (ed) *Best Practices in Computer Network Defense: Incident Detection and Response* (IOS Press 2014) 120.
[146] Ministry of Security and Justice, National Cyber Security Strategy: From Awareness to Capability 2 (2013) 19.
[147] Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet), <http://wetten.overheid.nl/BWBR0009950/volledig/geldigheidsdatum_12-11-2014> accessed 12 November 2014.
[148] The Telecommunications Act is primarily applicable to the operators of public electronic communications networks and providers of public electronic communications services (unless explicitly expanded to non-public networks and services as pointed in this section). For brevity, this section will refer to these parties as 'network and service providers'.

obligations. In urgent cases where non-compliance is serious and poses a direct threat to public security, public order or public health, a compliance order may be issued with immediate effect. The same is true where a spill over impact to other network operators or service providers is likely.

The Minister of Economic Affairs, in consultation with the Minister of Security and Justice or Minister of Interior and Kingdom Relations, is authorised to issue binding rules regarding the maintenance and operation of public electronic communications networks as well as the provision and use of their public electronic communications services where this is necessary in the interest of the security of the state (Article 18.9).

Chapter 14 of the Telecommunications Act outlines the rights of government authorities to issue directives in exceptional circumstances. If necessitated by the interests of national security, certain obligations specified in the Telecommunications Act can also be imposed upon the operators of non-public telecommunications networks, non-public telecommunications service providers, or leased line providers (Article 13.7).

10.3. Cross-border aspects

There are no particular legal obligations to assess and mitigate cross-border dependencies on critical information infrastructure in the Netherlands. A draft act on *Security Breach Notification* is currently in the parliamentary process and will place an obligation on relevant parties to report incidents in their CII.

The current National Cyber Security Strategy considers lines of action that are potentially relevant also to cross-border CII. The strategy emphasises the 'interwovenness' of the national and international dimensions, in particular ICT chain structure, and expresses the Dutch Government's intent to 'work to an effective joint public-private and civil-military response with the help of our international partners' in increasing the resilience of vital services and processes. The definition of basic security requirements will be based on risk analyses to be carried out.[149]

The strategy also proposes a study to determine the (technical and organisational) feasibility of creating **a** separate ICT vital network for public and private vital processes. The idea is to widen the range of options to safeguard the continuity of vital processes; such vital networks can also be used to set up private, cloud-based data storage.[150] The responsible ministry is the Ministry of Security and Justice and the deadline proposed foresees completion of the feasibility study in 2014.[151]

With regard to other measures taken nationally to assess and mitigate cross-border dependencies on critical information infrastructure, bilateral and multilateral networks were reported in the survey, in which the Netherlands is working together with relevant counterparts in other nations; in particular, a bilateral agreement with the US was pointed out.

[149] NCSS 2 (n 137) 9, 23.
[150] ibid 9, 24.
[151] ibid 28.

SPAIN

11.1. Concept and designation

In Spain there are two main legal instruments that deal with the regimentation of critical infrastructures: the Act for the Establishment of CIP Measures[152] and the Royal Decree for the Approval of the Regimentation of CIP.[153]

According to Article 2 e) of the Act for the Establishment of CIP Measures, critical infrastructure is considered as:

> 'The strategic infrastructures (that is, those that supply essential services) the functioning of which is necessary and does not allow alternative solutions, reason why their disruption or destruction would have serious impact on essential services.'

Spain classifies CI within the following twelve sectors listed in the annex of the Decree: administration, space, nuclear industry, research laboratories, chemical industry, water, energy, health, ICT, transport, food supply, financial and tax system.

CII in Spain is approached as information infrastructure and as such it is declared as part of CI, or as CI that supports a critical service or object. Spain has not separately defined CII.

11.2 Responsibilities

The Spanish protection system involves according to title II of the Act (Articles 5-13), a series of institutions, bodies and companies from the public and private sectors discharging the duties defined. Among this series of actors are the Secretariat of State for Security, the National Centre for the Protection of Critical Infrastructures (CNPIC), the ministries and organs appointed to the sectors (as shown in the annex to the Act), the autonomous communities, the governmental delegations of the autonomous communities, local corporations, the National CIP Commission, the intersectoral CIP task force and the public and private operators of CI. The following main agents shall be described for a quick overview:

According to Article 6 of the Act, the Secretariat of State for Security is the highest body of the Ministry of Interior. It is responsible for the overall protection system of the national CI and has a mainly coordinating function. Article 7 of the Act reveals that the National Centre for the Protection of Critical Infrastructures (CNPIC)[154] was created as the ministerial organ in charge of the coordination and supervision of all-embracing activities connected to CIP for which the Secretariat of State for Security is competent at national level.

Its duties are described by Article 7 and include:

- Assistance to the Secretariat of State for Security;
- Execution and maintenance of the National Protection Plan;

[152] Author's translation of the 'Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas', <http://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf>, accessed 10 November 2014.
[153] Author's translation of the 'Real Decreto 704/2011, de 20 de mayo por el que se aprueba el Reglamento de protección de las infraestructuras críticas', <http://www.boe.es/boe/dias/2011/05/21/pdfs/BOE-A-2011-8849.pdf>, accessed 10 November 2014.
[154] Spanish National Centre for the Protection of Critical Infrastructure <http://www.cnpic.es/en/index.html>, accessed 10 November 2014.

- Determination of the criticality of the strategic infrastructure; and
- Co-ordination of the risk analysis and evaluation of emergency plans.

The CNPIC is also the responsible institution in charge of coordinating CIIP during routine everyday operation as well as during crisis situations. The execution of this task is carried out by the Security and Industry Cert (CERT-SI) which is an organ of the National Institute of Cyber Security (INCIBE). The CERT-SI is jointly operated by CNPIC and INCIBE.[155]

For each strategic sector, there is at least one ministry, body or entity of the General State Administration involved in the protection system (Article 8 and the annex to the Act). They serve as contact points and carry the burden to provide the appropriate impulse for the governmental security policies.

The operators are the agents ultimately responsible for the functioning of C(I)I which means that they are in charge of making investments in the installations, networks and systems. Their list of duties is listed in to Article 13 of the Act:

- Providing technical assessment to the MOI, updating data at least on an annual basis;
- Collaboration with the CIP task force, elaborating strategic sectoral plans;
- Elaboration of the emergency plan – including a specific protection plan for each CI;
- Designation of responsible security persons; and
- Facilitating inspections by competent authorities.

11.3 Cross-border aspects

Four out of ten sectors were assessed as being of critical dependency on cross-border information infrastructure by the Spanish expert who participated in the survey (ICT, finances, government and administration, and media). An additional five were considered substantial (energy, healthcare, water supply, traffic and transportation, public security and public order). Only the nutrition/agriculture sector was classified as of minimal cross-border dependency on information infrastructure.

Notable is the high number of dependencies estimated as of higher dependency. This classification correlates with the obligation of CI operators who have to include their findings on cross-border dependencies in the main security plan. Therefore CI operators must detect and assess trans-border risks on a regular basis.

CII administrators also have to identify the relationship between ICT and the essential service provided by the CI operator. The findings on these dependencies must be reflected in the operator's and facilities security plans.

Availability risks referring to Denial of Service (DoS) were mentioned as specific risk with regard to the trans-border CII dependency.

Special measures in order to assess or mitigate the risks are described in the National Cyber Security Strategy[156] in general: All bodies and organisations responsible for cyber security must show collaboration and work in a cooperative manner. This way, it is ensured that the Security and CERT-SI, the CNPIC is able to initiate all the procedural and political measures needed in case of a major incident. In case of a major crisis, CNPIC is able to

[155] CERT, *Critical Infrastructures Incident Handling,* <https://www.incibe.es/CERT_en/Critical_Infrastructures/>, accessed 13 November 2014.
[156] Spanish Cyber Security Institute, *National Cyber Security, a Commitment for Everybody* (2012) 49, <http://www.ismsforum.es/ficheros/descargas/a-national-cyber-security-strategy-.pdf>, accessed 10 November 2014.

connect with the responsible body, which in this case is the National Security Department (DSN). Lastly, bilateral and multilateral agreements with other Nations are taken into account in order to improve information channels and the detection of cyber incidents.

TURKEY

12.1. Concept and designation

The Turkish concept of CI includes five sectors of critical importance which are set out together with the definition of CI in the 'Decree 2011/2237 on the Regulation Amending the Regulation on Military Forbidden Zones and Security Zones':[157] Energy, manufacturing, water management, transportation, and telecommunication. At its last meeting the Cyber Security Council of Turkey decided that Banking and Finance and Critical Public Services, including the health system, shall be added to the list. Regardless of this decision, until today this decision remained in the meeting record and has not been part of a legislative act or official document yet. Moreover, it only reflects the 2013-2014 Action Plan so far.[158] The Decree defines CI as: '[t]he public or private facilities that contribute to homeland security and national economy to a great extent. In case of partial damage or a pause of their functionalities, it may cause negative results in terms of national security and social order.'[159]

Taking a closer look at the National Cyber Security Strategy and the 2013-2014 Action Plan provide a similar definition but with different wording:

> 'Critical infrastructures: The infrastructures which host the information systems that can cause,
>
> - Loss of lives,
> - Large scale economic damages,
> - Security vulnerabilities and disturbance of public order at national level
>
> when the confidentiality, integrity or accessibility of the information they process is compromised,'

Similar to most other countries, there is a notable absence of a CII definition. However, CII is approached as a distinct critical sector or service.

12.2. Responsibilities

The coordinating body for the protection of CI is the Ministry of Transport, Maritime Affairs and Communications.[160] As indicated by its name, it is responsible for issues related to transport, maritime affairs, communication but also for improving postal business and postal services. This includes determining,

[157] Decree No. 2011/2237 on the Regulation Amending the Regulation on Military Forbidden Zones and Security Zones, 18th October 2011, <http://www.resmigazete.gov.tr/eskiler/2011/10/20111018-4.htm> [in Turkish], accessed 12 November 2011; besides listing the determined CI and providing a definition thereof, as indicated by its title, the decree does not refer to any other aspects related to cyber security.

[158] Ministry of Transport, Maritime Affairs and Communications, *National Cyber Security Strategy and 2013-2014 Action Plan* (2013) 23ff, <https://www.ccdcoe.org/sites/default/files/strategy/TUR_CyberSecurityEng.pdf>, accessed 13 November 2014; our acknowledgements referring this information go to the national expert, as the research did not show any information available in English on this aspect.

[159] Original text in Decree No 2011/2237 (translation provided by national expert): 'Yurt savunmasına veya yurt ekonomisine önemli ölçüde katkıda bulunan ve kısmen dahi tahripleri veya geçici bir zaman için faaliyetten alıkonmaları halinde milli güvenlik veya toplum hayatı bakımından olumsuz sonuçlar doğurabilecek kamu veya özel kuruluşlara ait alanlardır.'

[160] Ministry of Transport, Maritime Affairs and Communications <http://www.ubak.gov.tr/>, accessed 12 November 2014.

implementing and updating, when required, national policy, strategy and objectives on the aforementioned points.[161] The Information and Communications Technologies Authority bears direct legal responsibility for the security and functioning of critical information infrastructure both during everyday routine operations and during crises.

Legal obligations pertaining to CII can be found in Part Two (Articles 5-6) of the Electronics Communications Law (ECL).[162] Art. 6 ECL contains a whole set of obligations of the authority competent in the electronic communications sector. These include:

- Making necessary arrangements and supervisions pertaining to the rights of subscribers, users, consumers and end users;
- Conducting dispute resolution procedures between operators;
- Following the developments in the sector, conducting research in order to promote the development of the CI;
- Performing necessary regulations and inspections;
- Requesting any kind of information and documents from the operators, public authorities and institutions, natural persons and legal entities where deemed necessary;
- Inspection of the conformity of operators with legislation and imposing sanctions; and
- Ensuring the coordination with access providers, content providers, hosting providers and related other organisations in order to detect and avoid cyber-attacks and conduct activities in order to take precautionary measures[163]

As to the rights and obligations of the operators, the ECL foresees in Article 12 a list of utmost importance. The operator's obligation includes:

- Levying administrative charges;
- Ensuring interoperability of services and interconnection of the networks;
- Submitting information and documents to the Authority;
- Taking necessary measures for maintaining uninterrupted communication under major disaster situations; and
- Ensuring the security of network against unauthorised access.

The list contains an extensive variety of obligations among which there are monitoring and reporting obligations. Additionally, with the amendment of the ECL in 2014, the obligation of 'Submitting to specific security measures or government guidelines in the case of incidents' was added to the list.

12.3. Cross-border aspects

Referring to the question of which sectors or services show a particularly relevant dependence on cross-border information infrastructure, the energy as well as the traffic and transportation sector were assessed as having substantial dependency, and the information systems and telecommunication sector was classified as having critical dependency. The manufacturing sector was assessed as having minimal dependency on cross-border

[161] See also Legislative Decree on Organization and Duties of the Ministry of Transport, Maritime Affairs and Communication, 1.11.2011, <http://www.ubak.gov.tr/BLSM_WIYS/UBAK/en/en_dokuman_sol_menu/20120402_144700_204_2_64.pdf>, accessed 12 November 2014.

[162] Electronic Communications Law (ECL) (2008), updated version (2014) <http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6518.pdf> (in Turkish only), English non-updated version available at <http://eng.btk.gov.tr/mevzuat/kanunlar/dosyalar/5809.pdf>, accessed 12 November 2014.

[163] This obligation was added in an amendment of 2014 under the 10th article of the Law no 5651 – 'The Law of struggling with the crime that is committed by using Internet'; we are indebted for translation to the national expert.

located information infrastructure. None of the remaining seven sectors could be assessed due to a lack of knowledge, nor did research reveal any hints.

Notable is the emphasis of the national expert on the call for information sharing, which was mentioned by many other nations. Information sharing is regarded as crucial, not only after an incident but, and probably of greater importance, before an incident occurs. Further risks which are connected to cross-border dependencies, namely differences in perceptions, legislations and policies, were highlighted of being aggravating factors. So far, no specific legal regulations have been set up for the involved actors in order to assess and mitigate cross-border dependencies on CII, the National Cyber Security Strategy and the 2013-2014 Action Plan call for steps in an international direction, calling for more international cooperation and an increased use of international agreements and regulations.[164]

[164] Ministry of Transport, Maritime Affairs and Communications, *National Cyber Security Strategy and 2013-2014 Action Plan* (2013) 15ff, <https://www.ccdcoe.org/sites/default/files/strategy/TUR_CyberSecurityEng.pdf>, accessed 12 November 2014.

PART II.
Annotated bibliography

Academic publications[165]

1. Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research

By P. Pederson, D. Dudenhoeffer et al (Idaho National Laboratory 2006)

Available at http://www.inl.gov/technicalpublications/Documents/3489532.pdf

Keywords

Interdependency (types); infrastructure interdependency modelling; geospatial proximity; connectivity; interactions; infrastructure boundaries; vulnerabilities; interrelationship among infrastructures; cascading effects

Synopsis

An early fundamental work on critical infrastructure interdependencies. The report explains the concept of interdependence modelling and explains types of interdependency (including informational interdependency;[166] the main part of the report presents a survey on modelling tools to simulate critical infrastructure behaviour and identify interdependencies and vulnerabilities. Survey conclusions are helpful; individual survey results (presented in Appendix A) are mostly outdated.

Although not focusing on cross-border dependencies in particular, the report gives a conceptual and methodological foundation about critical infrastructure dependencies in general.

Recommendations

The report criticises the lack of standards which directly address infrastructures and specifically cross sector modelling, and suggests the development of a national or international cross-program working group with a central focus of infrastructure interdependency analysis.

2. Cross-Border Issues in Protecting Critical Infrastructure from Terrorism

By Kevin Freese. In James J.F. Forest (Ed.) Homeland Security: Protecting America's Targets (Greenwood Publishing Group 2006)

Keywords

Threats to critical infrastructure; sectoral threats; C(I)IP activities; international cooperation

[165] Any URLs to publications included in the bibliography were checked for accessibility as of 25 Nov 2014.
[166] The concept of types of interdependency originates from an earlier work published in 2001: Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, 'Identifying, Understanding and Analysing Critical Infrastructure Interdependencies', IEEE Control Systems Magazine, December 2001, 11-25. <http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf> accessed 7 May 2014.

Synopsis

The overall volume discusses the need to engage with the public in ensuring the security of critical infrastructure from terrorist threat, which implies the need to equip the public with the knowledge of where and why specific locations and activities may be a terrorist target, what is being done to protect those targets, and how they can help.

Chapter 6 of the volume relates, in particular, to cross-border issues in protecting critical infrastructure from terrorist threat, covering various sectoral threats (those related to energy supply are primarily relevant with regard to critical information infrastructure), steps that have been taken to protect the nation, and legal and cultural obstacles hindering international cooperation that need to be addressed, together with a long-term commitment to innovation, organisational learning, and public vigilance.

3. Modelling Interdependencies between the Electricity and Information Infrastructures

By Jean-Claude Laprie, Karama Kanoun, Mohamed Kaâniche (LAAS-CNRS, Université de Toulouse, France 2007)

Available at http://arxiv.org/ftp/arxiv/papers/0809/0809.4107.pdf

Keywords

Failures: cascading, escalating, common-cause, accidental, interdependency-related; electricity infrastructure; (global) information infrastructure

Synopsis

The authors demonstrate the effects of a failure resulting from the failure of one critical infrastructure (electricity) and linking to another, related critical infrastructure (the associated information infrastructure). The focus lies in the cascading and escalating failures which form part of the main causes of failures due to interdependencies. Hereby the relationships between two states in which the infrastructures are located are discussed. Notably, the operators' behaviour of each of the involved infrastructures are taken into consideration. Lastly, it is shown in brief how malicious attacks in the information infrastructure can be divided into different categories as: perceptible and deceptive ones or passive and active ones. Their effects to the discussed CIs are finally presented in brief. Figures and tables enhance the understanding of the technical description which is kept in a simple way anyhow.

4. Critical Infrastructure Dependencies 1-0-1.

By H.A.M. Luiijf, A.H. Nieuwenhuijs, and M.H.A. Klaver (2008)

Available at http://publications.tno.nl/publication/102547/FOpThI/luiijf-2008-critical.pdf

Keywords

Dependency and interdependency; cascading failures; realistic threat scenarios; cross-border dependency risk perception

Synopsis

The publication is a short paper providing a model view on critical infrastructure dependencies based on real-life data.[167] The findings indicate that energy and telecommunication sectors are main drivers of cascade effects of critical infrastructure failure; other sectors are more the 'victim' of dependencies than cascade initiators. The authors conclude that cascading effects due to dependencies appear to be more common than expected, while the number of multiple cascading events is lower than some models suggest and interdependencies hardly seem to occur when considering the major effects of disruptions.

Recommendations

The authors argue for updated models for critical infrastructure dependencies that take into account the increased understanding of existing dependencies.

5. International CIIP Handbook 2008/2009

By Elgin M. Brunner and Manuel Suter (Center for Security Studies, ETH Zürich 2008)

Available at http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf

Keywords

Critical sectors; national initiatives and policies; national law; early warning and public outreach; international issues; international organisations

Synopsis

The CIIP Handbook provides an overview of the critical sectors, national policies, organisational setup, programmes, mechanisms and services, and legal acts for critical information infrastructure protection (CIIP) in 25 nations globally. The second part of the handbook contains information about the relevant CIIP documents, events and actions of seven international organisations and forums. In the final section, overall conclusions on the (primarily national) state of CIIP are offered.

The cross-border (inter)dependency aspect is not paid much attention, but is mentioned in the context of recognising the cross-border nature of both threats and vulnerabilities especially due to common reliance of critical infrastructure on energy and telecommunications, and arguing for the necessity for public-private partnership and international cooperation in critical (information) infrastructure protection. Activities of international organisations in the area of cross-border CIIP are also included in the second part of the handbook.

Recommendations

The handbook asserts a need for a long-term research into CIP and CIIP matters. The authors recommend promotion of a holistic and strategic threat and risk assessment on an interdisciplinary level, including a physical, virtual and even psychological analysis.

[167] A constructed database of critical infrastructure outages and subsequent cascading effects as reported by international news sources. The database contained over 2590 critical infrastructure disruption events in 107 nations.

6. Towards a Research Framework for Critical Infrastructure Interdependencies

By Jose M. Sarriegi, Finn O. Sveen, J.M. Torres, Jose J. Gonzalez

International Journal of Emergency Management, 5/3/4 (2008), 235-249

Available at http://inderscience.metapress.com/content/H13776116K7T7602

Keywords

Crisis management; interdependencies; cross-border; modelling methodologies; sectoral vulnerabilities

Synopsis

The article identifies aspects that need to be investigated to gain a more complete understanding of the development of large-scale, cross-border crises in critical 'metasystems'. Aspects covered include understanding critical infrastructures as interdependent elements of a complex system; new complexities created by increasing interdependencies; dynamically complex nature of crises in critical infrastructure and the related need for a long-term perspective; the need to identify and bring together the fragmented and sectorally dispersed knowledge about CIs; the need for modelling techniques that can unite the fragmented critical infrastructure knowledge; and the need to create effective training and communication tools to transfer insights to crisis managers, policy-makers and the general public.

7. Dependency Indicators

By Theresa J. Brown, In *Wiley Handbook of Science and Technology for Homeland Security* (2008)

Keywords

Infrastructures; dependency indicators: geographical; physical; logical; modelling

Abstract

This chapter provides examples of infrastructure dependencies and representative dependency indicators developed in the course of creating models of infrastructures for disruption analysis. Infrastructures are a complex set of interconnected, interdependent systems of systems on which the nation, commerce, industry and individuals depend. Indicators provide a starting point for describing and evaluating infrastructures and their effects on each other, populations and commerce. Indicators do not provide historical or situational context, although they can be designed to account for long-term dynamics. The dynamics of infrastructure dependencies and interdependencies are due to variable supply and demand conditions occurring due to diurnal, seasonal variations as well as changes in physical infrastructure or the management of operations. Examples of widely used indicators developed for individual infrastructures and sectors are provided along with new indicators based on models of dynamic dependencies.

8. Final Report on Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure

By Dr. Stephan Gottwald, Industrieanlagen-Betriebsgesellschaft (European Commission DG Justice, Freedom and Security 2009)

Available at http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/2009_dependencies_en.pdf

Keywords

European Critical Infrastructures; modelling; critical energy infrastructure; critical finance Infrastructure; critical transport infrastructure; critical ICT dependencies; security standards; best practices

Synopsis

The study provides a systematic methodology for the assessment of the cross-sector and cross-border dependency of critical infrastructure on ICT, applying the method to the sample sectors of energy, transportation and finance. The primary objective of this exercise is to support the identification and designation of European Critical Infrastructures (ECI), but the study also offers input and guidance for national activities.

The report proposes definitions of criticality; rules on how to reduce the huge spectrum of ICT threats/sub-sectors/components to those expected to bear severely critical potential; and seek commonalities in the risk spectrum and procedures across the different critical infrastructures. Finally, recommendations for typical security measures to support decision-making are proposed.

9. Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating risks, and Interdependencies

By Tyson Macaulay, CRC Press, FL, USA, 2009

Available at http://www.crcpress.com/product/isbn/9781420068368

Keywords

Econometrics and critical infrastructure interdependency; information and data dependency analysis correlation; dependency latency; vulnerabilities; threat-risk; CI interdependency case studies;

Synopsis

The book looks at all the defined CI sectors, introducing an econometric concept for mitigating risks. It follows a strong focus on analysing the CI situation in Canada and the U.S. The book provides observations on the dependencies of each single sector (energy, communication and IT, finance, health, food, water, transport, safety and government, manufacturing) and draws a comparison study with the U.S. situation. In addition, the work presents information and data dependency analysis, and notably a case study on cyber-attacks on the water infrastructure. Finally it depicts the outbound cascading impacts under cyber-attack conditions.

10. Final Report JLS/2007/D1/037 Study: Stock-Taking of Existing Critical Infrastructure Protection Activities

By Booz & Company (Italia), 2009, contracting authority: European Commission

Available at http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/2009_cip_stock_taking_en.pdf

Keywords

Key actors; CI protection activities; public-private partnership and collaboration; sector-specific players; sector-specific initiatives

Synopsis

This study was conducted under the umbrella of the European Commission and provides an overview of existing CIP activities within the EU and EU countries as well as of Norway. It provides identification of key insights, key players and trends in the CIP field. The reader gets an easy to understand overview of each country examined; overview is also facilitated through charts and tables.

11. A Group Model Building Approach for Identifying Simulation Scenarios in Critical Infrastructure

By Finn Olav Sveen, Eliot Rich, Jose Manuel Torres, Josune Hernantes, Jose J. Gonzalez (Proceedings of the 43rd Hawaii International Conference on System Sciences – 2010)

Available at http://origin-www.computer.org/csdl/proceedings/hicss/2010/3869/00/04-06-01.pdf

Keywords

Crisis management; exercises; computer simulation; scenario design methodologies; cross-border impact; risks of uncoordinated single country action

Synopsis

The paper discusses the development of realistic crisis scenarios by using computer simulation methodology, based on the example of a critical infrastructure & IT crisis with cross-border effects. The example relies on a simulation model used to design and test policies with regard to energy supply crisis prevention and response, where ICT failure is an integral part of the assessment.

The lessons learned from the model indicate a negative effect of poorly coordinated single country action, potentially resulting increased duration and severity of the crisis due to information and communication delays and waste of resources.

12. Protecting Critical Infrastructure in the EU. CEPS Task Force Report

By Bernhard Hämmerli and Andrea Renda (Centre for European Policy Studies Brussels 2010)

Available at http://aei.pitt.edu/15445/1/Critical_Infrastructure_Protection_Final_A4.pdf

Keywords

Awareness; all-hazards/holistic approach; common risk metrics; C(I)IP policies; critical infrastructure resilience; emergency management; interdependencies (including cross-border); preparedness and resilience; public-

private partnership; risk assessment; standardised approach; vulnerabilities of critical infrastructure; economics of C(I)IP

Synopsis

The report studies the state of critical (information) infrastructure policies of the EU and contains recommendations with regard to future policy directions, both on the EU and the national level. It provides basic facts on CIP and CIIP and the existing policies; explains the delineation between CIP and CIIP, the key players, the CIP life cycle and existing trends in national policies for CIP and CIIP as well as the EU-level policy initiatives and EU actions. The analytical part of the study focuses on identifying the policy challenge with a look on the economics of CIP and CIIP, building common metrics, and assessing the EU's preparedness with regard to specific sectors. Finally, the report depicts a holistic approach to CIP and CIIP and makes recommendations for CIP policy, in particular with regard to the need to develop tools that are able to address the market failures that may emerge in different sectors.

The cross-border and interdependence dilemma is emphasised in the introductory part and mentioned throughout the report:

1. In the context of *threat and vulnerability awareness*:
   - Certain infrastructures are prone to trigger cross-border effects due to their inherently regional or global nature (energy sources, the Internet);
   - The current development of CIP policies is arguably focused at causes of failure of a given infrastructure due to a fault in a single component; while the 'dynamics with which the failure propagates to other critical infrastructures […], the impact of faults in ICT on critical infrastructures […] and the inter-state propagation of failures […]are little known today'.
2. In the context of current cross-border *threat response*:
   - The fragmented nature of national CIP policies (across the EU);
   - Lack of international cooperation between national governments and EU institutions in setting up coordinated emergency response, even in the case of common critical infrastructure (e.g. the Internet backbone network);
   - The effect of one nation's potentially weaker emergency response to the whole system and thereby to other nations.
3. In *recommendations*:
   - Adopt a coordinated, holistic approach encompassing both CIP and CIIP;
   - Build up a central CIP modelling and simulation centre for the EU 'to allow cross-border and multilateral infrastructure simulation, understanding complexity, dependencies and cascading effects';
   - Optimal public-private partnerships may be sector-specific.

Recommendations

The authors argue that in order for CIP policies to be meaningful, they should consider the need to develop tools that are able to address potential market failures in different sectors; in particular:

1. Providing a clear risk management and assessment framework;
2. Promoting information-sharing between public policy-makers;
3. Building up a central CIP modelling and simulation centre for the EU;
4. Facilitating information-sharing and cooperation between public and private agents; and
5. Promote awareness-raising initiatives;

Take action to ensure that missing CIP profiles and skills are developed.

13. Handbook on Securing Cyber-Physical Critical Infrastructure

By Sajal Das, Krishna Kant, Nan Zhang, 2012

Available at http://www.elsevier.com/books/handbook-on-securing-cyber-physical-critical-infrastructure/das/978-0-12-415815-3

Keywords

Cyber-physical infrastructure/networks; theoretic approach; game theory; security management

Synopsis

This handbook focuses on the technical challenges of CIs and provides theoretical approaches as well as solution methods. It demonstrates solution techniques for safeguarding critical cyber and physical infrastructures and their computing and communication architectures which form the basis of these systems by showing examples of both internal and external attack scenarios. It also points out the proper integration of policies and suggests how these human made policies could be enhanced by an automated system.

14. Cyber Security and Global Interdependence: What Is Critical?

By Dave Clemente (Chatham House 2013)
Available at http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0213pr_cyber.pdf

Keywords

Interdependence; emerging threats; realistic threat scenarios; responsibility of system owners; criteria of criticality; cross-border/global dependencies; risk management; case studies; distinction between 'infrastructure' and 'information infrastructure'

Synopsis

The paper analyses primary (including cross-border) challenges surrounding interdependence as it relates to cyber security and the protection of infrastructure. It argues that the current lack of conceptual clarity entails a risk of broadening categories of what is 'critical', thereby undermining sustained, focused and coordinated response and contributing to the waste of resources.

A comprehensive approach to critical infrastructure protection – i.e. one that integrates interests of all stakeholders – may be unrealistic due to varying interests and incentives among the parties. The author advocates designing policies that set clear core principles and are designed for flexibility and adaptation.

Recommendations

The following recommendations are made by the author:

- Adapt: Accept uncertainty where possible, encourage adaptability within organisational hierarchies.
- Prioritise: Scrutinise upstream and downstream risks, identify links with the highest levels of risk, and consider restricting dependency where uncertainty is too high and unowned risk too great. Draw broad sectors down to a manageable set of truly critical sub-sectors.
- Incentivise: Acknowledge the economic and political incentives that guide stakeholder behaviour. Higher levels of cyber security tend to lead to higher transaction costs in cyberspace; policy

interventions should therefore be calibrated with a long-term perspective and awareness of second- and third-order consequences.

- Invest in resilience: prioritise dependencies that also enhance resilience or redundancy.

15. The Making of Europe's Critical Infrastructure. Common Connections and Shared Vulnerabilities

By Per Högselius, Anique Hommels, Arne Kaijser, Erik van der Vleuten (Eds.) (Palgrave Macmillan 2013)

Keywords

Infrastructure vulnerabilities; case studies; European critical infrastructure; cross-border dependencies; joint interdependencies

Synopsis

The book demonstrates how present-day infrastructure vulnerabilities in Europe were shaped through the past policy choices of infrastructure builders, discussing the vulnerability perception, negotiation, and prioritisation of the era of infrastructure development. The book also investigates which countries and peoples were historically connected in joint interdependency, and why.

16. Interdependency-induced risk with applications to healthcare

By Polinpapilinho F. Katinaa, C. Ariel Pinto, Joseph M. Bradley, Patrick T. Hester

In International Journal of Critical Infrastructure Protection 7 (2014) 12-26, available at http://dx.doi.org/10.1016/j.ijcip.2014.01.005

Keywords

Structural complexity; interconnections; measuring interdependency; risk assessment; risk formulation; geographical healthcare interdependency

Synopsis

Based on the example of the healthcare sector, the authors discuss the influence of system interconnections to the protection, mitigation and recovery measures for critical infrastructures, arguing the need to understand and consider system interdependencies in risk formulation and risk management.

The paper is primarily valuable for outlining interdependency concerns in the healthcare sector and pointing out relevance of cross-border (inter)dependencies in the sector.

Publications by international organisations

17. OECD Recommendation of the Council on the Protection of Critical Information Infrastructures [C(2008)35]

Available at http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=121&Lang=en&Book=False

Keywords

Policy objectives; responsible government agencies; public-private partnership and cooperation; legal framework; interdependencies; risk management; information sharing; cross-border collaboration

Synopsis

An OECD document setting out general recommendations for member countries[168] regarding critical infrastructure protection (CIIP) cooperation, focusing in particular on policy-level domestic and cross-border CIIP activities.

Recommendations

With regard to cross-border aspects specifically, the recommendation notes the following:

a) Member countries are called on to systematically review policy and legal frameworks which apply to critical information (CII) infrastructure and address cross-border threats;

b) Member countries are called on to cooperate, both with other member countries and with the private sector, at the strategy, policy and operational levels to ensure the protection of CII beyond the capacity of individual countries to address alone. Among other issues, members are invited to proactively engage in bi- and multilateral cooperation is invited with the objective of:
   - Sharing knowledge and experience (on domestic policies and practices; on models for coordinating with private sector CII owners and operators);
   - Developing a common understanding of
     - risk management applicable to cross-border dependencies and inter-dependencies;
     - generic vulnerabilities, threats and impacts on the CII;
   - Supply information regarding the national agencies involved in the protection of CII, their roles and responsibilities (in order to facilitate identification of counterparts and improve the timeliness of cross border action);
   - Support participation in international or regional networks (with a view to enable operational-level information sharing and better manage crisis in case of an incident developing across borders);
   - Support cross-border collaboration and information sharing about research and development in critical information infrastructure protection.

18. Good Practices Guide on Non-Nuclear-Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace

By Organization for Security and Co-operation in Europe (OSCE) (2013)
Available at http://ec.europa.eu/energy/infrastructure/studies/doc/2013_08_good_practice_guide_on_nnceip.pdf

[168] Australia, Austria, Belgium, Canada, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States,

Keywords

Critical energy infrastructure; controlling risks in cross-border energy supply; cross-border risk management; risk governance framework; integrated (all-hazard) approach; risk-based approach; risk assessment; contingency planning; public-private partnerships; international/cross-border cooperation; best practices

Synopsis

The publication proposes a framework to encourage the formulation and implementation of policies and institutional management of cyber security related to critical energy infrastructure. It is based on a cooperative, integrated (all-hazard) and risk-based approach which emphasises achieving incident response preparedness, overall infrastructure resilience, and energy reliability, and encompasses both an EU cross-border and a non-EU cross-border dimension in addition to the national one.

Recommendations

The following are proposed as 'key policy recommendations' to addressing critical infrastructure vulnerabilities in the energy sector (including cross-border):

- Follow a comprehensive risk-based approach (dynamic critical infrastructure protection arrangements that are informed by an all-hazard and regularly updated assessment);
- Develop a multi-stakeholder co-operation framework (coordinated involvement of multiple stakeholders from different state agencies as well as the private sector and stakeholders across borders);
- Design flexible security arrangements ensuring an adequate minimum level of protection (taking into account the different vulnerabilities and risk environment of each critical energy infrastructure and their dynamic operation);
- Place greater emphasis on preparedness and overall resilience (advanced contingency planning, testing and exercising, including plans for communicating with the public/consumers and markets; more investments in network interconnections and alternative routes, as well as increasing storage capacity/strategic reserves);
- Identify and address cyber vulnerabilities of the energy sector (raising public and corporate awareness and understanding; development of cyber security expertise);
- Develop effective public-private partnerships (clear definition of roles and responsibilities, developing partnerships in areas of joint critical energy infrastructure security assessment, review of security measures, elaboration of contingency plans, and incident response training);
- Enhance cross-border cooperation (considering the potential impact of disruption of a single energy infrastructure – examine direct and indirect dependencies, commit to cooperating in order to ensure the integrity of energy infrastructure).

19. OECD Recommendation of the Council on the Governance of Critical Risks

Adopted on 6 May 2014

Available at http://www.oecd.org/mcm/C-MIN(2014)8-ENG.pdf

Keywords

Critical risks; cross-border impact; national risk assessment; non-structural measures; 'whole-of-society approach'; comprehensive/all-hazards approach; cross-border approach to country risk governance; public-private partnership

Synopsis

An OECD document setting forth general recommendations for member countries regarding country risk governance to enhance 'national resilience and responsiveness'. The recommendation promotes multidisciplinary, interagency approaches in primarily policy making and implementation.

No particular attention to cross-border critical information infrastructure (CII) dependencies, mainly advocating a comprehensive approach in risk management and international cooperation. Useful for contextualising cross-border CII measures with regard to existing international policy consensus.

Recommendations

The document makes the following recommendations to OECD member countries relevant to cross-border CII dependencies:

- Establish and promote a comprehensive, all-hazards and cross-border approach to country risk governance (including adopt an all-hazards approach that identifies interdependencies between critical systems);
- Raise awareness of critical risks to mobilise 'households, businesses and international stakeholders', as well as foster investment in risk prevention and mitigation (including facilitating cross-border cooperation using risk registries, media and other public communications on critical risks);
- Develop adaptive capacity in crisis management by coordinating resources across government, its agencies and broader networks to support timely decision making, communication and emergency responses (including by driving transboundary cooperation).

(Multi)national programme documents and instruments

20. National Infrastructure Protection Plan (NIPP). Partnering to enhance protection and resiliency

By United States Department of Homeland Security (2009)

Available at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Keywords

Public-private partnership; partnership criteria; risk management program; information sharing; roles and responsibilities; comprehensive risk picture/all-hazards approach; interconnected global networks; cross-border infrastructures; international CIIP activities

Synopsis

The NIPP is an in-depth arrangement outlining the principles and setup for partnership between the federal government, critical infrastructure owners and operators, and other agencies and partners in order to manage risks and achieve security and resilience in the critical infrastructure sectors. The plan defines processes and mechanisms for protection of U.S. CI and key resources; it recurrently considers international CIP issues, including interconnected global networks which the US critical infrastructure depends upon, implications of cross-border infrastructures (especially those with neighbouring countries), international vulnerabilities, as well as cross-sector (inter)dependencies.

21. Canada-United States Action Plan for Critical Infrastructure

By United States Department of Homeland Security/Public Safety Canada (Washington, DC/Ottawa 2010)

Available at http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf

Keywords

Cross-border cooperation; integrated approach to critical infrastructure protection and resilience; coordination of national activities; building partnerships; information sharing; risk management; best practices

Synopsis

The governments of United States Government and Canada agreed, in 2010, on a bilateral, cross-border plan to strengthening the resiliency of critical infrastructure (*Canada-United States Action Plan for Critical Infrastructure*). The plan promotes an 'integrated approach' to critical infrastructure protection and resilience by means of a) improving coordination of activities and b) facilitating 'continuous dialogue' among cross-border stakeholders. Three directions of activity are set:

- Building partnerships for critical infrastructure resiliency. This firstly includes the setup of an Emergency Management Consultative Group to support joint emergency management by means of promoting dialogue between stakeholders in Canada and the US and providing a platform for collaborative emergency management initiatives; and secondly, the establishment of sectoral partnerships between both nations' government departments and agencies, concentrating on discussion and information exchange among sector-specific industry and government stakeholders, but also joint activities such as risk assessments, exercises, and collaborative analytic products with cross-border applicability.
- Improving information sharing in terms of improving the protection of critical infrastructure information exchange (including compatible mechanisms and protocols under a Canada-US Framework), improving information products in priority areas, and coordinated information dissemination.
- Advancing risk management, including **'**setting protection and resiliency goals, identifying critical infrastructure and key dependencies, assessing and prioritising risks, developing and executing plans and programs to address the identified risks and dependencies, and measuring the effectiveness of the plans and programs'. Both Governments commit to work together develop plans to address priority areas, based on review of each country's risk-informed priorities and identification of areas of mutual interest.

It bears noting that the implementation of the Action Plan itself has been criticised for remaining superficial and overly modest in effort. As of 2012 however, both the US and Canadian Governments had apparently recommitted to raising the Action Plan issues among domestic policy priorities.[169]

[169] William de Laat 'The Beyond the Border Action Plan: A Tool for Enhanced Canada-U.S. Cooperation on Critical Infrastructure and Cyber Security - Or More Window Dressing', Canada-United States Law Journal, Vol. 37, Issue 2 (2012), pp. 451-468.

22. Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP) [SWD(2012)190 final]

By European Commission, 22.6.2012

Available at http://ec.europa.eu/dgs/home-affairs/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf

Keywords

EPCIP; evaluation of EPCIP; risk assessment methodology; EPCIP's external dimension; legal basis for critical infrastructure protection in the EU; implementation of Directive 2008/114/EC; Identification of ECI; designation of ECIs; risk analysis

Synopsis

The document offers the main findings of the comprehensive review carried out in 2011-2012 to assess the experience of implementing the European Programme for Critical Infrastructure Protection (EPCIP)[170] and Directive 2008/114/EC.[171] The review considers the three phases of European Critical Infrastructure (ECI) process: 1) identification of potential ECI, 2) designation of ECI, and 3) protection of ECI. It also takes into account developments since the adoption of the EPCIP Communication and the Directive (technological developments mainly in ICT, gas and electricity market liberalisation).

Main conclusions of the review were the following:

1. All Member States have legally implemented Directive 2008/114/EC and the process has (although by side effect) contributed to raising CIP awareness in the EU and in the Member States, as well as mainly bilateral cooperation of the Member States in the CIP process;
2. The varied setup of national CIP programmes rendered the Directive's sector-focused approach cumbersome (e.g. several Member States rely on system-focused or service-focused national CIP programmes, which involve activities across multiple sectors);
3. Member States with comparatively mature national CIP programmes did not see much added value from the Directive, although those with less mature programmes did benefit;
4. Overall, there was a dominant perception that the 'implementation of the Directive did not result in sufficiently clear and tangible improvements to ECI security levels'.

From a cross-border perspective, one of the main deficiencies of the current ECI approach appeared its inappropriateness for pan-European services, in particular main energy transmission networks, since vulnerabilities in such infrastructures and services could not be remedied by protective measures adopted by a single Member State or operator.

[170] Communication from the Commission on a European Programme for Critical Infrastructure Protection 12.12.2006; COM(2006)786 final <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF> accessed 8 December 2015. The EPCIP set the overall framework for activities aimed at improving the protection of critical infrastructure in Europe across all EU Member States.

[171] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L [2008] 345/75). The Directive constituted the first stage in an approach to identify, designate and adopt protective measures for infrastructures that are critical from a European perspective (European Critical Infrastructures or ECI, i.e. those which disruption would have an impact on at least two EU Member States). The Directive had to be transposed into Member States' national law by January 2011.

Section 5 (Report on the external dimension of EPCIP) of the review might be of particular interest in the context of cross-border activities in C(I)IP as it outlines cooperation initiatives and frameworks of some Member States with (typically neighbouring) non-EU countries. These include e.g. informal cooperation between the relevant national authorities in information and best practice exchange, discussions on methodological and procedural issues etc. Also, ongoing and intended cooperation of some EU Member States with US, Canada, Russia, Israel, and international organisations is described to some detail.

23. Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure [SWD(2013) 318 final]

By European Commission, 28.8.2013

Available at http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/docs/swd_2013_318_on_epcip_en.pdf

Keywords

EPCIP; risk assessment methodology; new approach to EPCIP; implementation of Directive 2008/114/EC; sectoral and cross-border (inter)dependencies; prevention, preparedness, and response

Synopsis

This document sets out a 'revised and more practical' implementation of the European Programme for Critical Infrastructure Protection (EPCIP), which offers common CIP and resilience tools and approach in the EU. Importantly, the new approach aims to take better account of interdependencies between critical infrastructures, industries and sectors, including those with a cross-border dimension.

The new approach bases upon the 2006 EPCIP framework[172] and retains Directive 2008/114/EC[173], but concentrates on four critical infrastructures of European dimension: Eurocontrol (EU Air Traffic Management Network Manager), Galileo (European programme for a global satellite navigation system), the electricity transmission grid and the gas transmission network (both of which are networks without national boundaries). It is expected that other relevant infrastructures can benefit from the processes and tools developed within these four ECIs, and the European Commission could potentially support the Member States in their own CI protection and resilience work and facilitate cooperation on CIP and resilience within the EU.

The new approach focuses on three phases: prevention (setting up tools for risk assessment and risk management), preparedness (increasing consideration for how the relevant parties can prepare in response to events affecting ECIs, and response (including long-term recovery of critical services).

[172] Communication from the Commission on a European Programme for Critical Infrastructure Protection 12.12.2006; COM(2006)786 final <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF> accessed 8 December 2015. The EPCIP set the overall framework for activities aimed at improving the protection of critical infrastructure in Europe across all EU Member States.

[173] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L [2008] 345/75). The Directive constituted the first stage in an approach to identify, designate and adopt protective measures for infrastructures that are critical from a European perspective (European Critical Infrastructures or ECI, i.e. those which disruption would have an impact on at least two EU Member States). The Directive had to be transposed into Member States' national law by January 2011.

As for CII and ICTs, operators of critical infrastructures would additionally fall under the risk management and incident reporting requirements of the proposed directive on network and information security[174]; in addition, the EU Cybersecurity Strategy[175] identifies actions that will contribute to the cyber resilience and security of infrastructures covered by EPCIP.

In addition, the document provides an overview of current EU level CIP-related actions and programmes (Section 2.4). A few of those appear to relate to CII interdependencies; however, no explicit reference to cross-border considerations is made in the programme descriptions.

[174] Brussels, 7.2.2013
COM(2013) 48 final
Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union
http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666

[175] High Representative of the European Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.' 7.2.2013 join(2013) 1 final <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667> accessed 8 January 2015.

Keyword index[176]

[176] Numeric references in the index point to the corresponding item in the literature review.

ANNEX:
National CI and CII coordinating authorities

AUSTRIA

CIP

Federal Chancellery

Website	www.bka.gv.at
E-mail	
Phone	

Ministry of the Interior

Website	www.bmi.gv.at
E-mail	sipol@bmi.gv.at
Phone	

Federal Ministry *(Federal Agency for State Protection and Counter Terrorism [BVT])*

Website	
E-mail	ski@bvt.gv.at aki@bvt.gv.at apcip@gv.at
Phone	

CIIP

Austrian Government Computer Emergency Response Team (GovCERT)

Website	www.govcert.gv.at
E-mail	reports@govcert.gv.at (security incidents) team@govcert.gv.at (other issues)
Phone	+43 1 5056416 78

BELGIUM

CIP and CIIP

National Crisis Centre

Website	http://crisiscentrum.be/nl
E-mail	crisiscentrum@ibz.fgov.be
Phone	+32 (0) 2 506 47 11
Fax	+32 (0) 2 506 47 09

Address	Hertogsstraat, 53 1000 Brussel, Belgium

CZECH REPUBLIC

CIP

Ministry of the Interior *(General Directorate of Fire Rescue Service of the Czech Republic)*

Website	http://www.hzscr.cz/hasicien/
E-mail	sekretariat.gr@grh.izscr.cz
Phone	+420 974 819 220
Fax	+420 974 819 960

CIIP

National Security Authority (NSA)

Website	http://www.nbu.cz/cs/ http://www.govcert.cz/en/
E-mail	czech.nsa@nbu.cz (international relations)
Phone	+420 257283 129
Fax	+420 257 283 220

ESTONIA

CIP

Ministry of the Interior (*Rescue and Crisis Management Policy Department)*

Website	https://www.siseministeerium.ee/en
E-mail	info@siseministeerium.ee
Phone	+372 612 5135
Address	Pikk 61, 15065 Tallinn, Estonia

CIIP

Estonian Information System Authority (RIA) *(Risk Control and Advisory Department, CIIP Section)*

Website	https://www.ria.ee/ciip/
E-mail	ragnar.rattas@ria.ee (Ragnar Rattas, Head of CIIP Section)
Phone	+372 666 8845

FRANCE

CIP

General Secretariat for Defence and National Security

Website	http://www.sgdsn.gouv.fr/site_rubrique70.html

E-mail	courrier.sgdsn@sgdsn.gouv.fr
Phone	
Address	51 boulevard de La Tour-Maubourg 75700 Paris 07 SP, France

CIIP

Network and Information Security Agency (ANSSI)

Website	http://www.ssi.gouv.fr/en/
E-mail	communication@ssi.gouv.fr
Phone	
Address	51 boulevard de La Tour-Maubourg 75700 Paris 07 SP, France

GERMANY

CIP and CIIP

German Federal Ministry of the Interior (BMI)

Website	http://www.bmi.bund.de/EN/Home/home_node.html
E-mail	poststelle@bmi.bund.de
Phone	+49 228 99 681 0 +49 30 18 681 0
Fax	+49-(0)30 18 681-2926
Address	Alt-Moabit 101D 10559 Berlin, Germany

CIIP

German Federal Office for Information Security (BSI)

Website	https://www.bsi.bund.de/EN/Home/home_node.htm https://www.bsi.bund.de/EN/Topics/Criticalinfrastructures/criticalinfrastructures_node.html
E-mail	poststelle@bsi.bund.de
Phone	+49 228 99 9582-0
Fax	+49 228 99 9582-5400
Address	Godesberger Allee 185-189 53175 Bonn, Germany

HUNGARY

CIP

Ministry of Interior *(National Directorate General for disaster Management)*

Website	http://www.katasztrofavedelem.hu/index.php
E-mail	
Phone	
Address	

CIIP

Government CERT/CIP CERT

Website	http://www.cert-hungary.hu/en
E-mail	ugyelet@govcert.hu
Phone	+36 1 336 4840
Fax	+36 1 269 1706
Address	1063 Budapest, Munkácsy Mihály u. 22 Hungary

ITALY

CIP and CIIP

Nucleus Inter Ministerial Unit for Situation and Planning (NISP)

Website	http://www.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/UfficiDirettaPresidente/ufficio_militare.html
E-mail	ucm@mailbox.governo.it ucm@palazzochigi.it
Phone	+39 06 6779 3871
Fax	+39 06 6779 2059
Address	Palazzo Verospi (Verospi Palace), Via della Impresa, 90 – 00187 Rome, Italy

CIIP

National Anti-Crime Computer Centre for Critical Infrastructure Protection (C.N.A.I.P.I.C.)

Website	http://www.poliziadistato.it/articolo/23401/ https://www.commissariatodips.it/profilo/cnaipic.html https://www.commissariatodips.it/profilo/contatti.html (regional offices)
E-mail	
Phone	

LATVIA

CIP

Ministry of Internal Affairs *(Commission of Intermediary Institutions for State Security)*

Website	http://www.iem.gov.lv/eng/
E-mail	kanceleja@iem.gov.lv
Phone	+371 67219263
Fax	+371 67829686

CIIP

Information Technology Security Incident Response Institution

Website	www.cert.lv
E-mail	cert@cert.lv cert@cert.gov.lv
Phone	+371 67085888
Fax	+371 67225072
Address	Raina bulvaris 29 Riga, LV-1459, Latvia

Constitution Protection Bureau

Website	www.sab.gov.lv
E-mail	sab@sab.gov.lv
Phone	+371 67025404
Fax	+371 67025406
Address	Post Box 286 Riga, LV-1001, Latvia

THE NETHERLANDS

CIP

National Coordinator for Security and Counterterrorism

Website	https://english.nctv.nl/
E-mail	
Phone	+ 31 70 751 50 50
Address	Postbus 16950 2500 BZ Den Haag, Netherlands

National Crisis Centre

Website	
E-mail	frontoffice-ncc@nctv.minvenj.nl
Phone	+31 70 751 54 00 (24/7)
Address	

CIIP

National Cyber Security Centre

Website	www.ncsc.nl
E-mail	info@ncsc.nl
Phone	+31 70 751 55 55
Address	Turfmarkt 147 2511 DP Den Haag, Netherlands

SPAIN

CIP

National Centre for the Protection of Critical Infrastructures (CNPIC)

Website	http://www.cnpic.es/en/index.html
E-mail	ses.cnpic-buzon@interior.es
Phone	

CIIP

National Institute of Cyber Security

Website	https://www.incibe.es/home/national_cibersecurity_institute/
E-mail	
Phone	+34 987 877 189
Fax	+34 987 261 016
Address	Avenida José Aguado, 41 Edificio INCIBE 24005 León

TURKEY

CIP

Ministry of Transport, Maritime Affairs and Communications

Website	http://www.ubak.gov.tr/
E-mail	
Phone	+90 312 203 10 00

Address	Hakkı Turayliç Cad. No: 5 06338 Emek/Ankara, Turkey

CIIP

Information and Communication Technologies Authority

Website	http://eng.btk.gov.tr/
E-mail	
Phone	+90 312 294 72 00 (contacts of regional offices available on the website)
Fax	+90 312 294 71 45
Address	Sokak No: 16 Demirtepe 06430 Ankara, Turkey

Bibliography

[1] Agence Nationale de la Sécurité des Systèmes d'Information, 'Information Systems Defence And Security: France's Strategy' (2011). <http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf> accessed 02 December 2014.

[2] Agence Nationale de la Sécurité des Systèmes d'Information, 'Mission'. <http://www.ssi.gouv.fr/fr/anssi/missions/> accessed 14 November 2014.

[3] Austrian Federal Agency for State Protection and Counter Terrorism (2014). <http://www.bmi.gv.at/cms/bmi_verfassungsschutz/> accessed 6 November 2014.

[4] Austrian Federal Chancellery, 'Austrian Cyber Security Strategy' (2013). <https://www.bka.gv.at/DocView.axd?CobId=50999> accessed 06 November 2011.

[5] Austrian Federal Chancellery, 'Austrian Security Strategy' (2013). <https://www.bka.gv.at/DocView.axd?CobId=52251> accessed 06 November 2011.

[6] Austrian Federal Economic Chamber, 'Statistical Classification of NACE, Austria ÖNACE' (2008). <https://www.wko.at/Content.Node/Interessenvertretung/ZahlenDatenFakten/Oenace_2008_2014.html> accessed 05 November 2014.

[7] Austrian Federal Government Cabinet of Ministers, 'Master Plan for the Protection of Critical Infrastructure' (2008). <http://www.kiras.at/uploads/media/MRV_APCIP_Beilage_Masterplan_FINAL.pdf> accessed 05 November 2014.

[8] Austrian Government Computer Emergency Response Team <http://www.govcert.gv.at> accessed 6 November 2014.

[9] Bauer J M, van Eeten M J G, Chattopadhyay T, Wu Y, 'ITU Study on the Financial Aspects of Network Security: Malware and Spam' (ITU 2008), < www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf> accessed 12 Dec 2014.

[10] Belgian Institute for Postal Services and Telecommunications (2014) <http://www.bipt.be/en> accessed 23 September 2014.

[11] Belgian National Crisis Centre, 'Législation'. <http://crisiscentrum.be/nl/inhoud/kritieke-infrastructuur-0> accessed 06 November 2014.

[12] Belgian National Crisis Centre, 'Evaluation De La Menace'. <http://crisiscentrum.be/fr/content/evaluation-de-la-menace-0> accessed 24 September 2014.

[13] Belgian National Crisis Centre. <http://crisiscentrum.be/nl> accessed 6 November 2014.

[14] Booz & Company (Italia) Srl, *Stock-Taking of Existing Critical Infrastructure Protection Activities* (European Commission 2009).

[15] Boszormenyi Z, Szente M. 'National Directorate General For Disaster Management (NDGDM)'. Katasztrofavedelem.Hu. <http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_intro&lang=eng> accessed 05 January 2015.

[16] Brown T, 'Dependency Indicators', *Wiley Handbook of Science and Technology for Homeland Security* (2008)

[17] Brunner E and Suter M, *International CIIP Handbook 2008/2009* (Center for Security Studies, ETH Zürich 2008) <http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf> accessed 14 October 2014

[18] 'Canada-United States Action Plan for Critical Infrastructure' (United States Department of Homeland Security/Public Safety Canada 2010) <http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf>, accessed 5 November 2014.

[19] Clemente D, *Cyber Security And Global Interdependence: What Is Critical?* (Chatham House 2013) <http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0213pr_cyber.pdf> accessed 21 November 2014

[20] Commission (EC) Green Paper on a European Programme for Critical Infrastructure Protection COM (2005) 576 final, Brussels 17.11.2005. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF> accessed 03 December 2014.

[21] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L [2008] 345/75).

[22] Csaba K, Szilárd T 'Hungary's Cyber Defense Readiness from the Perspective of International Recommendations' IX. Évfolyam 1. szám - 2014. Március. <http://hadmernok.hu/141_20_krasznaycs.pdf> accessed 07 November 2014.

[23] Das S, Kant K and Zhang N, *Handbook On Securing Cyber-Physical Critical Infrastructure* (Morgan Kaufmann 2012)

[24] Director General of the Crisis Centre (DGCC) of the Federal Public Service Justice of Belgium. <http://centredecrise.be/fr> accessed 23 September 2014.

[25] Estonian Information System Authority. <https://www.ria.ee/en/> accessed 2 December 2014.

[26] Estonian Ministry of Economic Affairs and Communications, 'Cyber Security Strategy 2014-2017' (2014). <https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf>.

[27] European Commission, *Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure,* 28.8.2013, SWD(2013) 318 final <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/docs/swd_2013_318_on_epcip_en.pdf> accessed 16 December 2014.

[28] European Commission, *Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP)*, 22.6.2012, SWD(2012) 190 final, <http://ec.europa.eu/dgs/home-affairs/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf>, accessed 16 December 2014.

[29] Frankfurter Allgemeine Zeitung, 'Unser Datenschutzrecht hat ausgedient' (2014). <http://www.faz.net/aktuell/politik/inland/de-maiziere-ueber-die-digitale-agenda-deutschland-wird-it-vorreiter-13103217.html>.

[30] Freese K, 'Cross-Border Issues In Protecting Critical Infrastructure From Terrorism', *Homeland Security: Protecting America's Targets* (Greenwood Publishing Group 2006)

[31] French General Secretariat for Defence and National Security. <http://www.sgdsn.gouv.fr/site_rubrique70.html> accessed 11 December 2014.

[32] French National Security Agency Information Systems (ANSSI), 'Missions', available at <http://www.ssi.gouv.fr/fr/anssi/missions/>, accessed 14 November 2014.

[33] German Federal Ministry of the Interior, 'Cyber Security Strategy For Germany' (2011). <http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile>.

[34] German Federal Ministry of the Interior, 'National Plan for Information Infrastructure Protection' (2005). <http://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf> accessed 02 October 2014.

[35] German Federal Ministry of the Interior, 'National Strategy For Critical Infrastructure Protection' (2009). <http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf> accessed 02 October 2014

[36] German Federal Ministry of the Interior, 'Nationale Strategie Zum Schutz Kritischer Infrastrukturen' (2009). <http://www.bmi.bund.de/cae/servlet/contentblob/598730/publicationFile/34416/kritis.pdf> accessed 30 June 2014.

[37] German Federal Ministry of the Interior, 'News Report: Federal Minister Of The Interior At The IT Summit' (2014). <http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/EN/2014/10/it-summit.html>.

[38] German Federal Office for Information Security, 'Critical Infrastructure Protection Plan' (2007). <https://www.bsi.bund.de/EN/Topics/Criticalinfrastructures/ImplementationPlan/implementationplan.html>, accessed 02 October 2014.

[39] German Federal Office for Information Security, 'Kritis - Sectors'. <http://www.kritis.bund.de/SubSites/Kritis/EN/introduction/sectors/sectors_node.html> accessed 11 December 2014.

[40] German Federal Office for Information Security, 'Recommendations For Critical Information Infrastructure Protection'. <https://www.bsi.bund.de/EN/Topics/Criticalinfrastructures/criticalinfrastructures_node.html> accessed 30 June 2014.

[41] German Federal Office for Information Security, 'Schutz Kritischer Infrastrukturen'. <https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Content_Cyber-Sicherheit/Strategie/kritis/kritis.html;jsessionid=2983CDCEAA93577F138A1C9B21B6E09C.2_cid359> accessed 01 October 2014.

[42] *Good Practices Guide On Non-Nuclear-Critical Energy Infrastructure Protection (NNCEIP) From Terrorist Attacks Focusing On Threats Emanating From Cyberspace* (Organization for Security and Co-operation in Europe (OSCE) 2013)

<http://ec.europa.eu/energy/infrastructure/studies/doc/2013_08_good_practice_guide_on_nnceip.pdf> accessed 14 November 2014

[43] Gottwald S, *Final Report On Study On Critical Dependencies Of Energy, Finance And Transport Infrastructures On ICT Infrastructure* (1st edn, Industrieanlagen-Betriebsgesellschaft; European Commission DG Justice, Freedom and Security 2009) <http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/2009_dependencies_en.pdf> accessed 21 November 2014

[44] Government of the Netherlands, 'Crises En Rampen Voorkomen' (2014). <http://www.rijksoverheid.nl/onderwerpen/veiligheid-en-terrorismebestrijding/crises-en-rampen-voorkomen> accessed 8 October 2014

[45] Government of the Netherlands, 'National Security'. <http://www.government.nl/issues/crisis-national-security-and-terrorism/national-security> accessed 12 November 2014.

[46] Government of the Netherlands, 'Protecting Critical Infrastructure'. <http://www.government.nl/issues/crisis-national-security-and-terrorism/protecting-critical-infrastructure> accessed 12 November 2014.

[47] High Representative of the European Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.' 7.2.2013 join(2013) 1 final <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667> accessed 8 January 2015.

[48] Hämmerli B and Renda A, *Protecting Critical Infrastructure In The EU. CEPS Task Force Report* (Centre for European Policy Studies 2010) <http://aei.pitt.edu/15445/1/Critical_Infrastructure_Protection_Final_A4.pdf> accessed 17 November 2014

[49] Högselius P and others, *The Making Of Europe's Critical Infrastructure* (Palgrave Macmillan 2013)

[50] Katina P and others, 'Interdependency-Induced Risk With Applications To Healthcare' (2014) 7 International Journal of Critical Infrastructure Protection

[51] Laprie J, Kanoun K and Kaâniche M, *Modelling Interdependencies Between The Electricity And Information Infrastructures* (LAAS-CNRS, Université de Toulous 2007) <http://arxiv.org/ftp/arxiv/papers/0809/0809.4107.pdf> accessed 17 October 2014

[52] Latvian Constitution Protection Bureau. <http://www.sab.gov.lv>.

[53] Latvian Information Technology Security Incident Response Institution. <https://www.cert.lv/?lang=en> accessed 11 December 2014.

[54] Luiijf H A M, Nieuwenhuijs A H, Klaver M H A, *Critical Infrastructure Dependencies 1-0-1* (2008), <http://publications.tno.nl/publication/102547/FOpThI/luiijf-2008-critical.pdf>, accessed 8 September 2014.

[55] Macaulay T, *Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, And Interdependencies* (CRC Press 2009)

[56] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, '5 Vragen Over Het Strategisch Overleg Vitale Infrastructuur (SOVI)' (2010). <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/brochures/2009/06/23/5-vragen-over-het-strategisch-overleg-vitale-infrastructuur-sovi/5vragenoversovi-1.pdf> accessed 12 November 2014.

[57] Ministerie van Veiligheid en Justitie, 'National Cyber Security Strategy: From Awareness to Capability 2' (2013).

[58] Ministerie van Veiligheid en Justitie, 'Strategie Nationale Veiligheid' (2007). <https://www.nctv.nl/Images/strategie-nationale-veiligheid-2007_tcm126-495325.pdf> accessed 12 November 2014.

[59] Ministerie van Veiligheid en Justitie, 'Working with Scenarios, Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands' (2009). <http://www.preventionweb.net/files/26422_guidancemethodologynationalsafetyan.pdf>, accessed 12 November 2014.

[60] Ministry of Transport, Maritime Affairs and Communications of the Republic of Turkey. <http://www.ubak.gov.tr/> accessed 12 November 2014.

[61] Ministry of Transport, Maritime Affairs and Communications of the Republic of Turkey, 'National Cyber Security Strategy and 2013-2014 Action Plan' (2013). <https://www.ccdcoe.org/sites/default/files/strategy/TUR_CyberSecurityEng.pdf> accessed 13 November 2014.

[62] National Coordinator for Security and Counterterrorism of the Netherlands. <https://english.nctv.nl/> accessed 2 December 2014.

[63] National Cyber Security Centre of the Netherlands, 'Coordination During Crisis' <https://www.ncsc.nl/english/services/crisis-management-reinforcement/coordination-during-crisis.html> accessed 13 November 2014

[64] National Cyber Security Centre of the Netherlands, 'ICT Response Board' (2014) <https://www.ncsc.nl/english/services/crisis-management-reinforcement/ict-response-board.html> accessed 13 November 2014

[65] 'National Infrastructure Protection Plan (NIPP). Partnering to Enhance Protection and Resiliency' (United States Department of Homeland Security 2009) <http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf>, accessed 15 December 2014.

[66] National Security Authority of the Czech Republic, 'Draft Regulation on Important Information Systems' (2014). <http://www.govcert.cz/download/nodeid-1227/>.

[67] National Security Authority of the Czech Republic, 'Draft Regulation On Cyber Security' (2014). <http://www.govcert.cz/download/nodeid-1216/>.

[68] National Security Authority of the Czech Republic, 'Explanatory Report on Draft Regulation On Important Information Systems' (2014). <http://www.govcert.cz/download/nodeid-1257/>.

[69] National Security Authority of the Czech Republic, 'Explanatory Report On The Draft Regulation On Cyber Security' (2014). <http://www.govcert.cz/download/nodeid-1304/>.

[70] NATO, 'Handbook For The Identification Of NATO Critical Dependencies On National CIS' (2013)

[71] OECD, *Recommendation of the Council on the Governance of Critical Risks*, 6 May 2014 <http://www.oecd.org/mcm/C-MIN(2014)8-ENG.pdf> accessed 17 November 2014

[72] OECD, *Recommendation Of The Council On The Protection Of Critical Information Infrastructures*, 30 April 2008 - C(2008)35 <http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=121&Lang=en&Book=False> accessed 17 November 2014

[73] Oxford Dictionaries, 'dependent, <http://www.oxforddictionaries.com/definition/english/dependent> accessed 2 December 2014.

[74] Oxford English Dictionary, 'dependency', <http://www.oed.com/view/Entry/50244?redirectedFrom=dependency#eid>, accessed 2 December 2014.

[75] Pederson P and others, *Critical Infrastructure Interdependency Modeling: A Survey of U.S. And International Research* (Idaho National Laboratory 2006) <http://www.inl.gov/technicalpublications/Documents/3489532.pdf> accessed 18 November 2014

[76] Presidency of the Council of Ministers of the Government of Italy, 'National Strategic Framework For Cyberspace Security' (2013). <http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf>.

[77] Pruyt E, Wijnmalen D, 'National Risk Assessment In The Netherlands: A Multi-Criteria Decision Analysis Approach (ed), *Multiple Criteria Decision Making for Sustainable Energy and Transportation Systems. Proceedings of the 19th International Conference on Multiple Criteria Decision Making, Auckland, New Zealand, 7th - 12th January 2008* (Springer 2010).

[78] Rinaldi S, Peerenboom J, and Kelly T, 'Identifying, Understanding and Analysing Critical Infrastructure Interdependencies', IEEE Control Systems Magazine, December 2001. <http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf> accessed 7 May 2014.

[79] Sarriegi J and others, 'Towards A Research Framework For Critical Infrastructure Interdependencies' (2008) 5/3/4 International Journal of Emergency Management, 5/3/4 (2008), 235-249 <http://inderscience.metapress.com/content/H13776116K7T7602> accessed 17 November 2015

[80] Seidl M, Šimák L, 'Protection Of Critical Infrastructure' (2014) 1 Logistics and Transport. <http://www.logistics-and-transport.eu/index.php/main/article/viewFile/204/197> accessed 11 December 2014.

[81] Spanish Cyber Security Institute, 'National Cyber Security, A Commitment For Everybody' (2012). <http://www.ismsforum.es/ficheros/descargas/a-national-cyber-security-strategy-.pdf> accessed 10 November 2014.

[82] Spanish National Centre for the Protection of Critical Infrastructure (CNIP) (2014). <http://www.cnpic.es/en/index.html> accessed 10 November 2014.

[83] Spanish National Institute of Cyber Security, 'INCIBE-CERTSI, Critical Infrastructures'. <https://www.incibe.es/CERT_en/Critical_Infrastructures/> accessed 13 November 2014.

[84] Spanish National Institute of Cyber Security, 'INCIBE-CERTSI, Publications'. <https://www.incibe.es/CERT_en/publications/> accessed 10 November 2014.

[85] Springer A, 'Bund Plant TÜV für IT-Sicherheit' *Die Welt* (2014). <http://www.welt.de/print/welt_kompakt/article131357115/Bund-plant-TUeV-fuer-IT-Sicherheit.html>.

[86] Study*: Stock-Taking Of Existing Critical Infrastructure Protection Activities. Final Report JLS/2007/D1/037* (European Commission 2009) <http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/2009_cip_stock_taking_en.pdf> accessed 12 November 2014

[87] Sveen F and others, *A Group Model Building Approach For Identifying Simulation Scenarios In Critical Infrastructure* (Proceedings of the 43rd Hawaii International Conference on System Sciences 2010) <http://origin-www.computer.org/csdl/proceedings/hicss/2010/3869/00/04-06-01.pdf> accessed 19 November 2014

[88] U.S. Department of Homeland Security, 'National Infrastructure Protection Plan' (2009). <http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf> accessed 02 December 2014.

National legal acts

BELGIUM

[1] Loi du 1er juillet 2011, Loi relative à la sécurité et la protection des infrastructures critiques (2011). <http://www.ejustice.just.fgov.be/mopdf/2011/07/15_2.pdf#Page6> accessed 02 July 2014.

[2] Loi relative à la sécurité et la protection des infrastructures critiques (NOTE : Consultation des versions ant érieures à partir du 15-07-2011 et mise à jour au 07-05-2014) <http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2011070108&table_name=loi>

[3] Royal Decree of 27th May 2014, 'Arrêté royal exécution dans le secteur des communications électroniques de l'article 13 de la loi du 1er juillet 2011 relative á la sécurité et la protection des infrastructures critiques', C-2014/11429, Moniteur Belge 11.08.2014. <http://www.bipt.be/en/operators/telecommunication/legislation/national-framework/royal-decree-of-27-may-2014-implementing-in-the-electronic-communications-sector-article-13-of-the-act-of-1-july-2011-on-the-security-and-protection-of-critical-infrastructures>, accessed 25 September 2014.

CZECH REPUBLIC

[4] Crisis Management Act No. 240/2000 Coll. <http://www.hzscr.cz/hasicien/file/crisis-management-act-n-240-2000-coll-pdf.aspx>

[5] Act on Cyber Security and Change of Related Acts (Act on Cyber Security) no. 181/2014 Coll. <http://www.govcert.cz/download/nodeid-577/>; <http://www.govcert.cz/download/nodeid-591/> [in English].

ESTONIA

[6] Hädaolukorra seadus (RT I 2009, 39, 262), passed 15.06.2009. [Emergency Act; English translation available <https://www.riigiteataja.ee/en/eli/517122014005/consolide> accessed 19 December 2014].

[7] Korrakaitseseadus (RT I, 12.07.2014, 84), passed 23.02.2011. [Law Enforcement Act; English translation available <https://www.riigiteataja.ee/en/eli/522082014007/consolide> accessed 19 December 2014].

[8] Vabariigi Valitsuse 25.04.2013 korraldus nr 208 'Nende hädaolukordade nimekiri, mille kohta koostatakse riskianalüüs ja lahendamise plaan, ning hädaolukorra riskianalüüsi ja hädaolukorra lahendamise plaani koostamiseks pädevate täidesaatva riigivõimu asutuste määramine', (RT III, 30.04.2013, 16) [in Estonian].

[9] Vabariigi Valitsuse 14.03.2013 määrus nr 43 "Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmed" (RT I, 20.03.2013, 7) [Security Measures for Vital Service Information Systems and Related Information Assets; English translation at <https://www.ria.ee/public/KIIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf>, accessed 03 December 2014].

FRANCE

[10] Act No. 2013-1168 on Military Programming for the years 2014 to 2019 and Various Provisions Concerning Defence and National Security, 18 December 2013. <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte&categorieLien=id> accessed 14 November 2014.

[11] Decree No. 2009-834 Establishing a National Service Called 'National Security Agency Information Systems', 7 July 2009. <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212> accessed 27 November 2014.

[12] French Defence Code. <http://www.legifrance.gouv.fr/affichCode.do;jsessionid=FE83165666A431AE6F030DBDB97612DE.tpdjo17v_2?idSectionTA=LEGISCTA000028342597&cidTexte=LEGITEXT000006071307&dateTexte=20141113> accessed 03 July 2014.

[13] Prime Minister's Order Establishing on the List of the Sectors of Critical Infrastructure and Designating Coordinating Ministers of these Sectors, 2 June 2006. <http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20060604&numTexte=1&pageDebut=08502&pageFin=08502> accessed 14 November 2014.

GERMANY

[14] Draft of German Law on the Security Enhancement of IT systems (IT-Security law), 18 August 2014. <http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf?__blob=publicationFile> accessed 21 August 2014.

HUNGARY

[15] Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies. <http://www.nbf.hu/anyagok/Act%20L%20of%202013%20on%20the%20Electronic%20Information%20Security%20of%20Central%20and%20Local%20Government%20Agencies.docx> accessed 07 November 2014.

[16] Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies. Justification for the Act on the Electronic Information Security of Central and Local Government Agencies <http://www.nbf.hu/anyagok/Act%20L%20of%202013%20on%20the%20Electronic%20Information%20Security%20of%20Central%20and%20Local%20Government%20Agencies.docx> accessed 07 November 2014.

ITALY

[17] Decreto del Ministro dell'Interno, 9 January 2008. <http://archivio.cnipa.gov.it/HTML/RN_ICT_cron/si_20080109%20Decreto%20Ministero%20interno.pdf> [in Italian], accessed 14 November 2014.

[18] Decree of the President of the Council of Ministers of 5 May 2010 final (National Organization for Crisis Management). <http://www.gazzettaufficiale.it/gunewsletter/dettaglio.jsp?service=1&datagu=2010-06-17&task=dettaglio&numgu=139&redaz=10A07594&tmstp=1276847998921>, [in Italian], accessed 04 December 2014

[19] Decree of the President of the Council of Ministers, 'Directive Laying Down Guidelines for the National Defence and Cyber Security', 24 January 2013, (OJ Series General n.66 of 19/03/2013), art 11 para 1.

[20] Law no 124, 'Information System for the Security of the Republic and New Secret Discipline', 3.08.2007. <http://www.camera.it/parlam/leggi/07124l.htm accessed 25 November 2014

[21] Legislative Decree no. 61, 11 April 2011. <http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2011-05-04&atto.codiceRedazionale=011G0101&elenco30giorni=false>. A short summary of the Decree is available

at <http://terna2011.message-asp.com/en/electricity-system/italy%E2%80%99s-regulatory-framework> accessed 04 December 2014.

[22] Legislative Decree no 259, 'Electronic Communications Code', 18 December 2013, (OJ 214 of 09.15.2003 - Suppl. Ordinario n. 150). <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-08-01;259>.

LATVIA

[23] Cabinet Regulation No. 496, 'Procedures for the Identification of Critical Infrastructures, Including European Critical Infrastructures and Planning and Implementation of Security Measures', 1 June 2010.

[24] Cabinet Regulation No 100, 'Procedures for the Planning and Implementation of Security Measures for the Critical Infrastructure of Information Technologies'. Adopted on 1 February 2011. <http://likumi.lv//ta/id/225776>; English translation available at <http://www.vvc.gov.lv/export/sites/default/docs/LRTA/MK_Noteikumi/Cab._Reg._No._100_-_Planning_and_Implementation_of_Security_Measures.doc>.

[25] Law on the Security of Information Technologies (2010). English text available at <http://www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_the_Security_of_Information_Technologies.doc>.

NETHERLANDS

[26] Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet). <http://wetten.overheid.nl/BWBR0009950/volledig/geldigheidsdatum_12-11-2014>

SPAIN

[27] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas [Act for the Establishment of CIP Measures]. <http://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf> accessed 10 November 2014.

[28] Real Decreto 704/2011, de 20 de mayo por el que se aprueba el Reglamento de protección de las infraestructuras críticas <http://www.boe.es/boe/dias/2011/05/21/pdfs/BOE-A-2011-8849.pdf> accessed 10 November 2014.

TURKEY

[29] Decree No. 2011/2237 on the Regulation Amending the Regulation on Military Forbidden Zones and Security Zones, 18th October 2011. <http://www.resmigazete.gov.tr/eskiler/2011/10/20111018-4.htm> [in Turkish], accessed 12 November 2011.

[30] Legislative Decree on Organization and Duties of the Ministry of Transport, Maritime Affairs and Communication, 1.11.2011. <http://www.ubak.gov.tr/BLSM_WIYS/UBAK/en/en_dokuman_sol_menu/20120402_144700_204_2_64.pdf> accessed 12 November 2014.

[31] Electronic Communications Law (ECL) (2008). Updated version (2014) available at <http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6518.pdf> [in Turkish]; English non-updated version available at <http://eng.btk.gov.tr/mevzuat/kanunlar/dosyalar/5809.pdf> accessed 12 November 2014.